SECOND AMENDMENT TO MANAGED CARE SOFTWARE AGREEMENT BETWEEN EAP EXPERT INC. AND POUDRE SCHOOL DISTRICT R-1

This Second Amendment ("Second Amendment") effective as of the 27th day of July, 2025, is attached to and forms part of the Managed Care Software Agreement between and Poudre School District R-1 (the "District") and EAP Expert Inc. (the "Contractor") executed May 2, 2023 and the First Amendment to the Agreement executed July 23, 2024 ("Agreement"), both of which are attached and made part of this Second Amendment. To the extent that any of the terms or conditions contained in this Second Amendment may contradict with any of the terms or conditions of the attached Agreement, it is expressly understood and agreed that the terms of this Second Amendment shall take precedence and supersede the attached Agreement. The parties agree to amend the Contract by adding the following language:

1. **Purpose of Amendment.** This Amendment shall constitute the Second Amendment to the Agreement between the District and the Contractor. The purpose of this Second Amendment is to amend the terms and deliverables between the District and Contractor.

2. **Term of Agreement.**

   2.1. At the conclusion of the term dated July 31, 2025, as outlined in section 2.1 of the Agreement, the District and Contractor elect to extend the term of the Agreement beginning on August 1, 2025, through July 31, 2026.

3. **Special Provisions.**

   3.1. **Terms and Conditions.** With the exception of items explicitly delineated in this Second Amendment, all terms and conditions of the original Agreement between the District and Contractor shall remain unchanged and in full force and effect.

4. **General Provisions.**

   4.1. **Entire Agreement.** The original Agreement, the First Amendment and this Second Amendment, constitutes the entire Agreement of the parties regarding the subject matter addressed herein and supersedes all prior Agreements, whether oral or written, pertaining to said subject matter.

   4.2. **Signatures.** This Agreement may be executed and delivered via portable document format (pdf), and the pdf signature of any party shall be considered valid, binding, effective and an original for all purposes.

IN WITNESS WHEREOF, the District and the Contractor have signed this Agreement as of the date first set forth above.

EAP EXPERT, INC.

By: Chris Coleman

Name: Chris Coleman
Title: SVP, Global Solutions

POUDRE SCHOOL DISTRICT R-1

By: R David Montoya
R David Montoya (Aug 19, 2025 09:52:46 MDT)

R. David Montoya
Chief Finance Officer

By: Renee Gilkey
Renee Gilkey (Aug 19, 2025 09:21:00 MDT)

~~Barbara Fisher~~ Renee Gilkey
Employee Assistance Services Manager

FIRST AMENDMENT TO MANAGED CARE SOFTWARE AGREEMENT BETWEEN EAP EXPERT INC. AND POUDRE SCHOOL DISTRICT R-1

This First Amendment ("Amendment") effective the 23rd day of July 2024, is attached to and forms part of the Managed Care Software Agreement between Poudre School District R-1 (the "District") and EAP Expert Inc. (the "Contractor") executed May 2, 2023 ("Agreement"), hereby attached and made part of this Amendment. To the extent that any of the terms or conditions contained in this Amendment may contradict with any of the terms or conditions of the attached Agreement, it is expressly understood and agreed that the terms of this Amendment shall take precedence and supersede the attached Agreement. The parties agree to amend the Agreement by adding the following language:

1. **Purpose of Amendment.** This Amendment shall constitute the First Amendment to the Agreement between the District and the Contractor. The purpose of this Amendment is to amend the terms and deliverables between the District and Contractor.

2. **Term of Agreement.**

   2.1. At the conclusion of the term dated July 31, 2024, as outlined in section 2.1 of the Agreement, the District and Contractor elect to extend the term of the Agreement beginning on August 1, 2024, through July 31, 2025.

3. **Amended Responsibilities.**

   3.1. Within section 21, delete the language which has a strikethrough and replace with the following language which is underlined:

   Poudre School District R-1
   Attn: ~~Tracy Stibitz~~
   2407 LaPorte Avenue
   Fort Collins, CO 80521
   E-mail: ~~tstibitz@psdschools.org~~

   Poudre School District R-1
   Attn: Contracts Administrator
   2407 LaPorte Avenue
   Fort Collins, CO 80521
   E-mail: contracts@psdschools.org

4. **Special Provisions.**

   4.1. Terms and Conditions. With the exception of items explicitly delineated in this Amendment, all terms and conditions of the original Agreement between the District and Contractor shall remain unchanged and in full force and effect.

5. **General Provisions.**

5.1. Entire Agreement. The original Agreement and this First Amendment constitutes the entire Agreement of the parties regarding the subject matter addressed herein and supersedes all prior Agreements, whether oral or written, pertaining to said subject matter.

5.2. Signatures. This Agreement may be executed and delivered via portable document format (pdf), and the pdf signature of any party shall be considered valid, binding, effective and an original for all purposes.

IN WITNESS WHEREOF, the District and the Contractor have signed this Agreement as of the date first set forth above.

EAP EXPERT INC.

By: Chris Coleman
Chris Coleman (Aug 9, 2024 08:00 EDT)

Name: Chris Coleman
Title: SVP, Global Solutions

POUDRE SCHOOL DISTRICT R-1

By: R David Montoya
R David Montoya (Aug 11, 2024 18:20 MDT)

R. David Montoya
Chief Finance Officer

By: Barb Fisher
Barb Fisher (Aug 11, 2024 10:19 MDT)

Barbara Fisher
Employee Assistance Services Manager

MANAGED CARE SOFTWARE AGREEMENT
BETWEEN EAP EXPERT INC.
AND POUDRE SCHOOL DISTRICT R-1

This Managed Care Software Agreement ("Agreement") is entered into as of the 2nd day of May 2023, by and between Poudre School District R-1, a school district organized and existing under the laws of the state of Colorado (the "District"), and EAP Expert Inc. ("Contractor"), collectively referenced herein as the "parties." In consideration of the mutual covenants and promises contained in this Agreement, the sufficiency of which is hereby acknowledged, the parties agree as follows:

1. **Purpose of Agreement.** The purpose of this Agreement is to specify the terms and conditions pursuant to which Contractor will provide Employee Assistance Program and Managed Care Software.

2. **Term and Termination of Agreement.**

2.1. This Agreement shall commence as of the date first set forth above and shall continue through and including July 31, 2024, unless earlier terminated as provided herein. The Agreement, at the option of the District, may be extended for up to four (4) additional one-year terms, upon a written mutually agreed upon amendment for each one-year term.

2.2. Notwithstanding any other term or provision of this Agreement, the District's obligations hereunder are expressly subject to its budgeting and appropriation of sufficient funds for each fiscal year (July 1 - June 30) an Agreement is in effect. In no event, shall the District's obligations in an Agreement constitute a multiple-fiscal year direct or indirect debt or other financial obligation under Article X, Section 20(4)(b) of the Colorado Constitution.

2.3. Notwithstanding the provisions of sections 2.1 and 2.2 above, either party may terminate this Agreement at any time in that party's sole discretion for any reason, with or without cause, by providing the other party with thirty (30) days' advance written notice. In the event of such termination: (a) the District shall pay Contractor for all Services performed under and in accordance with this Agreement up to the date of termination; and (b) Contractor shall reimburse the District for all payments made in excess of Services performed up to the date of termination.

3. **Obligations of Contractor.**

3.1. The Contractor's responsibility under this Agreement is to provide Employee Assistance Program and Managed Care Software. The parties agree to the following, as specified in:

3.1.1. Request for Proposal ("RFP") #23-690-001, which is part of this agreement and attached hereto as Exhibit A.

3.1.2. Contractor's Response to RFP #23-690-001, which is part of this agreement and attached hereto as Exhibit B.

3.1.3. All documents which are made a part of this Agreement (hereinafter the "Services") and incorporated herein by reference.

3.2. The total cost for all Services under this contract as set forth on the attached Exhibit B, shall not exceed Eight Thousand, Four Hundred and Ninety-Six Dollars and Zero Cents ($8,496.00), due and payable thirty (30) days from receipt of Contractor's invoice.

3.3. Services shall be provided at the direction as authorized by the District's Employee Assistance Services Manager or designee ("Project Coordinator").

4. **Scope of Work Design Plan.** The Contractor, Project Coordinator and any other necessary personnel shall hold a kickoff meeting within seven (7) days of execution of this Agreement and develop a collaborative execution plan for the full scope of the project within the fourteen (14) days of first kickoff meeting, which shall include but not limited to:

4.1. Identify key lead for each party.

4.2. Identify key contacts and team members from both parties for project.

4.3. Identify roles, responsibilities and expectations for each team member.

4.3.1. Anticipated workforce hours for Contractor.

4.3.2. Determine expectation for District staff resources.

4.4. Identify key external and internal groups integral to project.

4.4.1. Outline expectation of external and internal groups.

4.5. Outline communication plan, procedures and format.

4.6. Parties shall clearly identify mutual understandings of:

4.6.1. Identified scope of work

4.6.2. Completion of objectives

4.6.3. Overview of Contractors proposed methodology

4.7. Develop Timeline for key deliverables, which shall include:

4.7.1. Benchmarks for progress checks to ensure timely completion of deliverables.

4.7.2. Measurable indicators of deliverables

4.7.3. Key deliverables target completion dates.

4.8. Identify project constraints across the projected timeline.

4.9. Timeline and schedule of deliverables.

4.9.1. Timeline shall include any anticipated training or onboarding service hours and total estimated billable costs.

4.9.2. No changes or modifications to timeline or schedule shall be allowed, except through a mutual written approval from the Project Coordinator and Contractor key lead.

4.10. If both parties are unable to come to an agreement on the scope of work outlined in this section 4 within forty-five (45) days from the first day of the kickoff meeting, then the parties may mutually agree to discontinue the Agreement.

5. **Implementation Plan.**

5.1. Contractor shall work directly with the District's Project Coordinator to develop a plan for Services for implementation ("Implementation Plan").

5.2. Contractor shall provide updates to the Implementation Plan to the Project Coordinator for review and approval based on the timeline established in section 4.7.

5.2.1. Project Coordinator reserves the right to request modification, additions or additional services to Implementation Plan as they determine appropriate.

5.3. Any delay beyond the completion date, must be submitted in writing to the Project Coordinator. Delays will be denied or approved in writing by the Project Coordinator.

6. **Review of Product.** Payment for Services furnished under the Contract shall not constitute acceptance thereof. The Project Coordinator shall have the right to confirm the completion of the Services provided, the product of such Services, and to reject any or all of which are in the District's judgment defective or nonconforming. In addition to the District's other rights, and Services which had been rejected. The District will not be charged for Services to correct Contractor's errors for correcting such Services.

7. **Acceptance of Services.** Services are considered complete, only after the Project Coordinator has formally accepted Services in writing. Payments will not be made until Services are formally accepted.

7.1. The Project Coordinator reserves the right to cancel Services at any time upon written notice, including Services which may have been requested and have not been completed.

8. **Timeline Delays or Extension of Work.** If the Contractor experiences a delay in the completion of work, the Contractor shall provide a reasonable period of time, which does not delay the timeline for completion identified in section 4.7.

8.1. The Contractor shall not invoice the District for any delayed Services or products to be produced.

8.2. The District shall determine what constitutes a reasonable period of time and may cancel requested Services, seek the items from another Contractor, and may charge the original Contractor for any difference in costs.

9. **Materials.** All labor, licenses, materials, supplies, equipment, and all other items necessary to complete the Services shall be furnished by the Contractor (the "Materials") and shall be part of and not in addition to the Agreement price. The Contractor shall be responsible and liable for any damage or destruction to any Materials resulting from any cause other than the willful or reckless acts of the District for which it could be held liable under the Colorado Governmental Immunity Act.

10. **Primary Contractor and Subcontractors.** The Contractor shall assume all responsibility for performance of all Services in this Agreement, whether or not the Contractor uses subcontractors. Any consequences resulting from non-performance under the terms of this Agreement are the sole responsibility and liability of the Contractor. The Contractor shall be the sole point of contact with the District with regard to all matters covered by this Agreement. The District shall not initiate or maintain contact with any subcontractor unless such contact becomes necessary to mitigate the District's damage in the event the Contractor is in default or breach of any term or obligation of this Agreement.

11. **Confidential Information.**

11.1. **Ownership of Confidential Student Records, Information, Photography, and Developed Materials.** All confidential student records, personally identifiable student information, photography, and developed materials shall remain the exclusive property of the District with all rights, title and interest including but not limited to intellectual property rights, to the confidential student records and information, photography and developed materials, belonging to and retained solely by the District.

11.2. **Non-Disclosure of Confidential Information.** Contractor understands that while performing Services under this Agreement, it may be provided access to student records or personally identifiable information protected from disclosure to third parties and subject to the Individuals with Disabilities Education Act (20 U.S.C. §§ 1400 et seq.), the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) ("FERPA") and the Colorado Open Records Act (C.R.S. §§ 24-72-201 *et seq.*). Such records and information are considered confidential and protected. Accordingly, Contractor hereby agrees that it shall keep confidential and shall not disclose any information, including but not limited to information regarding any District student, student family, student health/medical condition, student disability, student IEP and/or student accommodation, to which it gains access in connection with its provision of the Services. To the extent Contractor has access to such records and information, Contractor shall be deemed a "school official" as such term is defined under FERPA. Contractor agrees that it or its employees, volunteers and subcontractors shall not use education records or personally identifiable student information for any purpose other than in performance of this Agreement.

11.2.1. At the termination of this Agreement or earlier, if requested by the District, Contractor shall promptly return all such information, and/or shall at the request of the District destroy or delete any and all copies or duplicates of said information, whether the information is in hard copy or electronic form. If Contractor violates the terms of this section 11.2.1, Contractor agrees to indemnify, defend and hold harmless the District, and/or its employees and agents, from any and all claims, liabilities, or causes of action, including attorney fees and costs, asserted against the District and/or its employees or agents as a result of the violation. Contractor also agrees to indemnify the District, and/or its employees and agents, from the costs of complying with and/or resolving any regulatory investigation caused by the violation, including costs and attorney fees.

11.3. **Obligations and Return of Confidential Information.** The receiving parties obligation hereunder shall survive for a period of five (5) years following termination of this Agreement; provided however, any confidential obligations with respect to protected District information shall survive indefinitely to the extent required to comply with applicable law. All confidential information shall remain the sole property of the disclosing party, and all materials containing any such confidential information, including all copies made by the receiving party, shall be returned to the disclosing party or destroyed immediately upon termination or expiration of this Agreement, or upon the receiving party's determination that it no longer has a need for such confidential information. Upon the request of the disclosing party, the receiving party shall certify in writing that all materials containing such confidential information, including all copies thereof, have been returned to the disclosing party or have been destroyed.

11.4. **Colorado Open Records Act.** Information and materials submitted under this Agreement may be considered public records subject to disclosure under the Colorado Open Records Act, (C.R.S. §§ 24-72-200.1 to -205.5) ("CORA"). Information and materials that the Contractor believes are confidential and not subject to disclosure under CORA must be submitted separately with a citation to the section of CORA and any other relevant law under which the Contractor believes they are confidential. The District, not the Contractor, shall determine whether information and materials so identified will be withheld as confidential, but will inform the Contractor in advance of disclosure to give it an opportunity to take legal action to protect its interests vis-à-vis the party making the CORA request.

12. **Warranties.** Notwithstanding prior acceptance of Services by the District, the Contractor shall expressly warrant all Services or deliverables provided under this Agreement, will be of good quality, new and properly functioning at the start of operations and conform to any sample and any specifications, drawings or other description furnished or adopted by the District and will be fit and sufficient for their intended purpose, of merchantable quality, of good material and workmanship and free from defect. Contractor warrants that all Services furnished under the Contract shall be new unless otherwise specified by the District, and that the title conveyed regarding such Services shall be complete and its transfer

rightful The warranty period will begin at the time the Services or deliverables have been formally accepted in writing by the District.

12.1. Contractor further warrants that the development processes and methods employed to perform the work shall be suitable for the results required and expected. If the Contractor proposes to use an unproved and untried method, process or product, the District must be advised of the proposal in writing and give approval. The District may permit experimentation but may require special guarantees by the Contractor to cover the experimental work. The Contractor shall assign to the District all manufacturers' warranties and guarantees upon acceptance of Services.

12.2. Nothing contained in this section 12 shall affect the warranties provided by the Contractor through any proposal submissions, product literature, exhibits or other warranties provided as part of the scope of this Agreement.

12.3. During the warranty period, the Contractor will correct all defects and/or deficiencies associated with this contract and replace incorrect or defective Services within five (5) business days of written notification from the District to the Contractor. If, within five (5) business days after written notice by the District to the Contractor, the Contractor has not corrected all defects and/or deficiencies, the District may correct all defects and/or deficiencies at the Contractor's expense.

12.4. The Contractor shall be responsible and bear all costs to correct any problems, defects and/or deficiencies which do not meet the specifications set forth in the Agreement.

12.5. Contractor shall be responsible for filing, processing and collecting all damage claims.

12.6. Defects and/or deficiencies properly noted in writing to the Contractor before expiration of the warranty period will be fully covered regardless of such subsequent expiration. In the case of emergency, repairs and/or replacement may be made without notice being given to the Contractor, if determined by the District that delay would cause certain loss or damage. The Contractor shall pay the cost of these emergency repairs and/or replacements.

13. **Independent Contractor.** Contractor shall provide the Services under this Agreement as an independent contractor of the District. As such, Contractor shall have the right to determine how and by whom the Services will be provided and the right to provide the Services free from the direction and control of the District, subject to and consistent with the terms and conditions of this Agreement.

13.1. Contractor shall be exclusively responsible for: (a) all compensation, employment tax withholdings and payments, and all fringe benefits for its employees (if any) in full compliance with all applicable federal, state and local laws; (b) all insurance coverages and benefits for its employees (if any) in full compliance with all applicable federal, state and local laws, including but not limited to pension or retirement benefits, workers' compensation, unemployment compensation, and Social Security benefits; and (c) all payments to its contractors and subcontractors for goods and/or services directly or indirectly related to this Agreement.

13.2. Nothing in this Agreement shall be construed as creating a single enterprise, partnership, joint venture or employer-employee relationship between Contractor and the District. Contractor is not a partner, agent or representative of the District and shall not represent itself to be a partner, agent or representative of the District. The District is not a partner, agent or representative of Contractor and shall not represent itself to be a partner, agent or representative of Contractor.

13.3. Contractor shall not attempt or purport to extend the faith and credit of the District to any third party, person or entity. Contractor acknowledges and agrees that it has no authority to enter into any contract with a third party that would bind or in any way obligate the District. The District shall not attempt or purport to extend the faith and credit of Contractor to any third party, person or entity. The District acknowledges and agrees that it has no authority to enter into any contract with a third party that would bind or in any way obligate Contractor.

14. **Equal Opportunity.** It is agreed that no otherwise qualified Contractor shall be excluded from participating in, be denied the benefits of, or be subject to discrimination, including harassment, under any provision of this Agreement on the basis of race; creed; color; national origin; age; sex; pregnancy; physical recovery from childbirth or a related condition; sexual orientation; marital status; veteran status; religion; genetic information; gender expression; gender identity; ancestry; or disability.

15. **Conflict of Interest.** Contractor avers to their knowledge of no employee of the District having any personal or beneficial interest whatsoever in the service or property described in this Agreement. Contractor has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of the Contractor's Services and Contractor shall not employ any person having such known interest.

16. **Invoicing.** The District utilizes an online vendor portal to collect, validate, and manage vendor information, including but not limited to tax ID verification, sanction monitoring, receipt of W9 and other required forms. Prior to the issuance of a purchase order or payment, the Contractor will be required to complete the online registration process through the online vendor portal, which shall include the Contractor providing all required documentation, and receiving approval of the submission of all documentation, including but not limited to, TIN and bank account verification.

16.1. Invoices for Services provided shall be submitted directly to the District's accounts payable department within thirty (30) days of completion of Services. Invoices for such Services shall include (a) date on which Services were provided, (b) the District Location for which the Service were provided, (c) details of Products delivered, (d) and purchase order number. All invoices must be submitted within 30 days of fiscal year end June 30 and may not include items received by the District outside of the fiscal year July 1 – June 30.

16.2. Invoices received from the Contractor pursuant to this Agreement will be reviewed and approved by the District's representative, indicating that services have been rendered in

conformity with the Agreement and then will be sent to the Finance Department for payment. Payment for Services not approved by the District in writing, shall not be considered valid and the District will not be responsible for covering associated costs. Invoices will generally be paid within thirty (30) days following the District representative's approval.

16.3. Invoices which do not conform with the agreement will be paid thirty (30) days from receipt of a revised and corrected invoice.

16.4. Invoices shall be sent to ap@psdschools.org.

16.5. The District is exempt from federal and state taxes under Colorado Tax Exempt Number 98-03335.

16.6. If the contract results in the right to use an asset, the Contractor shall provide the District, if requested, documentation necessary to facilitate the District's compliance with the Governmental Accounting Standards Board ("GASB") issued GASB Statement No. 87, Leases.

17. **Insurance.** Contractor shall procure and maintain the required insurance specified below for the duration of this Agreement, which insurance shall be written for not less than the amounts specified or greater if required by law. Specified coverages and amounts may be provided by a combination of a primary policy plus an umbrella or following form excess policy. If not otherwise required by law, lower amounts may be acceptable upon review and written approval by the District's Director of Records and Risk Management. All insurance shall be with a carrier licensed in the state of Colorado and shall have a minimum A.M. Best rating of A- VII. Contractor shall furnish the District's Director of Records and Risk Management with certificates of the required insurance prior to the District's approval and signing of this Agreement, and with renewal certificates prior to the expiration of any required insurance that expires during the term of this Agreement. Certificates of Insurance and all communication regarding insurance shall be sent to:

    Poudre School District
    Attention: Risk Management
    Email: risk@psdschools.org
    2407 Laporte Ave
    Ft. Collins, CO 80521

Any insurance and/or self-insurance carried by the District is excess of the coverage extended to the District by Contractor. Contractor shall provide at least thirty (30) days' advance written notice to the District prior to cancellation, change of coverage, or non-renewal. The insurance requirements specified in this section 16 shall not reduce the indemnification liability that Contractor has assumed in section 17.

Commercial General Liability

Minimum Limits

a. Each Occurrence Bodily Injury & Property Damage $2,000,000
b. General Aggregate $3,000,000
c. Products/Completed Operations Aggregate $2,000,000
d. Personal/Advertising Injury $2,000,000
e. Coverage must be written on an "occurrence" basis.
f. Poudre School District R-1 and its elected officials, employees, agents, and volunteers shall be named as an additional insured or covered as an additional insured by way of a blanket endorsement and shall be insured to the full limits of liability purchased by the Provider even if those limits of liability are in excess of those required by this Agreement.

Technology Errors and Omissions Liability (Professional Liability, including Network Security and Privacy Liability)

Minimum Limits

a. Per Loss $1,000,000
b. Aggregate $3,000,000
c. Liability extends for a period of three (3) years beginning at the time work under this Agreement is completed. Provider shall maintain continuous coverage, as required by the Agreement, for this period.

The insurance shall provide coverage for:

a. Liability arising from theft, dissemination and/or use of confidential information (defined term including but not limited to bank account, credit card account, personal information such as name, address, social security numbers, etc. information) stored or transmitted in electronic form.
b. Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party to gain access to Provider's services including denial of service, unless caused by a mechanical or electrical failure.
c. Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a District or third person's computer, computer system, network, or similar computer related property and the data, software, and programs thereon.
d. Poudre School District R-1, its elected officials, employees, agents, and volunteers, the contractor, and subcontractors, shall be named insureds under the policy.

Crime Coverage (for agreements allowing privileged access to network systems, valuable property or sensitive data)

Minimum Limit

a. Per Loss $1,000,000

The policy shall include:

a. Coverage for all directors, officers, agents, and employees of the Provider.

b. Employee dishonesty, forgery and alteration, monies and securities, and computer (cyber) crime.
c. Extended theft and mysterious disappearance.
d. The policy shall not contain a condition requiring an arrest and conviction.
e. Policy must be endorsed to cover Third Party Fidelity and include Poudre School District R-1 as a Loss Payee.

Workers' Compensation and Employers' Liability

Minimum Limits

a. State of Colorado Statutory
b. Employer's Liability — $100,000 Each Accident; $500,000 Disease – Policy Limit; $100,000 Disease – Each Employee
c. Waiver of subrogation in favor of Poudre School District R-1.
d. This requirement shall not apply if Contractor is exempt under the Colorado Workers' Compensation Act and if Provider has a current Workers' Compensation Coverage Rejection on file with the Colorado Department of Labor and Employment, Division of Worker's Compensation.

18. **Indemnification.** The Contractor shall indemnify and hold harmless the District and the District's Board members, employees, representatives and agents from and against any and all liability arising from any suit, action, third party claims, grievance, or proceeding, including all attorneys' fees, costs and expenses, incurred as a result of any negligent or intentional act or omission by Contractor, or its employees, agents, Subcontractors, or assignees related to the terms of this Agreement and any Services provided under this Agreement.

19. **Governmental Immunity.** It is specifically understood and agreed that nothing contained in this Agreement shall be construed as an express or implied waiver by the District of any of the immunities, rights, benefits, protections, or other provisions of the Colorado Governmental Immunity Act, C.R.S. §§ 24-10-101 *et seq*, as now or hereafter amended.

20. **Remedies.** If Contractor fails to comply with any of the foregoing requirements at any time during or after the term of the Contract the District may, as applicable, terminate the Contract and/or disqualify Contractor from future contracts and subcontracts with the District.

21. **Notices and Communications.** All notices and communications required or permitted under this Agreement shall be in writing and shall be: (a) sent via certified mail, return receipt requested and postage prepaid, to the address of the other party set forth below; or (b) sent via e-mail to the other party via the e-mail address set forth below.

Poudre School District R-1
Attn: Tracy Stibitz
2407 LaPorte Avenue
Fort Collins, CO 80521
E-mail: tstibitz@psdschools.org

EAP Expert Inc.
Attn: Chris Coleman
7111 Syntex Drive Suite 100
Mississauga, Ontario L5N 8C3
Email: ccoleman@eapexpert.com

22. **General Provisions.**

22.1. **No Assignment.** The Contractor shall not assign this Agreement or any of its rights, interests or obligations under this Agreement without the prior written consent of the District, which consent may be withheld for any reason or no reason as determined by the District in its sole discretion.

22.2. **No Waiver.** The parties agree that no assent or waiver, express or implied, to any breach of any one or more of the covenants of this Agreement shall be construed as or deemed to be an assent to or a waiver of any subsequent breach.

22.3. **Press Contacts/News Releases.** The Contractor shall not initiate any press, media, or social media contact nor respond to press, media or social media requests regarding this Agreement and/or any related matters concerning the District without the prior written approval of the District's Executive Director of Communications or designee.

22.4. **Survival of Certain Contract Terms.** Notwithstanding anything herein to the contrary, the parties understand and agree that all terms and conditions of this Agreement and the exhibits and/or attachments hereto which may require continued performance, compliance, or effect beyond the termination date of the Agreement shall survive such termination date and shall be enforceable by the District as provided herein in the event of such failure to perform or to comply by the Contractor.

22.5. **Amendment or Modification.** No amendment or modification of this Agreement shall be valid unless set forth in writing and executed by the District and the Contractor through written amendments to the Agreement, in the same manner and with the same formality as was done for this Agreement.

22.6. **Governing Law and Venue.** All issues regarding the formation, performance and/or legal enforcement of the Contract shall be governed by and construed in accordance with the laws of the State of Colorado. Venue for the resolution of any disputes arising out of or relating to the Contract shall be in Larimer County, Colorado.

22.7. **No Third-Party Beneficiary.** Enforcement of the terms and conditions of this Agreement, and all rights of action relating to such enforcement, shall be strictly reserved to the District and the Contractor. Nothing contained in this Agreement shall give or allow any claim or right of action whatsoever by any third person other than the District or the Contractor. It is the express intent of the parties that any third person receiving services or benefits pursuant to this Agreement shall be deemed an incidental beneficiary only.

22.8. **Attorney Fees and Costs.** In the event it becomes necessary for either party to institute litigation to enforce any provision of this Agreement, the substantially prevailing party in such litigation shall receive, as part of any judgment or award entered, its reasonable attorney fees and costs, including expert witness fees.

22.9. **Binding Arbitration Prohibited.** The District does not agree to binding arbitration by any extra-judicial body or person. Any provision to the contrary is null and void.

22.10. **Binding Effect.** This Agreement shall be binding upon and inure to the benefit of the parties and their respective heirs, legal representatives, successors and permitted assigns.

22.11. **Headings.** The headings used in this Agreement are for convenience only and shall have no effect upon the construction or interpretation of this Agreement.

22.12. **Conflict of Terms.** In the event of any conflict of terms found between this Agreement, any incorporated exhibits, any other terms and conditions, end user license agreements or privacy policies, the terms of this Agreement shall prevail.

22.13. **Entire Agreement.** This Agreement constitutes the entire Agreement of the parties regarding the subject matter addressed herein and supersedes all prior Agreements, whether oral or written, pertaining to said subject matter.

22.14. **Signatures.** This Agreement may be executed and delivered via portable document format (pdf), and the pdf signature of any party shall be considered valid, binding, effective and an original for all purposes. This Agreement may be signed in counterparts, and each counterpart shall be deemed an original, and all the counterparts taken as a whole shall constitute one and the same instrument.

22.15. **Warranty of Authority.** The individuals signing below represent and warrant that they have the authority to execute this Agreement on behalf of their respective organizations and bind their respective organizations to the terms of this Agreement.

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, the District and the Contractor have signed this Agreement as of the date first set forth above.

EAP Expert Inc.

By: Chris Coleman

Name: Chris Coleman
Title: SVP, Global Solutions

POUDRE SCHOOL DISTRICT R-1

By: R David Montoya
R David Montoya (May 18, 2023 12:44 MDT)
R. David Montoya
Executive Director of Finance

By: Barbara Fisher
Barbara Fisher (May 18, 2023 10:43 MDT)

Barbara Fisher
Employee Assistance Services Manager

Exhibit A

POUDRE SCHOOL DISTRICT R-1

REQUEST FOR PROPOSALS

EAP & MANAGED CARE SOFTWARE

RFP 23-690-001

PROPOSAL SCHEDULE

RFP Issued	**March 8, 2023**
Questions due	**March 16, 2023, 2:00 p.m. MT**
Q&A Issued (Tentative)	**March 17, 2023**
RFP Closing Date	**March 23, 2023, 2:00 p.m. MT**

TABLE OF CONTENTS

REQUEST FOR PROPOSALS
EAP & MANAGED CARE SOFTWARE
RFP 23-690-001

Poudre School District (the "District") is requesting electronic proposals from professional and qualified software developers ("Suppliers") for EAP & Managed Care Software as specified in this Request for Proposals ("RFP").

The District shall provide copies of this RFP to Suppliers through the electronic solicitation platform www.bidnetdirect.com where registered Suppliers are required to submit their electronic RFP response along with the first and last name, telephone number and e-mail address of the employee within their organization who will be designated as the District's primary contact with respect to this RFP and their Supplier's response thereto.

Questions regarding this RFP must be in writing and shall only be directed to the District via the BidNet platform any time after the issuance of this RFP through and including 2:00 p.m. MT on March 16, 2023. Questions received after the date/time and/or not submitted electronically through the BidNet platform may not be addressed. Each question submitted, as well as the District's response thereto, shall be provided in a questions and answers document via www.bidnetdirect.com. Note: Every question must be submitted individually. Multiple questions per entry will not be answered.

The District will only accept and consider electronically submitted proposals from Suppliers, which must be submitted and received in the www.bidnetdirect.com electronic solicitation portal on or before 2:00 p.m. MT on March 23, 2023 at which time the submission portal will close, and no further submissions be allowed or considered. It is the sole responsibility of the Supplier to see that the proposals are submitted through the BidNet portal by the submission deadline.

Sales Prohibited/Conflict of Interest: No officer, employee, or member of the School Board, shall have a financial interest in the sale to the school district of any real or personal property, equipment, material, supplies or services where such officer or employee exercises directly or indirectly any decision-making authority concerning such sale or any supervisory authority over the services to be rendered. This rule also applies to subcontracts with the School District. Soliciting or accepting any gift, gratuity favor, entertainment, kickback or any items of monetary value from any person who has or is seeking to do business with the District is prohibited.

Collusive or sham proposals: Any proposal deemed to be collusive or a sham proposal will be rejected and reported to authorities as such. Your authorized signature on this proposal assures that such proposal is genuine and is not a collusive or sham proposal.

The District reserves the right to reject any and all proposals and to waive any irregularities or informalities.

Sincerely,
Rob Turf
Strategic Sourcing Supervisor
lturf@psdschools.org

REQUEST FOR PROPOSALS
EAP & MANAGED CARE SOFTWARE
RFP 23-690-001

BACKGROUND

Poudre School District is a high-performing district, covering more than 1,800 square miles in northern Colorado with diverse school settings. The District's instructional program is centered around District Ends, under the Policy Governance model, developed to support a comprehensive curriculum.

While more than 70% of the District's families choose to send their children to their neighborhood school, the District does support school choice and offers a wide spectrum of educational programs to fit any child's needs. Program options include International Baccalaureate, Core Knowledge, Bilingual/Dual Language Immersion, Hybrid/Online, Expeditionary Learning, Science, Technology, Engineering and Math (STEM) along with extra-curriculars and athletics. The District has two LEED certified school buildings and over 30 Energy Star awards and supports operational sustainability in all areas of work.
Our Schools:

- 31 elementary schools
- 10 middle schools
- 4 comprehensive high schools
- 2 additional combined middle/high schools
- 6 option (100% choice) schools
- 3 alternative high schools
- 1 online school
- 1 hybrid school (classes on campus and online learning)
- 5 charter schools

The District is fully accredited by the Colorado Department of Education Accreditation and Accountability Unit and is subject to periodic monitoring to ensure continued compliance with accreditation standards.

1.0 GENERAL CONDITIONS

1.1 Information and materials submitted in response to this solicitation may be considered public records subject to disclosure under the Colorado Open Records Act ("CORA"), C.R.S. §§ 24-72-200.1 to -205.5. Information and materials that Supplier believes are confidential and not subject to disclosure under CORA must be submitted separately with a citation to the section of CORA and any other relevant law under which Supplier believes they are confidential. The District, not Supplier, shall determine whether information and materials so identified will be withheld as confidential, but will inform Supplier in advance of disclosure to give it an opportunity to take legal action to protect its interests vis-à-vis the party making the CORA request.

1.2 This is a solicitation for an offer and is not an offer to contract for goods or services.

1.3 Supplier must provide all requested information. Failure to do so may result in rejection of the proposal at the option of the District.

1.4 Proposals must meet or exceed specifications contained in this document.

1.5 The District is exempt from city, county, state, and federal sales/excise taxes. Tax exempt certificates will be issued upon request.

1.6 Submission of a proposal is deemed as acceptance of all terms, conditions and specifications contained in the District's solicitation package initially provided to the Supplier. Any proposed modification must be accepted in writing by the District prior to award of the contract.

1.7 Each Supplier, its employees, representatives, and subcontractors, agrees to abide by all applicable federal, state, and local codes, laws, rules and regulations.

1.8 The successful Supplier shall furnish all supplies, which conform to all applicable safety codes and regulations.

1.9 Contact with District personnel regarding this RFP, other than inquiries to the specific Procurement Agent identified in this document, may be grounds for elimination from the selection process.

1.10 Proposals shall contain a signature of an authorized representative in the space provided on the Proposal Certification Form. Failure to properly sign the proposal may invalidate same and it may not be considered for award.

1.11 The accuracy of the solicitation is the sole responsibility of the Supplier. No changes in the proposal shall be allowed after the submission deadline, except when the Supplier can show clear and convincing evidence that an unintentional factual mistake was made, including the nature of the mistake.

1.12 Supplier must provide proof of insurance that meets the insurance requirements stated in Section 6.0 of this document.

1.13 Health and Safety Standards**.** The Supplier shall have and maintain a set of protocols and guidelines to meet evolving health and safety requirements and implement any applicable communicable disease protocols, which must follow guidance and orders from state and/or local public health officials and be no less strict than the District's protocols.

1.13.1 Supplier shall ensure all individuals providing Services under this agreement for the Supplier wear appropriate personal protective equipment as designated in this section 1.13, at all times while on District property.

1.13.2 If the District is directed, or the District determines to limit or restrict access to any or all of its facilities or District Location due to a public health or safety concern, the District may, at its discretion, temporarily delay or stop Supplier's services, with or without prior notice.

1.14 The successful Supplier is not permitted to transfer any interest in the project whether by assignment or otherwise, without prior written consent of the District's Strategic Sourcing Department.

1.15 Suppliers are required to complete the Reference Form included in this solicitation as described.

1.16 Supplier must note in the solicitation response any intent to use subcontractors. The subcontractor's name, address, phone number and three client references, along with the type of work to be performed must be included. Use of subcontractors may be considered as a factor in the District's evaluation process. If the Supplier fails to notify the District of its intent to use subcontractors in the proposal submittal, the proposal may be considered a void offer. Subcontractors will be allowed only by written permission of the District. The Supplier agrees that it is fully responsible to the District for the acts or omissions of its subcontractors, or any persons employed by them, in the same way as it is for the acts and omissions of persons directly employed by the Supplier. Nothing contained in the contract, or any subcontract shall create any contractual relation between any subcontractor and the District.

1.17 The District reserves the right to reject any and all proposals or any part thereof, to waive any formalities, and further, to award the proposal to the responsible Supplier as deemed in the best interest of the District.

1.18 There is no expressed or implied obligation for the District to reimburse responding Suppliers for any expenses incurred in preparing proposals in response to this request.

1.19 Responses to this solicitation will be independently evaluated by an evaluation committee to be established for such purpose.

1.20 Proposals submitted will be evaluated using pre-determined objective rating criteria. Those that are clearly non-responsive to the stated requirements may be eliminated prior to the evaluation. Prior to proposal submission, Supplier are encouraged to check the BidNet website to ensure additional requirements are incorporated into its submissions.

1.21 The District reserves the right to negotiate further with one or more Suppliers or to request additional information. The District may make such inquiries and conduct such investigations as it deems necessary to determine the qualifications and ability of the Supplier to provide the services called for under the RFP and/or represented in the Supplier's response. Suppliers shall timely provide information to the District in connection with such inquiries and investigations. Suppliers may be asked to give presentations to the District regarding their proposals.

1.22 Should the District determine, in its sole discretion, that only one Supplier is fully qualified or that one Supplier is clearly more highly qualified than the others under consideration, a contract may be negotiated and awarded to that Supplier.

1.23 The District intends for the contract to commence upon complete execution of a successfully negotiated agreement and continue in full force and effect through and including June 30, 2024, unless earlier terminated by the District as provided in Section 1.27 below. The final award and contract start date is contingent upon a successfully negotiated and fully executed contract between the District and the recommended Supplier. The intended date is provided for planning purposes only.

1.24 For services provided, and at the option of the District, the agreement may be extended beyond the first term for up to four (4) additional one-year terms, subject to the parties' negotiation of mutually agreed upon amendments to the Agreement for each one (1) year term. Pricing will remain fixed and firm for the initial term and all extensions of the agreement.

1.25 Notwithstanding any other term or provision of this Request for Proposal, the District's obligations hereunder are expressly subject to its budgeting and appropriation of sufficient funds for each fiscal year (July 1 - June 30) a contract is in effect. In no event shall the District's obligations in a contract constitute a multiple-fiscal year direct or indirect debt or other financial obligation under Article X, Section 20(4)(b) of the Colorado Constitution.

1.26 Notwithstanding the other provisions of this RFP, either party may terminate this Agreement at any time in that party's sole discretion for any reason, with or without cause, by providing the other party with thirty (30) days' advance written notice. In the event of such termination: (a) the District shall pay Supplier for all Services performed under and in accordance with this Agreement up to the date of termination; and (b) Supplier shall reimburse the District for all payments made in excess of Services performed up to the date of termination.

1.27 The successful Supplier will be required to enter into and sign a formal agreement with the District. The agreement language will control over any language contained within this RFP that conflicts with the signed and fully executed agreement.

1.28 In the case of conflicts between the RFP and any referenced proposal documents, the more stringent requirements shall govern. In all cases, the Supplier is responsible for notifying the District of the conflict.

1.29 Supplier warrants that it has full power and authority to grant the rights of its license agreement to the District with respect to its program without consent of any other person or entity. Supplier also warrants that neither the performance of the services by its company, nor the license to and use by the District of its company's product and documentation will in any way constitute an infringement nor other violation of any United States issued copyright, trade secret, trademark, patent, invention, propriety information, non-disclosure, or other right of any third party.

1.30 Access to District Server. If access to any District server is necessary for the functionality of the Contractor's services. Upon written approval by the Executive Director of Information Technology or designee, the District grants the Contractor limited access to the District server for the sole purpose of providing Services

1.30.1 The Contractor agrees to protect the confidentiality, integrity and availability of all electronic District or student information at all times.

1.30.2 The Contractor agrees to take proper steps to ensure the security of the device in which they connect to the District's systems remotely. The Contractor agrees not to copy information accessed remotely to local devices and or portable devices. Printing information is not permitted unless specific authorization has been granted.

1.30.3 The Contractor shall not share passwords, codes, credentials or user accounts with others.

1.30.4 The Contractor shall have a valid and up-to-date antivirus agent installed to ensure protection against malware and viruses upon connection to the District network.

1.30.5 The Contractor acknowledges that if the District determines in its discretion that remote access has been compromised by unauthorized parties, or that remote access has been misused, the Contractor's access will be disabled or terminated immediately

1.31 The Supplier shall provide the services as an independent contractor of the District. As such, the Supplier shall have the right to determine how and by whom

the services will be provided, subject to and consistent with the terms and conditions of this solicitation.

1.31.1 The Supplier shall be exclusively responsible for: (a) all compensation, employment tax withholdings and payments, and all fringe benefits for its employees in full compliance with all applicable federal, state and local laws; (b) all insurance coverages and benefits for its employees in full compliance with all applicable federal, state and local laws, including but not limited to pension or retirement benefits, workers' compensation, unemployment compensation, and Social Security benefits; and (c) all payments to its suppliers and subcontractors for goods and/or services directly or indirectly related to this solicitation.

1.31.2 Nothing in this solicitation or as a result of this solicitation shall be construed as creating a single enterprise, partnership, joint venture or employer-employee relationship between a future Supplier and the District. The future Supplier will not be considered a partner, agent or representative of the District and will not represent itself to be a partner, agent or representative of the District. The District is not a partner, agent or representative of any future Supplier and shall not represent itself to be a partner, agent or representative of the Supplier.

1.32 Qualifications of Supplier

1.32.1 The District may make such reasonable investigations as deemed proper and necessary to determine the ability of the Supplier to perform the work and the Supplier shall furnish to the District all such information and data for this purpose as may be requested.

1.32.2 The District further reserves the right to reject any proposal if the evidence submitted by, or investigations of, such Supplier fails to satisfy the District that such Supplier is properly qualified to carry out the obligations of the contract and to complete the work/furnish the item(s) contemplated therein.

1.33 Miscellaneous

1.33.1 Once the evaluation is complete and the Intent to Award has been issued to the recommended Supplier, the recommended Supplier will work with the District's Contract Administrator to successfully negotiate an agreement.

1.33.2 Governing Law and Venue. All issues regarding the formation, performance and/or legal enforcement of the Contract shall be governed by and construed in accordance with the laws of the State of Colorado. Venue for the resolution of any disputes arising out of or relating to the Contract shall be in Larimer County, Colorado.

1.33.3 Equal Opportunity. It is agreed that no otherwise qualified Supplier shall be excluded from participating in, be denied the benefits of, or be subject to discrimination, including harassment, under any provision of this Agreement on the basis of race; creed; color; national origin; age; sex; pregnancy; physical recovery from childbirth or a related condition; sexual orientation; marital status; veteran status; religion; genetic information; gender expression; gender identity; ancestry; or disability.

1.33.4 Appeal of Award. The Supplier may appeal the award by submitting, in writing, a request for re-consideration to the District's Executive Director of Finance within seventy-two (72) hours after the receipt of the notice of award.

1.33.5 In the event the awarded Supplier defaults on its contract or the contract is terminated for cause due to performance, the District reserves the right to re-procure the Services from the next lowest Supplier or from other sources during the remaining term of the terminated/defaulted contract. Under this arrangement, the District shall charge the awarded Supplier any differences between its price and the price to be paid to the next lowest Supplier, as well as, any costs associated with the re-solicitation effort which resulted from such default or termination.

1.33.6 This solicitation does not commit the District to award a contract or to pay any costs incurred in the preparation of a proposal or to procure a contract for the services. The District reserves the right to accept or reject any or all proposals received as a result of this request or to cancel in part or in its entirety this solicitation if it is deemed to be in the best interest of the District. The District reserves the right to accept any portion of the proposal, or the entire proposal as deemed in the best interest of the District.

1.33.7 For the purposes of solicitation evaluation, Supplier must indicate any variances to the specifications and terms and conditions, no matter how slight. If variations are not stated in the Supplier's response, it shall be construed that the proposal fully complies with the specifications and terms and conditions. Notwithstanding the above, it is hereby agreed and understood that the District reserves the right to reject these variations if they individually or, as a whole, do not meet the standards established in the specifications. Modifications to this RFP document and/or exhibit will not be considered valid and may be cause for disqualification. Award of this solicitation does not constitute the District's acceptance of the Supplier's proposed variations.

1.33.8 Sustainability. The District is committed to be a responsible steward of our natural resources and believes that public education should provide leadership in developing an ethic of sustainability in all its practices. In the District we have both Energy Conservation and Waste Management

policies and espouse these values, making environmental stewardship and integral part of the physical plant operation.

1.34 Cooperative Purchasing Efforts. Poudre School District is a member of, or affiliated with, several regional professional procurement organizations within Colorado and Wyoming. These organizations are comprised of governmental purchasing agents, or agency representatives responsible for the purchasing function.

1.34.1 These organizations include:

1.34.1.1 Colorado Educational Purchasing Council (CEPC) - A cooperative purchasing organization comprised of purchasing agents/buyers representing all Colorado public school districts.

1.34.1.2 Multiple Assembly of Procurement Officials (MAPO) - A cooperative purchasing organization comprised of procurement representatives from state, county, municipal, governments, special districts or school districts along the front range of the Rocky Mountains in Colorado.

1.34.1.3 Rocky Mountain Governmental Purchasing Association (RMGPA) - A chapter member of the National Institute of Governmental Purchasing (NIGP), consisting of public procurement professionals and their representative agencies which include approximately 100 state, county, and municipal governments; school districts and higher education; and other special districts.

1.34.2 Members of these organizations, at their discretion, may request use of the contracts or awards that result from this solicitation. Each governmental entity which uses a contract(s) resulting from this solicitation would establish its own contract, issue its own orders, schedule deliveries, be invoiced individually, make its own payments, and issue its own exemption certificates as required by the Supplier. It is understood and agreed that Poudre School District is not a legally binding party to any contractual agreement made between another governmental entity and the Supplier as a result of this solicitation. The District shall not be liable for any costs or damages incurred by any other entity. Usage by any other entity shall not have a negative impact on the District in the current term or in any future terms.

2.0 SCOPE OF WORK AND REQUIREMENTS

The District is requesting electronic proposals from professional and qualified Suppliers to provide the following software that includes but is not limited the requirements in this RFP and EXHIBIT A.

2.1 Minimum Requirements. Describe how your software meets or exceeds the following requirements:

2.1.1 Ability to create and customize intake forms (with different access controls) to meet District project needs.

2.2 Added Value

2.2.1 Tell us about your integrations with other platforms, to include calendars (the District uses Google and Outlook calendars currently). While we are interested in all integration options, we would be most interested in Microsoft and Google integrations.

2.2.2 Tell us about your product's visual design and interface and how that impacts usability.

2.2.3 Tell us about your product's reporting tools. Can custom reports be created by users, or would that require your intervention?

2.2.4 Tell us about your product's licensing and access controls. Who can see what and how does that impact pricing?

2.2.5 Tell us about your product's data security. Where and how is the data generated by your product stored? What security measures are in place to minimize risk?

2.2.6 How do you support your product? What static resources and dynamic training options are available?

2.2.7 Describe the onboarding process you would use for the District and individual users within the District.

3.0 COST PROPOSAL

3.1 Provide a line-item cost proposal based on services provided. All costs shall include options for and outline all role-based permission options.

3.1.1 Cost of software

3.1.1.1 Cost per individual user

3.1.1.2 Cost per group of users

3.1.1.3 Cost for enterprise level of use

3.1.2 Annual cost of a maintenance contract, including phone and online support.

3.1.2.1 Year 1

3.1.2.2 Year 2-5

3.1.3 Cost of training

3.1.3.1 Indicate the number of days anticipated for on-site training.

3.1.3.2 Provide cost for onboarding

3.1.3.3 Provide cost for user trainings

3.1.4 Indicate the number of days for delivery of software and services after receipt of a signed purchase order.

4.0 EVALUATION AND AWARD OF CONTRACT

4.1 Proposals will be evaluated on the following criteria. A cumulative point system will be used. Award shall be made to the most responsive and responsible Supplier meeting the specifications and deemed the most advantageous to the District.

Criteria	Points
System design and features	30
Ease of use for staff accessing the system	20
Ease of deployment and import of existing data	20
Cost Proposal	10
Timeframe, Support and Maintenance, Training	10
References from other school districts (Colorado preferred)	10

4.2 The District may at its discretion, elect to interview one (1) or more Suppliers that submit a proposal, but is not required to do so. The interview may either be conducted via a virtual platform or in person at a Poudre School District location (Ft. Collins, Colorado).

4.2.1 The determination of whether to conduct interviews with the finalist(s) shall be made by the District based solely on its determination of whether interviews would be helpful in evaluating the proposals.

4.2.2 Any Supplier selected for an interview will be expected to make an introductory presentation followed by a demonstration and question and answer period. The District will not reimburse any travel related or other expenses related to an interview.

4.3 Once the evaluation is complete and the Intent to Award has been issued to the recommended Supplier, the recommended Supplier will work with the District's Contract Administrator to successfully negotiate a District agreement.

--Intentionally left blank--

References are mandatory – List three (3), non-Poudre School District, K-12 education market references, for which your company has completed similar services for projects of similar scope. The District may contact these references during the evaluation process. **Client reference letters shall be included in addition to the reference information listed below.**

5.1 Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

_____

5.2 Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

_____

5.3 Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

_____

6.0 INSURANCE

Supplier shall procure and maintain the required insurance specified below for the duration of this Agreement, which insurance shall be written for not less than the amounts specified or greater if required by law. The District's receipt of a Certificate of Insurance from the Provider with limits and or coverages that do not meet the requirements does not waive the requirements and the Provider shall still be responsible for the limits and coverages stated in this Agreement. Specified coverages and amounts may be provided by a combination of a primary policy plus an umbrella or following form excess policy. All insurance shall be with a carrier licensed in the state of Colorado and shall have a minimum A.M. Best rating of A-VII. Provider shall furnish the District's Director of Records and Risk Management with certificates of the required insurance prior to the District's approval and signing of this Agreement, and with renewal certificates prior to the expiration of any required insurance that expires during the term of this Agreement. Memorandums of Insurance will not be accepted. Certificates of Insurance and all communication regarding insurance shall be sent to:

Poudre School District
Attention: Risk Management
2407 Laporte Ave
Ft. Collins, CO 80521
Please Email Certificate to: COI@psdschools.org

Any insurance and/or self-insurance carried by the District is excess of the coverage extended to the District by Supplier. Supplier shall provide at least thirty (30) days' advance written notice to the District prior to cancellation, change of coverage, or non-renewal. The insurance requirements specified in this section 6.0 shall not reduce the indemnification liability that Supplier has assumed in section 6.1.

Commercial General Liability

Minimum Limits

- Each Occurrence Bodily Injury & Property Damage $2,000,000
- General Aggregate $3,000,000
- Products/Completed Operations Aggregate $2,000,000
- Personal/Advertising Injury $2,000,000
- Coverage must be written on an "occurrence" basis.
- Poudre School District R-1 and its elected officials, employees, agents, and volunteers shall be named as an additional insured or covered as an additional insured by way of a blanket endorsement and shall be insured to the full limits of liability purchased by the Provider even if those limits of liability are in excess of those required by this Agreement.

Technology Errors and Omissions Liability (Professional Liability, including Network Security and Privacy Liability)

Minimum Limits

- Per Loss $1,000,000
- Aggregate $3,000,000
- Liability extends for a period of three (3) years beginning at the time work under this Agreement is completed. Provider shall maintain continuous coverage, as required by the Agreement, for this period.

The insurance shall provide coverage for:

- Liability arising from theft, dissemination and/or use of confidential information (defined term including but not limited to bank account, credit card account, personal information such as name, address, social security numbers, etc. information) stored or transmitted in electronic form.
- Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party to gain access to Provider's services including denial of service, unless caused by a mechanical or electrical failure.
- Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a District or third person's computer, computer system, network, or similar computer related property and the data, software, and programs thereon.
- Poudre School District R-1, its elected officials, employees, agents, and volunteers, the contractor, and subcontractors, shall be named insureds under the policy.

Crime Coverage (for agreements allowing privileged access to network systems, valuable property or sensitive data)

Minimum Limit Per Loss $1,000,000

The policy shall include:

- Coverage for all directors, officers, agents, and employees of the Provider.
- Employee dishonesty, forgery and alteration, monies and securities, and computer (cyber) crime.
- Extended theft and mysterious disappearance.
- The policy shall not contain a condition requiring an arrest and conviction.
- Policy must be endorsed to cover Third Party Fidelity and include Poudre School District R-1 as a Loss Payee.

Workers' Compensation and Employers' Liability

If Provider is exempt under the Colorado Workers' Compensation Act, this requirement will be waived if proof a current Workers' Compensation Coverage Rejection is on file with the Colorado Department of Labor and Employment, Division of Worker's Compensation and a copy is submitted to the District.

Minimum Limits

- State of Colorado Statutory
- Employer's Liability $100,000 Each Accident
  $500,000 Disease – Policy Limit
  $100,000 Disease – Each Employee

- Waiver of subrogation in favor of Poudre School District R-1.

6.1 Supplier shall indemnify and hold harmless the District and the District's Board members, employees, representatives and agents from and against any and all liability arising from any suit, action, grievance, charge or proceeding brought in connection with or related to Supplier's operations, provision of services and/or conduct of any of its employees, volunteers, agents or representatives. The indemnification and hold harmless obligation hereunder shall include all attorney fees, costs and expenses incurred by the District and/or the District's Board members, employees, representatives and/or agents in defense of said suits, actions, grievances, charges and/or proceedings. Nothing in this section or otherwise in this contract shall be construed in any way or applied in any manner as a compromise or waiver of the District's rights and protections under the Colorado Constitution or the Colorado Governmental Immunity Act.

7.0 MODEL FORMAT OF PROPOSAL

To simplify the review process and obtain the maximum degree of comparability, proposals ***must*** be organized in the manner specified below.

7.1 Title Page

7.1.1 Show the solicitation subject, the name of the proposing Supplier, local address, telephone number, name of the contact person and the date.

7.2 Table of Contents

7.2.1 Include a clear identification of the material by section and by page number.

7.3 Letter of Transmittal – Limit to three (3) pages.

7.3.1 Briefly state the Supplier's understanding of the work to be done and describe in detail the Supplier's ability to fulfil the scope meet the deadlines requested by the District.

7.3.2 State the names of the persons who will be authorized to make representations for the Supplier, their titles, addresses, phone numbers, and email addresses.

7.4 Supplier's Approach

7.4.1 Submit a work plan to accomplish the scope and questions defined in the Scope of Work and Requirements (Section 2.0).

7.4.2 Responses should be formatted in order, labeled as such, and follow the exact sequence of the solicitation Scope of Work section.

7.4.3 Clarification questions and requests for information throughout the solicitation shall be clearly labeled with the section and subsection number and include the Supplier's response/information.

7.4.4 Any and all assumptions shall be clearly stated in the Supplier's response. Assumptions that are not clearly indicated, but raised later in the award process, may be grounds for the Supplier's response to be considered non-responsive.

7.5 References

7.5.1 Submit completed reference form in Section 5.0.

7.6 Cost Proposal

7.6.1 Provide a cost proposal as identified in Section 3.0. Cost proposal and supporting documentation shall be clearly labeled "RFP 23-690-001."

7.7 Proposal Certification Form

7.7.1 Submit the completed form in Section 8.0.

--Intentionally left blank--

Proposals must be submitted and received in BidNet's electronic solicitation portal on or before 2:00 p.m. MT on March 23, 2023.

The undersigned hereby affirms that:

- He/she is a duly authorized agent of the company issuing this proposal and that all information provided in the proposal is true and accurate.
- Supplier has read the conditions, including the insurance requirements and technical specifications, which were made available to the company in conjunction with this RFP, and fully understands and accepts these terms unless specific variations have been expressly requested in the response submitted by the Supplier. Requested variations will be reviewed by the District and approved on a case-by-case basis if deemed appropriate.
- The company will adhere to all terms and conditions and provide, at a minimum, all services as expressed in the solicitation and/or the company's proposal responding to the solicitation.
- The company meets or exceeds all of the required criteria as specified by this solicitation, or if not, has submitted a Justification for Consideration addressing any failure to meet the criteria.
- The company's proposal is being offered independently of any other Supplier and in full compliance with the terms specified in Sections 1 and 2 of the solicitation.
- The company will accept any awards made to it, contingent on contract negotiation, as a result of this solicitation for a minimum of ninety (90) calendar days following the date and time of the solicitation opening.

Company Name: _____

Signature of Agent: _____

Printed Name: _____

Title: _____

E-mail address: _____

Mailing address: _____

Telephone: _____

Contact Person: _____
(If different from Agent, include e-mail address and phone number)

NOTE: Proposals submitted without the signature of an authorized agent of the company may be considered non-responsive and ineligible for the award.

EXHIBIT A - EAS SOFTWARE RFP:
Specs for EAP and Managed Care software
2/28/2023

Client and clinical note Module

Provides fields for client demographics, HR information (position, location, date of hire, employee ID) and Benefit information

Customizable, Drop-down menus for

- Assessed Problem(s)
- Location
- Business Unit
- Who is the client (ee, spouse, child, other)
- "Referred by" source
- Health plan selection/who is covered
- Gender
- Marital status

Links to "related" cases for this client and covered family members

Ability to "manually relate" cases (e.g. when both parties are PSD EE's)

Ease of opening new cases – transfer of crucial information;

Ability to access to cases, documents, referrals, etc. across all cases for that individual.

Ability to change case number in clinical notes; scheduler; referral authorizations to move to the appropriate case as needed.

Ability to record, edit, and view all types of contacts with clients

Ability to create referral authorizations to EAS managed care network providers (integrated with Managed Care Provider Module)

Provide popup alerts for URs and authorization renewals

Maintain list of referrals per client across all cases

Ability to upload documents to client case

Interface with Workplace Consults and Auxiliary Services

Ability to edit a record when multiple users are viewing that record;

Access to view/edit contact notes is *not* time or date limited

Pop up warning of missing data/need to save/confirmation of "delete record"

Ability to assign a case to an EAS staff counselor

Mail merge capability

Customizable field naming

Organizational

Company/Organization management

Utilization figures (# EE's/# eligible individuals)

Dropdowns for

- Locations
- Business units

Scheduler

Centralized appointment scheduling that includes all EAS counselors on one screen

Ability to schedule appointments – that link to client note screen

Customizable for types of appointments

SMS/email reminders

Ability to search, cut/copy/paste, click-drag to move appointments

Ability to create, update and maintain recurring events

Ability to create, update and maintain events for all staff

Ability to report on scheduled events by date range and type
Options when manipulating recuring events

Workplace Consults and Auxiliary Services Modules Interface between WPC and AS
Tracks time allocations and contacts
Interfaces with client cases
Ability to upload documents
Customizable

Managed Care/Provider Network Module
Ability to add/view/maintain Provider Network participants
- Customizable demographic data fields
- Ability to define umbrella "group practices" AND providers within that organization
- dropdowns
- provider specialty checkboxes
- license/liability insurance renewal fields
- mail merge capability

Ability to upload documents to provider file
Interface with client referral screen; ability to create referrals
Flexibility in information recorded for providers
Searchable on any data field/using user defined criteria
Flexible reporting criteria
License and insurance expiration alerts
Mail merge capability
Customizable data fields and field names

Data management and reporting
Ability to report on various aspect of clinical contact, workplace consults, auxiliary services
Ability to convert existing EAS SQL queries to "like" data reports
Customizable ROI calculations
Customizable reports for client case information
Customizable reports for Managed Care Provider Networkdatabase

System Administration
Audit History (view/access user history)
User administration and password management
"Unlock records" feature (if needed, for multiple users to be in one case at the same time)
User security roles/levels
SQL query assistant (if database is SQL based) and printable code list (if appropriate)
Global messaging
Ability to set "default values" for defined data fields (city, state, hours/minutes of session, etc)

Misc.
Ability to convert data from Premier software
HIPAA compliant
Web-based; secure hosting
Ability to customize all database fields
User friendly
Unlimited Licenses
Support
Security – backups, monitoring, multifactor authentication
Spell Check
Reminders list

POUDRE SCHOOL DISTRICT R-1

REQUEST FOR PROPOSALS

EAP & MANAGED CARE SOFTWARE

RFP 23-690-001

PROPOSAL SCHEDULE

RFP Issued	**March 8, 2023**
Questions due	**March 21, 2023 ~~March 16, 2023~~, 2:00 p.m. MT**
Q&A Issued (Tentative)	**March 22 ,2023 ~~March 17, 2023~~**
RFP Closing Date	**March 28, 2023 ~~March 23, 2023~~, 2:00 p.m. MT**

TABLE OF CONTENTS

REQUEST FOR PROPOSALS
EAP & MANAGED CARE SOFTWARE
RFP 23-690-001

Poudre School District (the "District") is requesting electronic proposals from professional and qualified software developers ("Suppliers") for EAP & Managed Care Software as specified in this Request for Proposals ("RFP").

The District shall provide copies of this RFP to Suppliers through the electronic solicitation platform www.bidnetdirect.com where registered Suppliers are required to submit their electronic RFP response along with the first and last name, telephone number and e-mail address of the employee within their organization who will be designated as the District's primary contact with respect to this RFP and their Supplier's response thereto.

Questions regarding this RFP must be in writing and shall only be directed to the District via the BidNet platform any time after the issuance of this RFP through and including 2:00 p.m. MT on ~~March 16, 2023~~ March 21, 2023. Questions received after the date/time and/or not submitted electronically through the BidNet platform may not be addressed. Each question submitted, as well as the District's response thereto, shall be provided in a questions and answers document via www.bidnetdirect.com. Note: Every question must be submitted individually. Multiple questions per entry will not be answered.

The District will only accept and consider electronically submitted proposals from Suppliers, which must be submitted and received in the www.bidnetdirect.com electronic solicitation portal on or before 2:00 p.m. MT on ~~March 23~~, March 28, 2023 at which time the submission portal will close, and no further submissions be allowed or considered. It is the sole responsibility of the Supplier to see that the proposals are submitted through the BidNet portal by the submission deadline.

Sales Prohibited/Conflict of Interest: No officer, employee, or member of the School Board, shall have a financial interest in the sale to the school district of any real or personal property, equipment, material, supplies or services where such officer or employee exercises directly or indirectly any decision-making authority concerning such sale or any supervisory authority over the services to be rendered. This rule also applies to subcontracts with the School District. Soliciting or accepting any gift, gratuity favor, entertainment, kickback or any items of monetary value from any person who has or is seeking to do business with the District is prohibited.

Collusive or sham proposals: Any proposal deemed to be collusive or a sham proposal will be rejected and reported to authorities as such. Your authorized signature on this proposal assures that such proposal is genuine and is not a collusive or sham proposal.

The District reserves the right to reject any and all proposals and to waive any irregularities or informalities.

Sincerely,
Rob Turf
Strategic Sourcing Supervisor
lturf@psdschools.org

REQUEST FOR PROPOSALS
EAP & MANAGED CARE SOFTWARE
RFP 23-690-001

BACKGROUND

Poudre School District is a high-performing district, covering more than 1,800 square miles in northern Colorado with diverse school settings. The District's instructional program is centered around District Ends, under the Policy Governance model, developed to support a comprehensive curriculum.

While more than 70% of the District's families choose to send their children to their neighborhood school, the District does support school choice and offers a wide spectrum of educational programs to fit any child's needs. Program options include International Baccalaureate, Core Knowledge, Bilingual/Dual Language Immersion, Hybrid/Online, Expeditionary Learning, Science, Technology, Engineering and Math (STEM) along with extra-curriculars and athletics. The District has two LEED certified school buildings and over 30 Energy Star awards and supports operational sustainability in all areas of work.
Our Schools:

- 31 elementary schools
- 10 middle schools
- 4 comprehensive high schools
- 2 additional combined middle/high schools
- 6 option (100% choice) schools
- 3 alternative high schools
- 1 online school
- 1 hybrid school (classes on campus and online learning)
- 5 charter schools

The District is fully accredited by the Colorado Department of Education Accreditation and Accountability Unit and is subject to periodic monitoring to ensure continued compliance with accreditation standards.

1.0 GENERAL CONDITIONS

1.1 Information and materials submitted in response to this solicitation may be considered public records subject to disclosure under the Colorado Open Records Act ("CORA"), C.R.S. §§ 24-72-200.1 to -205.5. Information and materials that Supplier believes are confidential and not subject to disclosure under CORA must be submitted separately with a citation to the section of CORA and any other relevant law under which Supplier believes they are confidential. The District, not Supplier, shall determine whether information and materials so identified will be withheld as confidential, but will inform Supplier in advance of disclosure to give it an opportunity to take legal action to protect its interests vis-à-vis the party making the CORA request.

1.2 This is a solicitation for an offer and is not an offer to contract for goods or services.

1.3 Supplier must provide all requested information. Failure to do so may result in rejection of the proposal at the option of the District.

1.4 Proposals must meet or exceed specifications contained in this document.

1.5 The District is exempt from city, county, state, and federal sales/excise taxes. Tax exempt certificates will be issued upon request.

1.6 Submission of a proposal is deemed as acceptance of all terms, conditions and specifications contained in the District's solicitation package initially provided to the Supplier. Any proposed modification must be accepted in writing by the District prior to award of the contract.

1.7 Each Supplier, its employees, representatives, and subcontractors, agrees to abide by all applicable federal, state, and local codes, laws, rules and regulations.

1.8 The successful Supplier shall furnish all supplies, which conform to all applicable safety codes and regulations.

1.9 Contact with District personnel regarding this RFP, other than inquiries to the specific Procurement Agent identified in this document, may be grounds for elimination from the selection process.

1.10 Proposals shall contain a signature of an authorized representative in the space provided on the Proposal Certification Form. Failure to properly sign the proposal may invalidate same and it may not be considered for award.

1.11 The accuracy of the solicitation is the sole responsibility of the Supplier. No changes in the proposal shall be allowed after the submission deadline, except when the Supplier can show clear and convincing evidence that an unintentional factual mistake was made, including the nature of the mistake.

1.12 Supplier must provide proof of insurance that meets the insurance requirements stated in Section 6.0 of this document.

1.13 Health and Safety Standards**.** The Supplier shall have and maintain a set of protocols and guidelines to meet evolving health and safety requirements and implement any applicable communicable disease protocols, which must follow guidance and orders from state and/or local public health officials and be no less strict than the District's protocols.

1.13.1 Supplier shall ensure all individuals providing Services under this agreement for the Supplier wear appropriate personal protective equipment as designated in this section 1.13, at all times while on District property.

1.13.2 If the District is directed, or the District determines to limit or restrict access to any or all of its facilities or District Location due to a public health or safety concern, the District may, at its discretion, temporarily delay or stop Supplier's services, with or without prior notice.

1.14 The successful Supplier is not permitted to transfer any interest in the project whether by assignment or otherwise, without prior written consent of the District's Strategic Sourcing Department.

1.15 Suppliers are required to complete the Reference Form included in this solicitation as described.

1.16 Supplier must note in the solicitation response any intent to use subcontractors. The subcontractor's name, address, phone number and three client references, along with the type of work to be performed must be included. Use of subcontractors may be considered as a factor in the District's evaluation process. If the Supplier fails to notify the District of its intent to use subcontractors in the proposal submittal, the proposal may be considered a void offer. Subcontractors will be allowed only by written permission of the District. The Supplier agrees that it is fully responsible to the District for the acts or omissions of its subcontractors, or any persons employed by them, in the same way as it is for the acts and omissions of persons directly employed by the Supplier. Nothing contained in the contract, or any subcontract shall create any contractual relation between any subcontractor and the District.

1.17 The District reserves the right to reject any and all proposals or any part thereof, to waive any formalities, and further, to award the proposal to the responsible Supplier as deemed in the best interest of the District.

1.18 There is no expressed or implied obligation for the District to reimburse responding Suppliers for any expenses incurred in preparing proposals in response to this request.

1.19 Responses to this solicitation will be independently evaluated by an evaluation committee to be established for such purpose.

1.20 Proposals submitted will be evaluated using pre-determined objective rating criteria. Those that are clearly non-responsive to the stated requirements may be eliminated prior to the evaluation. Prior to proposal submission, Supplier are encouraged to check the BidNet website to ensure additional requirements are incorporated into its submissions.

1.21 The District reserves the right to negotiate further with one or more Suppliers or to request additional information. The District may make such inquiries and conduct such investigations as it deems necessary to determine the qualifications and ability of the Supplier to provide the services called for under the RFP and/or represented in the Supplier's response. Suppliers shall timely provide information to the District in connection with such inquiries and investigations. Suppliers may be asked to give presentations to the District regarding their proposals.

1.22 Should the District determine, in its sole discretion, that only one Supplier is fully qualified or that one Supplier is clearly more highly qualified than the others under consideration, a contract may be negotiated and awarded to that Supplier.

1.23 The District intends for the contract to commence upon complete execution of a successfully negotiated agreement and continue in full force and effect through and including June 30, 2024, unless earlier terminated by the District as provided in Section 1.27 below. The final award and contract start date is contingent upon a successfully negotiated and fully executed contract between the District and the recommended Supplier. The intended date is provided for planning purposes only.

1.24 For services provided, and at the option of the District, the agreement may be extended beyond the first term for up to four (4) additional one-year terms, subject to the parties' negotiation of mutually agreed upon amendments to the Agreement for each one (1) year term. Pricing will remain fixed and firm for the initial term and all extensions of the agreement.

1.25 Notwithstanding any other term or provision of this Request for Proposal, the District's obligations hereunder are expressly subject to its budgeting and appropriation of sufficient funds for each fiscal year (July 1 - June 30) a contract is in effect. In no event shall the District's obligations in a contract constitute a multiple-fiscal year direct or indirect debt or other financial obligation under Article X, Section 20(4)(b) of the Colorado Constitution.

1.26 Notwithstanding the other provisions of this RFP, either party may terminate this Agreement at any time in that party's sole discretion for any reason, with or without cause, by providing the other party with thirty (30) days' advance written notice. In the event of such termination: (a) the District shall pay Supplier for all Services performed under and in accordance with this Agreement up to the date of termination; and (b) Supplier shall reimburse the District for all payments made in excess of Services performed up to the date of termination.

1.27 The successful Supplier will be required to enter into and sign a formal agreement with the District. The agreement language will control over any language contained within this RFP that conflicts with the signed and fully executed agreement.

1.28 In the case of conflicts between the RFP and any referenced proposal documents, the more stringent requirements shall govern. In all cases, the Supplier is responsible for notifying the District of the conflict.

1.29 Supplier warrants that it has full power and authority to grant the rights of its license agreement to the District with respect to its program without consent of any other person or entity. Supplier also warrants that neither the performance of the services by its company, nor the license to and use by the District of its company's product and documentation will in any way constitute an infringement nor other violation of any United States issued copyright, trade secret, trademark, patent, invention, propriety information, non-disclosure, or other right of any third party.

1.30 Access to District Server. If access to any District server is necessary for the functionality of the Contractor's services. Upon written approval by the Executive Director of Information Technology or designee, the District grants the Contractor limited access to the District server for the sole purpose of providing Services

1.30.1 The Contractor agrees to protect the confidentiality, integrity and availability of all electronic District or student information at all times.

1.30.2 The Contractor agrees to take proper steps to ensure the security of the device in which they connect to the District's systems remotely. The Contractor agrees not to copy information accessed remotely to local devices and or portable devices. Printing information is not permitted unless specific authorization has been granted.

1.30.3 The Contractor shall not share passwords, codes, credentials or user accounts with others.

1.30.4 The Contractor shall have a valid and up-to-date antivirus agent installed to ensure protection against malware and viruses upon connection to the District network.

1.30.5 The Contractor acknowledges that if the District determines in its discretion that remote access has been compromised by unauthorized parties, or that remote access has been misused, the Contractor's access will be disabled or terminated immediately

1.31 The Supplier shall provide the services as an independent contractor of the District. As such, the Supplier shall have the right to determine how and by whom

the services will be provided, subject to and consistent with the terms and conditions of this solicitation.

1.31.1 The Supplier shall be exclusively responsible for: (a) all compensation, employment tax withholdings and payments, and all fringe benefits for its employees in full compliance with all applicable federal, state and local laws; (b) all insurance coverages and benefits for its employees in full compliance with all applicable federal, state and local laws, including but not limited to pension or retirement benefits, workers' compensation, unemployment compensation, and Social Security benefits; and (c) all payments to its suppliers and subcontractors for goods and/or services directly or indirectly related to this solicitation.

1.31.2 Nothing in this solicitation or as a result of this solicitation shall be construed as creating a single enterprise, partnership, joint venture or employer-employee relationship between a future Supplier and the District. The future Supplier will not be considered a partner, agent or representative of the District and will not represent itself to be a partner, agent or representative of the District. The District is not a partner, agent or representative of any future Supplier and shall not represent itself to be a partner, agent or representative of the Supplier.

1.32 Qualifications of Supplier

1.32.1 The District may make such reasonable investigations as deemed proper and necessary to determine the ability of the Supplier to perform the work and the Supplier shall furnish to the District all such information and data for this purpose as may be requested.

1.32.2 The District further reserves the right to reject any proposal if the evidence submitted by, or investigations of, such Supplier fails to satisfy the District that such Supplier is properly qualified to carry out the obligations of the contract and to complete the work/furnish the item(s) contemplated therein.

1.33 Miscellaneous

1.33.1 Once the evaluation is complete and the Intent to Award has been issued to the recommended Supplier, the recommended Supplier will work with the District's Contract Administrator to successfully negotiate an agreement.

1.33.2 Governing Law and Venue. All issues regarding the formation, performance and/or legal enforcement of the Contract shall be governed by and construed in accordance with the laws of the State of Colorado. Venue for the resolution of any disputes arising out of or relating to the Contract shall be in Larimer County, Colorado.

1.33.3 Equal Opportunity. It is agreed that no otherwise qualified Supplier shall be excluded from participating in, be denied the benefits of, or be subject to discrimination, including harassment, under any provision of this Agreement on the basis of race; creed; color; national origin; age; sex; pregnancy; physical recovery from childbirth or a related condition; sexual orientation; marital status; veteran status; religion; genetic information; gender expression; gender identity; ancestry; or disability.

1.33.4 Appeal of Award. The Supplier may appeal the award by submitting, in writing, a request for re-consideration to the District's Executive Director of Finance within seventy-two (72) hours after the receipt of the notice of award.

1.33.5 In the event the awarded Supplier defaults on its contract or the contract is terminated for cause due to performance, the District reserves the right to re-procure the Services from the next lowest Supplier or from other sources during the remaining term of the terminated/defaulted contract. Under this arrangement, the District shall charge the awarded Supplier any differences between its price and the price to be paid to the next lowest Supplier, as well as, any costs associated with the re-solicitation effort which resulted from such default or termination.

1.33.6 This solicitation does not commit the District to award a contract or to pay any costs incurred in the preparation of a proposal or to procure a contract for the services. The District reserves the right to accept or reject any or all proposals received as a result of this request or to cancel in part or in its entirety this solicitation if it is deemed to be in the best interest of the District. The District reserves the right to accept any portion of the proposal, or the entire proposal as deemed in the best interest of the District.

1.33.7 For the purposes of solicitation evaluation, Supplier must indicate any variances to the specifications and terms and conditions, no matter how slight. If variations are not stated in the Supplier's response, it shall be construed that the proposal fully complies with the specifications and terms and conditions. Notwithstanding the above, it is hereby agreed and understood that the District reserves the right to reject these variations if they individually or, as a whole, do not meet the standards established in the specifications. Modifications to this RFP document and/or exhibit will not be considered valid and may be cause for disqualification. Award of this solicitation does not constitute the District's acceptance of the Supplier's proposed variations.

1.33.8 Sustainability. The District is committed to be a responsible steward of our natural resources and believes that public education should provide leadership in developing an ethic of sustainability in all its practices. In the District we have both Energy Conservation and Waste Management

policies and espouse these values, making environmental stewardship and integral part of the physical plant operation.

1.34 Cooperative Purchasing Efforts. Poudre School District is a member of, or affiliated with, several regional professional procurement organizations within Colorado and Wyoming. These organizations are comprised of governmental purchasing agents, or agency representatives responsible for the purchasing function.

1.34.1 These organizations include:

1.34.1.1 Colorado Educational Purchasing Council (CEPC) - A cooperative purchasing organization comprised of purchasing agents/buyers representing all Colorado public school districts.

1.34.1.2 Multiple Assembly of Procurement Officials (MAPO) - A cooperative purchasing organization comprised of procurement representatives from state, county, municipal, governments, special districts or school districts along the front range of the Rocky Mountains in Colorado.

1.34.1.3 Rocky Mountain Governmental Purchasing Association (RMGPA) - A chapter member of the National Institute of Governmental Purchasing (NIGP), consisting of public procurement professionals and their representative agencies which include approximately 100 state, county, and municipal governments; school districts and higher education; and other special districts.

1.34.2 Members of these organizations, at their discretion, may request use of the contracts or awards that result from this solicitation. Each governmental entity which uses a contract(s) resulting from this solicitation would establish its own contract, issue its own orders, schedule deliveries, be invoiced individually, make its own payments, and issue its own exemption certificates as required by the Supplier. It is understood and agreed that Poudre School District is not a legally binding party to any contractual agreement made between another governmental entity and the Supplier as a result of this solicitation. The District shall not be liable for any costs or damages incurred by any other entity. Usage by any other entity shall not have a negative impact on the District in the current term or in any future terms.

2.0 SCOPE OF WORK AND REQUIREMENTS

The District is requesting electronic proposals from professional and qualified Suppliers to provide the following software that includes but is not limited the requirements in this RFP and EXHIBIT A.

2.1 Minimum Requirements. Describe how your software meets or exceeds the following requirements:

2.1.1 Ability to create and customize intake forms (with different access controls) to meet District project needs.

2.2 Added Value

2.2.1 Tell us about your integrations with other platforms, to include calendars (the District uses Google and Outlook calendars currently). While we are interested in all integration options, we would be most interested in Microsoft and Google integrations.

2.2.2 Tell us about your product's visual design and interface and how that impacts usability.

2.2.3 Tell us about your product's reporting tools. Can custom reports be created by users, or would that require your intervention?

2.2.4 Tell us about your product's licensing and access controls. Who can see what and how does that impact pricing?

2.2.5 Tell us about your product's data security. Where and how is the data generated by your product stored? What security measures are in place to minimize risk?

2.2.6 How do you support your product? What static resources and dynamic training options are available?

2.2.7 Describe the onboarding process you would use for the District and individual users within the District.

3.0 COST PROPOSAL

3.1 Provide a line-item cost proposal based on services provided. All costs shall include options for and outline all role-based permission options.

3.1.1 Cost of software

3.1.1.1 Cost per individual user

3.1.1.2 Cost per group of users

3.1.1.3 Cost for enterprise level of use

3.1.2 Annual cost of a maintenance contract, including phone and online support.

3.1.2.1 Year 1

3.1.2.2 Year 2-5

3.1.3 Cost of training

3.1.3.1 Indicate the number of days anticipated for on-site training.

3.1.3.2 Provide cost for onboarding

3.1.3.3 Provide cost for user trainings

3.1.4 Indicate the number of days for delivery of software and services after receipt of a signed purchase order.

4.0 EVALUATION AND AWARD OF CONTRACT

4.1 Proposals will be evaluated on the following criteria. A cumulative point system will be used. Award shall be made to the most responsive and responsible Supplier meeting the specifications and deemed the most advantageous to the District.

Criteria	Points
System design and features	30
Ease of use for staff accessing the system	20
Ease of deployment and import of existing data	20
Cost Proposal	10
Timeframe, Support and Maintenance, Training	10
References from other school districts (Colorado preferred)	10

4.2 The District may at its discretion, elect to interview one (1) or more Suppliers that submit a proposal, but is not required to do so. The interview may either be conducted via a virtual platform or in person at a Poudre School District location (Ft. Collins, Colorado).

4.2.1 The determination of whether to conduct interviews with the finalist(s) shall be made by the District based solely on its determination of whether interviews would be helpful in evaluating the proposals.

4.2.2 Any Supplier selected for an interview will be expected to make an introductory presentation followed by a demonstration and question and answer period. The District will not reimburse any travel related or other expenses related to an interview.

4.3 Once the evaluation is complete and the Intent to Award has been issued to the recommended Supplier, the recommended Supplier will work with the District's Contract Administrator to successfully negotiate a District agreement.

--Intentionally left blank--

References are mandatory – List three (3), non-Poudre School District, K-12 education market references, for which your company has completed similar services for projects of similar scope. The District may contact these references during the evaluation process. **Client reference letters shall be included in addition to the reference information listed below.**

5.1 Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

_____

5.2 Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

_____

5.3 Company Name _____

Address _____

Contact Person _____

Telephone _____

Email _____

Describe type of work/service performed or items supplied _____

_____

6.0 INSURANCE

Supplier shall procure and maintain the required insurance specified below for the duration of this Agreement, which insurance shall be written for not less than the amounts specified or greater if required by law. The District's receipt of a Certificate of Insurance from the Provider with limits and or coverages that do not meet the requirements does not waive the requirements and the Provider shall still be responsible for the limits and coverages stated in this Agreement. Specified coverages and amounts may be provided by a combination of a primary policy plus an umbrella or following form excess policy. All insurance shall be with a carrier licensed in the state of Colorado and shall have a minimum A.M. Best rating of A-VII. Provider shall furnish the District's Director of Records and Risk Management with certificates of the required insurance prior to the District's approval and signing of this Agreement, and with renewal certificates prior to the expiration of any required insurance that expires during the term of this Agreement. Memorandums of Insurance will not be accepted. Certificates of Insurance and all communication regarding insurance shall be sent to:

Poudre School District
Attention: Risk Management
2407 Laporte Ave
Ft. Collins, CO 80521
Please Email Certificate to: COI@psdschools.org

Any insurance and/or self-insurance carried by the District is excess of the coverage extended to the District by Supplier. Supplier shall provide at least thirty (30) days' advance written notice to the District prior to cancellation, change of coverage, or non-renewal. The insurance requirements specified in this section 6.0 shall not reduce the indemnification liability that Supplier has assumed in section 6.1.

Commercial General Liability

Minimum Limits

- Each Occurrence Bodily Injury & Property Damage $2,000,000
- General Aggregate $3,000,000
- Products/Completed Operations Aggregate $2,000,000
- Personal/Advertising Injury $2,000,000
- Coverage must be written on an "occurrence" basis.
- Poudre School District R-1 and its elected officials, employees, agents, and volunteers shall be named as an additional insured or covered as an additional insured by way of a blanket endorsement and shall be insured to the full limits of liability purchased by the Provider even if those limits of liability are in excess of those required by this Agreement.

Technology Errors and Omissions Liability (Professional Liability, including Network Security and Privacy Liability)

Minimum Limits

- Per Loss $1,000,000
- Aggregate $3,000,000
- Liability extends for a period of three (3) years beginning at the time work under this Agreement is completed. Provider shall maintain continuous coverage, as required by the Agreement, for this period.

The insurance shall provide coverage for:

- Liability arising from theft, dissemination and/or use of confidential information (defined term including but not limited to bank account, credit card account, personal information such as name, address, social security numbers, etc. information) stored or transmitted in electronic form.
- Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party to gain access to Provider's services including denial of service, unless caused by a mechanical or electrical failure.
- Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a District or third person's computer, computer system, network, or similar computer related property and the data, software, and programs thereon.
- Poudre School District R-1, its elected officials, employees, agents, and volunteers, the contractor, and subcontractors, shall be named insureds under the policy.

Crime Coverage (for agreements allowing privileged access to network systems, valuable property or sensitive data)

Minimum Limit Per Loss $1,000,000

The policy shall include:

- Coverage for all directors, officers, agents, and employees of the Provider.
- Employee dishonesty, forgery and alteration, monies and securities, and computer (cyber) crime.
- Extended theft and mysterious disappearance.
- The policy shall not contain a condition requiring an arrest and conviction.
- Policy must be endorsed to cover Third Party Fidelity and include Poudre School District R-1 as a Loss Payee.

Workers' Compensation and Employers' Liability

If Provider is exempt under the Colorado Workers' Compensation Act, this requirement will be waived if proof a current Workers' Compensation Coverage Rejection is on file with the Colorado Department of Labor and Employment, Division of Worker's Compensation and a copy is submitted to the District.

Minimum Limits

- State of Colorado Statutory
- Employer's Liability $100,000 Each Accident
  $500,000 Disease – Policy Limit
  $100,000 Disease – Each Employee

- Waiver of subrogation in favor of Poudre School District R-1.

6.1 Supplier shall indemnify and hold harmless the District and the District's Board members, employees, representatives and agents from and against any and all liability arising from any suit, action, grievance, charge or proceeding brought in connection with or related to Supplier's operations, provision of services and/or conduct of any of its employees, volunteers, agents or representatives. The indemnification and hold harmless obligation hereunder shall include all attorney fees, costs and expenses incurred by the District and/or the District's Board members, employees, representatives and/or agents in defense of said suits, actions, grievances, charges and/or proceedings. Nothing in this section or otherwise in this contract shall be construed in any way or applied in any manner as a compromise or waiver of the District's rights and protections under the Colorado Constitution or the Colorado Governmental Immunity Act.

7.0 MODEL FORMAT OF PROPOSAL

To simplify the review process and obtain the maximum degree of comparability, proposals ***must*** be organized in the manner specified below.

7.1 Title Page

7.1.1 Show the solicitation subject, the name of the proposing Supplier, local address, telephone number, name of the contact person and the date.

7.2 Table of Contents

7.2.1 Include a clear identification of the material by section and by page number.

7.3 Letter of Transmittal – Limit to three (3) pages.

7.3.1 Briefly state the Supplier's understanding of the work to be done and describe in detail the Supplier's ability to fulfil the scope meet the deadlines requested by the District.

7.3.2 State the names of the persons who will be authorized to make representations for the Supplier, their titles, addresses, phone numbers, and email addresses.

7.4 Supplier's Approach

7.4.1 Submit a work plan to accomplish the scope and questions defined in the Scope of Work and Requirements (Section 2.0).

7.4.2 Responses should be formatted in order, labeled as such, and follow the exact sequence of the solicitation Scope of Work section.

7.4.3 Clarification questions and requests for information throughout the solicitation shall be clearly labeled with the section and subsection number and include the Supplier's response/information.

7.4.4 Any and all assumptions shall be clearly stated in the Supplier's response. Assumptions that are not clearly indicated, but raised later in the award process, may be grounds for the Supplier's response to be considered non-responsive.

7.5 References

7.5.1 Submit completed reference form in Section 5.0.

7.6 Cost Proposal

7.6.1 Provide a cost proposal as identified in Section 3.0. Cost proposal and supporting documentation shall be clearly labeled "RFP 23-690-001."

7.7 Proposal Certification Form

7.7.1 Submit the completed form in Section 8.0.

--Intentionally left blank--

Proposals must be submitted and received in BidNet's electronic solicitation portal on or before 2:00 p.m. MT on ~~March 23, 2023~~ March 28, 2023.

The undersigned hereby affirms that:

- He/she is a duly authorized agent of the company issuing this proposal and that all information provided in the proposal is true and accurate.
- Supplier has read the conditions, including the insurance requirements and technical specifications, which were made available to the company in conjunction with this RFP, and fully understands and accepts these terms unless specific variations have been expressly requested in the response submitted by the Supplier. Requested variations will be reviewed by the District and approved on a case-by-case basis if deemed appropriate.
- The company will adhere to all terms and conditions and provide, at a minimum, all services as expressed in the solicitation and/or the company's proposal responding to the solicitation.
- The company meets or exceeds all of the required criteria as specified by this solicitation, or if not, has submitted a Justification for Consideration addressing any failure to meet the criteria.
- The company's proposal is being offered independently of any other Supplier and in full compliance with the terms specified in Sections 1 and 2 of the solicitation.
- The company will accept any awards made to it, contingent on contract negotiation, as a result of this solicitation for a minimum of ninety (90) calendar days following the date and time of the solicitation opening.

Company Name: _____

Signature of Agent: _____

Printed Name: _____

Title: _____

E-mail address: _____

Mailing address: _____

Telephone: _____

Contact Person: _____
(If different from Agent, include e-mail address and phone number)

NOTE: Proposals submitted without the signature of an authorized agent of the company may be considered non-responsive and ineligible for the award.

Exhibit B

SCOPE OF WORK AND REQUIREMENTS

Poudre School District Strategic Sourcing, RFP 23-690-001

2.1.1 Ability to create and customize intake forms (with different access controls) to meet District project needs.

Intake forms can be customized an used within the application. These forms can be added and populated within cases. EAP Expert also offers an Online Intake add-on service in which we work with your team to customize and brand the form for you to add to your website for members to request services digitally.

2.2.1 Tell us about your integrations with other platforms, to include calendars (the District uses Google and Outlook calendars currently). While we are interested in all integration options, we would be most interested in Microsoft and Google integrations.

EAP Expert offers the following integration:

- **Cronofy Calendar sync – Two-way sync with Outlook and Gmail**
- **DocuSign**
- **Twilio – Email, text, and voice appt reminders**
- **ProtoCall – Afterhours call center**
- **HR System import – Automatically imports eligibility files.**

2.2.2 Tell us about your product's visual design and interface and how that impacts usability.

EAP Expert uses tabbed layouts for users to easily see a clients history and the type of case without having to go digging. Our software is also has the ability for you team to customize the layouts of forms so you are not stuck with our look and feel off of the shelf.

2.2.3 Tell us about your product's reporting tools. Can custom reports be created by users, or would that require your intervention?

EAP Expert has both a report module which houses over 350 canned reports as well as a utilization report module. All reports in the system are customizable within the application by using the internal report designer. This allows your team to customize a canned report or create one from scratch.

2.2.4 Tell us about your product's licensing and access controls. Who can see what and how does that impact pricing?

Each person that requires access to the software will require a license. Each user will have a set of security access rights assigned to their account/role which will allow or prevent access to sensitive data. The access rights are controlled by the users you assign as administrators.

2.2.5 Tell us about your product's data security. Where and how is the data generated by your product stored? What security measures are in place to minimize risk?

EAP Expert partners with AWS for our server environment and Cloudticity for our security framework on our servers. EAP Expert also has a HiTrust certified hosted environment. Please review the attached security document for mor information.

2.2.6 How do you support your product? What static resources and dynamic training options are available?

10 Hrs of telephone training is standard with the implementation and additional training can be purchased. As for support, you will have a dedicated account manager as well has 24/7 tech support. EAP Expert also provides clients with an online knowledgebase to access user manuals an other training resources.

2.2.7 Describe the onboarding process you would use for the District and individual users within the District.

The implementation consists of a data conversion, needs analysis, software configuration and training. The average time it takes to complete the implementation is 3-4 months. We use an online project management tool called Teamwork to help manage each of the implantation stages. If EAP Expert is the chosen vendor, we will work with you to create a custom implementation plan that meets your needs and then transfer that to Teamwork.

COST PROPOSAL

3.1 Provide a line-item cost proposal based on services provided. All costs shall include

options for and outline all role-based permission options.

3.1.1 Cost of software: **N/A**

3.1.1.1 Cost per individual user: **$179/user/month**

3.1.1.2 Cost per group of users: **N/A**

3.1.1.3 Cost for enterprise level of use: **N/A**

3.1.2 Annual cost of a maintenance contract, including phone and online support.

3.1.2.1 Year 1: **See Below** 3.1.2.2 Year 2-5: **See Below**

EAP Expert Cost Breakdown

Item	Year One	Year Two	Year Three	Year Four	Year Five
7 FULL Licenses	$15,036.00	$15,036.00	$15,036.00	$15,036.00	$15,036.00
Training	$1,390.00				
Data Conversion	$4,500.00				
Eligibility File Import	$600.00	$600.00	$600.00	$600.00	$600.00
Yearly Total:	$21,526.00	$15,636.00	$15,636.00	$15,636.00	$15,636.00

3.1.3 Cost of training: **$1390.00 (10hrs telephone training)**

3.1.3.1 Indicate the number of days anticipated for on-site training: **Optional (2 days)**

3.1.3.2 Provide cost for onboarding: **Included**

3.1.3.3 Provide cost for user trainings: **Included**

3.1.4 Indicate the number of days for delivery of software and services after receipt of a signed purchase order: **3-4 Business days**

REFERENCE FORM EAP & MANAGED CARE SOFTWARE

References are mandatory – List three (3),

David Darmetko, LMSW

Business Relationship Manager

Henry Ford ENHANCE - Employee Assistance Program

313.874.6205 Office

313.673.9997 Mobile

DDarmet1@hfhs.org

Susan Weinstein, LCSW, CEAP, SAP

Clinical Director of EAP

Penn Medicine Employee Assistance Program

(609) 688-3212

Susan.weinstein2@PennMedicine.UPenn.edu

Pronouns: she/her/hers

www.princetonhcs.org/eap

Workplace Solutions

Rosanna Velat, LCPC, CEAP

Clinical Manager

rosanna.velat@wseap.com

EXHIBIT A - EAS SOFTWARE RFP:

Specs for EAP and Managed Care software

Client and clinical note Module**: Yes**

Provides fields for client demographics, HR information (position, location, date of hire, employee ID) and Benefit information**: Yes**

Customizable, Drop-down menus for

Assessed Problem(s) **: Yes**

Location**: Yes**

Business Unit**: Yes**

Who is the client (ee, spouse, child, other) **: Yes**

"Referred by" source**: Yes**

Health plan selection/who is covered**: Yes**

Gender**: Yes**

Marital status**: Yes**

Links to "related" cases for this client and covered family members**: Yes**

Ability to "manually relate" cases (e.g. when both parties are PSD EE's) **: Yes**

Ease of opening new cases – transfer of crucial information; **: Yes**

Ability to access to cases, documents, referrals, etc. across all cases for that individual**: Yes**

Ability to change case number in clinical notes; scheduler; referral authorizations to move to the appropriate case as needed. **: Yes**

Ability to record, edit, and view all types of contacts with clients**: Yes**

Ability to create referral authorizations to EAS managed care network providers (integrated with Managed Care Provider Module) **: Yes**

Provide popup alerts for URs and authorization renewals**: Yes**

Maintain list of referrals per client across all cases**: Yes**

Ability to upload documents to client case**: Yes**

Interface with Workplace Consults and Auxiliary Services**: Yes**

Ability to edit a record when multiple users are viewing that record; **: Yes**

Access to view/edit contact notes is not time or date limited**: Yes**

Pop up warning of missing data**: No**/need to save**: Yes** /confirmation of "delete record" **: Yes**

Ability to assign a case to an EAS staff counselor**: Yes**

Mail merge capability: **No, but can be easily done by exporting emails from a report.**

Customizable field naming**: Yes**

Organizational**: Yes**

Company/Organization management**: Yes**

Utilization figures (# EE's/# eligible individuals) **: Yes**

Dropdowns for:

Locations**: Yes**

Business units**: Yes**

Scheduler**: Yes**

Centralized appointment scheduling that includes all EAS counselors on one screen**: Yes**

Ability to schedule appointments – that link to client note screen**: Yes**

Customizable for types of appointments**: Yes**

SMS/email reminders**: Yes (additional cost for text appt reminders)**

Ability to search, cut/copy/paste, click-drag to move appointments**: Yes**

Ability to create, update and maintain recurring events**: Yes**

Ability to create, update and maintain events for all staff**: Yes**

Ability to report on scheduled events by date range and type**: Yes**

Options when manipulating recuring events**: Yes**

Workplace Consults and Auxiliary Services Modules Interface between WPC and AS**: Yes**

Tracks time allocations and contacts**: Yes**

Interfaces with client cases**: Yes**

Ability to upload documents**: Yes**

Customizable

Managed Care/Provider Network Module**: Yes**

Ability to add/view/maintain Provider Network participants**: Yes**

Customizable demographic data fields**: Yes**

Ability to define umbrella “group practices” AND providers within that organization

dropdowns**: Yes**

provider specialty checkboxes**: Yes**

license/liability insurance renewal fields**: Yes**

mail merge capability: **Same as above**

Ability to upload documents to provider file**: Yes**

Interface with client referral screen; ability to create referrals**: Yes**

Flexibility in information recorded for providers**: Yes**

Searchable on any data field/using user defined criteria**: Yes**

Flexible reporting criteria**: Yes**

License and insurance expiration alerts**: Yes (we suggest reports however)**

Customizable data fields and field names**: Yes**

Data management and reporting**: Yes**

Ability to report on various aspect of clinical contact, workplace consults, auxiliary services**: Yes**

Ability to convert existing EAS SQL queries to “like” data reports**: Yes**

Customizable ROI calculations**: Yes**

Customizable reports for client case information**: Yes**

Customizable reports for Managed Care Provider Network database**: Yes**

System Administration**: Yes**

Audit History (view/access user history) **: Yes**

User administration and password management**: Yes**

“Unlock records” feature (if needed, for multiple users to be in one case at the same time) **: Yes**

User security roles/levels**: Yes**

SQL query assistant (if database is SQL based) and printable code list (if appropriate) **: Yes but ideally we use the front end filtering tools and reports. It will mush easier.**

Global messaging: **: Yes Through the Alters and To-Dos**

Ability to set “default values” for defined data fields (city, state, hours/minutes of session, etc) **: Yes**

Ability to convert data from Premier software**: Yes**

HIPAA compliant**: Yes**

EAPexpert

Web-based; secure hosting**: Yes**

Ability to customize all database fields**: Yes**

User friendly**: Yes**

Unlimited Licenses: **Purchased as needed. No limit**

Support**: Yes**

Security – backups, monitoring, multifactor authentication**: Yes**

Spell Check**: Yes**

Reminders list**: Yes**

WRITTEN CYBERSECURITY PROGRAM (WISP)

EAP Expert, Inc.

NIST

WISP
Written Information Security Program
NIST 800-53 Rev 4

TABLE OF CONTENTS

WRITTEN CYBERSECURITY PROGRAM (WISP) OVERVIEW

INTRODUCTION

The Written Cybersecurity Program (WISP) provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program at EAP Expert, Inc. (EAP Expert).

EAP Expert is committed to protecting its employees, partners, clients and EAP Expert from damaging acts that are intentional or unintentional. Effective cybersecurity is a team effort involving the participation and support of every EAP Expert user who interacts with data and systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities accordingly.

Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems. This also includes against accidental loss or destruction.

PURPOSE

The purpose of the Written Cybersecurity Program (WISP) is to prescribe a comprehensive framework for:

- Creating a NIST-based Cybersecurity Management System (ISMS);
- Protecting the confidentiality, integrity, and availability of EAP Expert data and systems;
- Protecting EAP Expert, its employees, and its clients from illicit use of EAP Expert systems and data;
- Ensuring the effectiveness of security controls over data and systems that support EAP Expert's operations.
- Recognizing the highly-networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review, and maintenance of minimum security controls required to protect EAP Expert's data and systems.

The formation of these cybersecurity policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which EAP Expert operates and safeguards its data and systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related standards, procedures, and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure EAP Expert users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help EAP Expert comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of EAP Expert data.

Scope & Applicability

These policies, standards, procedures and guidelines apply to all EAP Expert data, systems, activities, and assets owned, leased, controlled, or used by EAP Expert, its agents, contractors, or other business partners on behalf of EAP Expert. These policies, standards, procedures and guidelines apply to all EAP Expert employees, contractors, sub-contractors, and their respective facilities supporting EAP Expert business operations, wherever EAP Expert data is stored or processed, including any third-party contracted by EAP Expert to handle, process, transmit, store, or dispose of EAP Expert data.

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting EAP Expert business functions shall comply with the policies. EAP Expert departments shall use these policies or may create a more restrictive policy, but none that are less restrictive, less comprehensive, or less compliant than these policies.

These policies do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

Appendix E: Cybersecurity Roles & Responsibilities provides a detailed description of EAP Expert user roles and responsibilities, in regards to Cybersecurity.

EAP Expert reserves the right to revoke, change, or supplement these policies, standards, procedures and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management unless otherwise stated.

Policy Overview

To ensure an acceptable level of Cybersecurity risk, EAP Expert is required to design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems.

EAP Expert users are required to protect and ensure the Confidentiality, Integrity, and Availability (CIA) of data and systems, regardless of how its data is created, distributed or stored.

- Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and
- Security controls must be designed and maintained to ensure compliance with all legal requirements.

Violations

Any EAP Expert user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exceptions

While every exception to a standard potentially weakens protection mechanisms for EAP Expert systems and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to policies, procedures or standards are available in Appendix F: Cybersecurity Exception Request Procedures.

Updates

Updates to the Written Cybersecurity Program (WISP) will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

KEY TERMINOLOGY

In the realm of Cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Cybersecurity Terms*, is the primary reference document that EAP Expert uses to define common Cybersecurity terms. [1] Key terminology to be aware of includes:

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended, and that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

Control: A term describing any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help EAP Expert accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Applicability: A term describing the scope in which a control or standard is relevant and applicable.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align EAP Expert with accepted due care requirements.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. Appendix A: Data Classification & Handling Guidelines provides guidance on data classification and handling restrictions.

Data Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Cybersecurity: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, and Availability (CIA) of data.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

Sensitive Personally Identifiable Information (sPII): sPII is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements: [2]

- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
- Driver License (DL) or other government-issued identification number (e.g., passport, permanent resident card, etc.)
- Financial account number
- Payment card number (e.g., credit or debit card)

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

[1] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[2] The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - http://www.leg.state.or.us/ors/646a.html and Massachusetts 201 CMR 17.00" Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Sensitive Data: A term that covers categories of data that must be kept secure. Examples of sensitive data include sensitive Personally Identifiable Information (sPII), Electronic Protected Health Information (ePHI), and all other forms of data classified as Restricted or Confidential in Appendix A: Data Classification & Handling Guidelines.

Standard: A term describing formally established requirements in regard to processes, actions, and configurations.

System: A term describing an asset; an information system or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.

Target Audience: A term describing the intended group for which a control or standard is directed.

POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Cybersecurity documentation is comprised of five main parts: a core policy; a control objective that identifies desired conditions; measurable standards used to quantify the requirement; procedures that must be followed; and guidelines that are recommended, but not mandatory.

Figure 1: Cybersecurity Documentation Framework

CYBERSECURITY CONTROL OBJECTIVES

EAP Expert's standards are organized into classes and families for ease of use in the control selection and specification process. There are four (4) general classes of security control objectives that align with FIPS 199.[3] These classes are further broken down into twenty-six (26) families of security control objectives.

- **Management**
  - Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics.
  - Management controls also play an important role in policy enforcement, since these focus on the management of the cybersecurity program and the management of risk within EAP Expert.
- **Operational**
  - Operational controls are primarily focused on resource the execution of the day-to-day cybersecurity program.
  - These controls generally focus on the means to control logical and physical access to information and to protect the security of supporting systems.
- **Technical**
  - Technical controls are primarily technical in nature. These controls, such as devices, processes, protocols, and other measures, are used to protect the confidentiality, integrity, and availability of the organization's technology assets and data.
  - These are dependent upon the proper functioning of the system for their effectiveness and therefore require significant operational considerations.
- **Privacy**
  - The focus is on controls that impact Personally Identifiable Information (PII).
  - These dependent upon the proper functioning of the other classes of controls for their effectiveness and therefore require significant operational considerations.

[3] FIPS 199 - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. The table below summarizes the classes and families in the security control catalog and the associated family identifiers.

FIPS 199 Focus	Family	Identifier
Management	Security Assessment & Authorization	CA
Management	Planning	PL
Management	Program Management	PM
Management	Risk Assessment	RA
Management	System & Services Acquisition	SA
Operational	Awareness & Training	AT
Operational	Contingency Planning	CP
Operational	Incident Response	IR
Operational	Media Protection	MP
Operational	Personnel Security	PS
Operational	Physical & Environmental Protection	PE
Technical	Access Control	AC
Technical	Audit & Accountability	AU
Technical	Configuration Management	CM
Technical	Identification & Authentication	IA
Technical	Maintenance	MA
Technical	System & Communications Protection	SC
Technical	System & Information Integrity	SI
Privacy	Authority & Purpose	AP
Privacy	Accountability, Audit & Risk Management	AR
Privacy	Data Quality & Integrity	DI
Privacy	Data Minimization & Retention	DM
Privacy	Individual Participation & Redress	IP
Privacy	Security	SE
Privacy	Transparency	TR
Privacy	Use Limitation	UL

Figure 2: NIST SP 800-53 Control Objectives Families & Identifiers

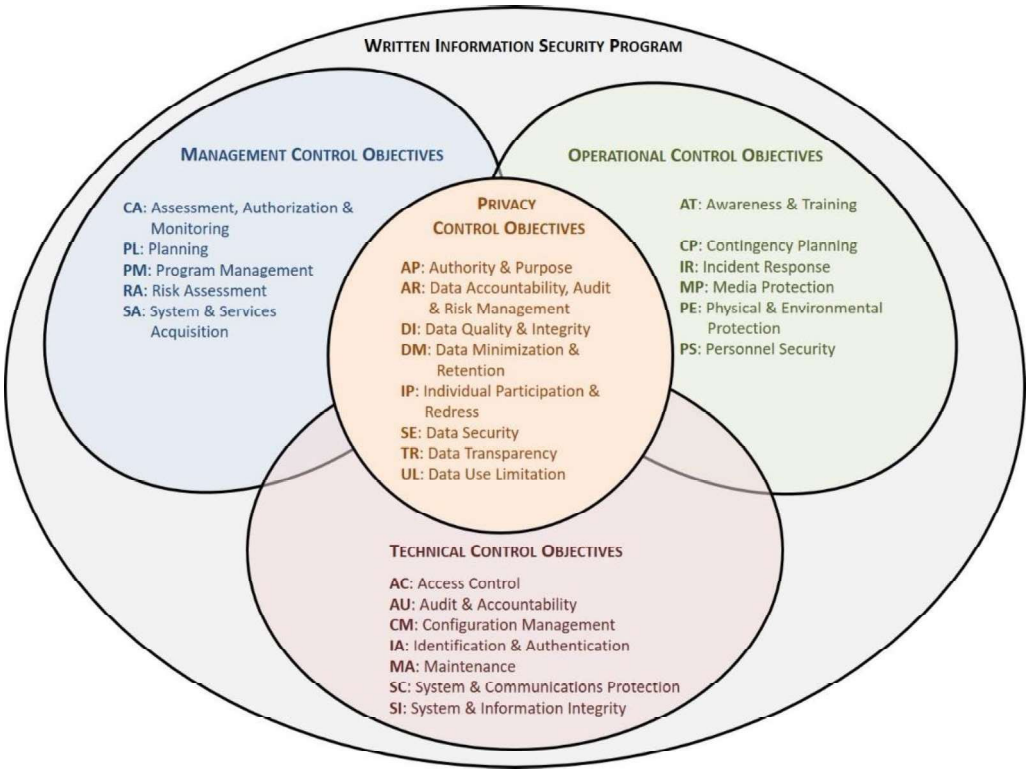

Figure 3: NIST 800-53 Security Control Objective Relationships

Cybersecurity Program Activities

An Information Security Management System (ISMS) focuses on Cybersecurity management and IT-related risks. The governing principle behind EAP Expert's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with ISO/IEC 27001, EAP Expert's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach:

- Plan: This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

Cybersecurity Considerations For Protecting Systems

Appendix G: Types of Security Controls provides a detailed description of cybersecurity considerations for protecting systems, based on the importance of the system and the sensitivity of the data processed or stored by the system.

MANAGEMENT CONTROLS

Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics. These cybersecurity controls address broader Information Security Management System (ISMS)-level governance of the security program that impact operational, technical and privacy controls.

SECURITY ASSESSMENTS & AUTHORIZATION (CA)

Security Assessment & Authorization Policy: EAP Expert shall periodically assess systems to determine if Cybersecurity controls are effective and ensure Cybersecurity controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Management Intent: The purpose of the Security Assessment & Authorization (CA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to the EAP Expert.

Supporting Documentation: Security Assessment & Authorization (CA)) control objectives & standards directly support this policy.

CA-01: SECURITY ASSESSMENT & AUTHORIZATION POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews, and updates:

- Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, and compliance; and
- Processes to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

Standard: EAP Expert is required to document cybersecurity assessment controls that, at a minimum, include:

(a) A formal, documented cybersecurity assessment procedure; and
(b) Processes to facilitate the implementation of cybersecurity assessments and authorizations.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

CA-02: SECURITY ASSESSMENTS

Control Objective: The organization:[4]

- Assesses the security controls in systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
- Produces a security assessment report that documents the results of the assessment; and
- Provides the results of the security control assessment, in writing, to the senior cybersecurity official or officially designated representative.

Standard: A formal cybersecurity risk analysis must be performed on all significant development and/or acquisitions, prior to systems being placed into production:

(a) New systems and applications must be appropriately tested for functionality prior to being placed in production; and
(b) Asset custodians and data/process owners are required to perform a gap analysis, at least once per year, to determine any deviations from their systems' current state of compliance and that which is required.

[4] MA201CMR17 17.03(2)(h) | OR646A.622(b)(B)(i)-(iv) | NIST CSF ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3

Supplemental Guidance: Security assessments should be performed on an ongoing basis since they are integral to identifying weaknesses, as well as validating that remediation actions were effective at eliminating or reducing vulnerabilities.

Control evaluators should have sufficient independence to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.

Enhancements:

- CA-02(a) – Independent Assessors
- CA-02(b) – Specialized Assessments
- CA-02(c) – External Organizations

CA-02(A): SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS

Control Objective: The organization employs assessors or assessment teams with independence to conduct security control assessments.

Standard: Whenever feasible, EAP Expert shall utilize independent assessors for security assessment functions.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational systems under assessment or to the determination of security control effectiveness.

CA-02(B): SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS

Control Objective: The organization includes as part of security control assessments, specialized assessments that may include:

- In-depth monitoring;
- Vulnerability scanning;
- Malicious user testing;
- Insider threat assessment; and
- Performance/load testing.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall utilize specialized assessments to address unique areas of risk.

Supplemental Guidance: Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes.

CA-02(C): SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS

Control Objective: The organization accepts the results of external assessments by impartial, external organizations.

Standard: EAP Expert shall accept the findings of assessments, when performed by impartial, external organizations with subject matter expertise in the area being assessed.

Supplemental Guidance: Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have with regard to assessments, the level of detail of supporting assessment documentation provided, or mandates imposed upon organizations by federal legislation, policies, or directives.

CA-03: INFORMATION SYSTEM CONNECTIONS

Control Objective: The organization allows connections only from authorized systems to connect to the Local Area Network (LAN).[5]

[5] NIST CSF ID.AM-3 & DE.AE-1

Standard: Only devices that are owned or managed by EAP Expert and meet baseline hardening standards are allowed to connect directly to EAP Expert's internal network(s).

Supplemental Guidance: Third-party remote access is allowed only through approved site-to-site VPN connections or through remote desktop-based connections.

Enhancements:

- CA-03(a) – Unclassified Non-National Security System Connections
- CA-03(b) – Restrictions on External System Connections
- CA-03(c) – Demilitarized Zones (DMZs)
- CA-03(d) – Guest Networks

CA-03(A): INFORMATION SYSTEM CONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

Control Objective: The organization prohibits the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device. [6]

Standard: Direct connections of EAP Expert systems to the Internet are:

(a) Allowed for mobile devices being operated outside of EAP Expert facilities, as long as the mobile devices have host-based anti-malware software installed and the host-based firewall is active;
(b) Prohibited for systems residing on EAP Expert's internal network(s); and
(c) Direct connections inbound or outbound for traffic between the Internet and sensitive data environments are prohibited.

Supplemental Guidance: Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between unclassified national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).

CA-03(B): INFORMATION SYSTEM CONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

Control Objective: The organization prohibits the direct connection of a system to an external network without the use of a boundary firewall device. [7]

Standard: Direct connections of EAP Expert systems to the Internet are:

(a) Allowed for computers being operated outside of EAP Expert facilities, as long as the mobile devices have host-based anti-malware software installed and the host-based firewall is active;
(b) Must connect via VPN; and
(c) Direct connections inbound or outbound for traffic between the Internet and the Cardholder Data Environment (CDE) are prohibited.

Supplemental Guidance: EAP Expert does not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (e.g., information flows) between internal systems and external networks.

CA-03(C): INFORMATION SYSTEM CONNECTIONS | DEMILITARIZED ZONES (DMZS)

Control Objective: If required for business needs, the organization will: [8]

- Implements a Demilitarized Zone (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;
- Limit inbound Internet traffic to IP addresses within the DMZ; and
- Block internal addresses from passing from the Internet into the DMZ.

Standard: EAP Expert's IT department is required to implement and configure DMZs in accordance with industry-recognized leading practices.

Supplemental Guidance: None

---

[6] PCI DSS 1.3, 1.3.3 & 1.3.5
[7] PCI DSS 1.3, 1.3.3 & 1.3.5
[8] PCI DSS 1.3.1, 1.3.2 & 1.3.4

CA-03(D): INFORMATION SYSTEM CONNECTIONS | GUEST NETWORKS

Control Objective: If required for business needs, the organization will implement a secure guest network. [9]

Standard: Guest access is required to:

(a) Be limited to a separate network that is logically separated;
(b) Permit only authorized traffic between the guest environment and internal networks; and
(c) Prevent direct access to EAP Expert's internal network(s).

Supplemental Guidance: None

CA-04: SECURITY VERIFICATION

Control Objective: The organization:

- Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
- Monitors system connections on an ongoing basis verifying enforcement of security requirements.

Standard: Asset custodians and data/process owners are required to document the environment related to their systems, which includes:

(a) Description of business requirements for each interface connections;
(b) Required security requirements; and
(c) The data classification of the information communicated through the interface(s).

Supplemental Guidance: In order to ensure data remains secure, it is important for EAP Expert to fully understand how its network communicates and validate that only authorized traffic is allowed. Additionally, the system connections should be monitored on an ongoing basis to verify enforcement of security requirements.

Enhancements: None

CA-05: PLAN OF ACTION & MILESTONES (POA&M)

Control Objective: The organization:

- Develops a Plan of Action and Milestones (POA&M) for systems to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
- Updates existing POA&M based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Standard: In a Plan of Action & Milestones (POA&M), or some other EAP Expert-approved method, asset custodians and data/process owners are required to document:

(a) All known vulnerabilities associated with the system(s);
(b) Planned remedial actions to correct the identified weaknesses or deficiencies; and
(c) Timeline to complete the remediation steps.

Supplemental Guidance: The POA&M should be kept up to date to reflect changes to the system or remedial actions taken to correct deficiencies.

Enhancements: None

CA-06: SECURITY AUTHORIZATION

Control Objective: The organization:

- Assigns a senior-level manager to the role of authorizing official for systems;
- Ensures that the authorizing official authorizes systems for processing before commencing operations; and
- Updates the security authorization.

[9] PCI DSS 1.2.3

Standard: EAP Expert requires all new technology platforms to be approved prior to the introduction of new systems in production environments. Unauthorized systems:

(a) Are prohibited from operating in a production environment; and
(b) May be disconnected from the network and/or powered off.

Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by management (e.g., authorizing officials) to authorize operation of systems and to explicitly accept the risk to organizational operations and assets, individuals, and other organizations based on the implementation of agreed-upon security controls. New technology platforms include, but are not limited to:

- Operating systems
- Productivity suites
- Firewalls

Enhancements: None

CA-07: Continuous Monitoring

Control Objective: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: [10]

- A configuration management process for systems;
- A determination of the security impact of changes to systems and the environment of operation;
- Ongoing security control assessments in accordance with organizational continuous monitoring strategy; and
- Reporting the security state of systems to appropriate organizational officials.

Standard: EAP Expert's management is required to assign a senior individual with technical experience the responsibility to monitor the effectiveness of EAP Expert's cybersecurity controls.

Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and cybersecurity to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and cybersecurity-related risks at a frequency sufficient to support organizational risk-based decisions.

Enhancements:

- CA-07(a) – Independent Assessment

CA-07(a): Continuous Monitoring | Independent Assessment

Control Objective: The organization employs assessors or assessment teams with reasonable independence to monitor the security controls in the information system on an ongoing basis.

Standard: EAP Expert may employ assessors or assessment teams with reasonable independence to monitor the security controls in the information system on an ongoing basis.

Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not:

- Create a mutual or conflicting interest with the organizations where the assessments are being conducted;
- Assess their own work;
- Act as management or employees of the organizations they are serving; or
- Place themselves in advocacy positions for the organizations acquiring their services.

CA-08: Penetration Testing

Control Objective: The organization conducts penetration testing on organization-defined systems or system components. [11]

[10] OR646A.622(b)(B)(iii) | NIST CSF ID.RA-1, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.CO-3 & RS.MI-3
[11] PCI DSS 11.3-11.3.3 | NIST CSF ID.RA-1 | NY DFS 500.04

Standard: EAP Expert shall perform external and internal penetration testing that includes the following:

(a) Is based on industry-accepted penetration testing approaches (e.g., NIST SP800-115);
(b) Coverage for the entire Cardholder Data Environment (CDE) perimeter and critical systems;
(c) Testing from both inside and outside the network;
(d) Testing to validate any segmentation and scope-reduction controls;
(e) Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5;
(f) Defines network-layer penetration tests to include components that support network functions as well as operating systems;
(g) Reviews and considerations of threats and vulnerabilities experienced in the last 12 months;
(h) Specifies retention of penetration testing results and remediation activities results;
(i) Internal and external testing that occurs at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment); and
(j) Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

Supplemental Guidance: The testing methods must be approved by EAP Expert. A standard method for penetration testing includes:

- Pretest analysis based on full knowledge of the target system;
- Pretest identification of potential vulnerabilities based on pretest analysis; and
- Testing designed to determine exploitability of identified vulnerabilities.

EAP Expert risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.

Enhancements:

- CA-08(a) – Independent Penetration Agent or Team
- CA-08(b) – Red Team Exercises

CA-08(A): PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM

Control Objective: The organization employs an independent penetration agent or penetration team to perform penetration testing on system or system components.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are authorized to contract for independent penetration agents or a penetration team to perform penetration testing on systems or system components.

Supplemental Guidance: Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the systems that are the targets of the penetration testing.

CA-08(B): PENETRATION TESTING | RED TEAM EXERCISES

Control Objective: The organization employs "red team" exercises to simulate attempts by adversaries to compromise organizational systems in accordance with organization-defined rules of engagement.

Standard: Red team exercises:

(a) May be used to improve security awareness and training and to assess levels of security control effectiveness; and
(b) Are only authorized to be conducted by the Cybersecurity Officer (ISO) and his/her designated representatives.

Supplemental Guidance: Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises should reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of systems and organizations.

CA-09: INTERNAL SYSTEM CONNECTIONS

Control Objective: The organization:

- Authorizes internal connections of systems; and
- Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Standard: For critical systems, all internal connections must be documented and authorized.

Supplemental Guidance: This control applies to both internal (intra) and external (extra) connections including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smartphones with a specific baseline configuration.

Enhancements: None

PLANNING (PL)

Planning Policy: EAP Expert shall develop, document, implement, and periodically update measures to protect its critical systems.

Management Intent: The purpose of the Planning (PL) policy is to ensure due care planning considerations are addressed to minimize risks to EAP Expert.

Supporting Documentation: Planning (PL) control objectives & standards directly support this policy.

PL-01: SECURITY PLANNING POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[12]

- A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Processes to facilitate the implementation of the security planning policy and associated security planning controls.

Standard: EAP Expert is required to document organization-wide security planning controls that, at a minimum, include:

(a) A formal, documented security planning policy; and
(b) Processes to facilitate the implementation of the security planning policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

PL-02: SYSTEM SECURITY PLAN (SSP)

Control Objective: The organization develops a functional architecture for identifying and maintaining key architectural information on each critical system that, at a minimum, includes:[13]

- External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;
- User roles and the access privileges assigned to each role;
- Unique security requirements;
- Types of information processed, stored, or transmitted by systems and any specific protection needs in accordance with applicable local, state and Federal laws; and
- Restoration priority of information or system services.

Standard: Asset custodians and data/process owners are required to document key architectural information on each critical system that, at a minimum, includes:

(a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;
(b) User roles and the access privileges assigned to each role;
(c) Unique security requirements;
(d) Types of information processed, stored, or transmitted by systems and any specific protection needs in accordance with applicable local, state and Federal laws;
(e) Restoration priority of information or system services; and
(f) Reviewing and revising the security of their system(s) on an annual basis, or as otherwise necessary. The review process should consider, but not be limited to, the following activities:
    i. Scope, impact, and urgency of any new threat(s) to EAP Expert;
    ii. Upcoming business initiatives and their potential security risk(s);
    iii. Mergers or acquisitions that have occurred and their potential security risk(s);

[12] NIST CSF ID.AM-3
[13] NIST CSF PR.IP-7 & DE.DP-5 | MA201CMR17 17.03(2)(b)(i)

iv. New technologies that have been introduced to EAP Expert's computing environment;
v. Anticipated technologies that may be introduced into EAP Expert's computing environment;
vi. Planned system conversions; and
vii. Industry trends and recent releases of industry-recognized leading practice controls and benchmarks.

Supplemental Guidance: Security plans relate security requirements to a set of security controls and control enhancements. Security plans also define the intent of the security controls and control enhancements with regard to meeting those security requirements but do not provide descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment/selection statements in security controls and control enhancements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, and other organizations if the plan is implemented as intended.

Effective security plans make extensive use of references to policies, standards, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information is contained. This reduces the documentation requirements associated with security programs and maintains security-related information in other management and operational areas related to enterprise architecture and system development life cycle activities. For example, security plans typically do not contain detailed contingency/incident response plan information but instead provide explicitly or by reference, sufficient information in order to define what needs to be accomplished by those plans.

Enhancements:
- PL-02(a) – Plan / Coordinate with Other Organizational Entities
- PL-02(b) – Adequate Security for Covered Defense Information (CDI)

PL-02(A): System Security Plan | Plan / Coordinate with Other Organizational Entities

Control Objective: The organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.

Standard: Asset and process owners must plan and coordinate security-related activities affecting the information system potentially affected parties before conducting such activities in order to reduce the impact on other business operations.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate.

PL-02(B): System Security Plan | Adequate Security for Covered Defense Information (CDI)

Control Objective: The organization protects all unclassified information that is collected, developed, received, transmitted, used, or stored by or on behalf of the organization in support of the performance of a U.S. Department of Defense (DoD) contract. [14]

Standard: EAP Expert shall provide adequate security for all Covered Defense Information (CDI) on all covered contractor information systems that support the performance of work under any DoD contract. In terms of CDI, "adequate security" means that EAP Expert shall:

(a) Implement information systems security protections on all Covered Contractor Information Systems (CCIS) including, at a minimum:
    i. For CCIS that are part of an Information Technology (IT) service or system operated on behalf of the Government—
        1. Cloud computing services are subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services; and
        2. Any other such IT service or system (i.e., other than cloud computing) are subject to the security requirements specified elsewhere in the DoD contract; or
    ii. For CCIS that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified DFARS 252.204-7012:
        1. The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and

[14] DFARS 252.204-7012

Organizations," that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017; or

2. Alternative, but equally effective, security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD; and

(b) Apply other information systems security measures when EAP Expert reasonably determines that information systems security measures, in addition to those identified in DFARS 252.204-7012, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Supplemental Guidance: None.

PL-03: System Security Plan Update

Control Objective: The organization updates the architecture for systems.

Standard: Asset custodians and data/process owners are required to perform an annual review that, at a minimum, includes:

(a) Review the security plan for their current system; and
(b) Update the security plan to address changes to the system/environment of operation or problems identified during plan implementation or security control assessments.

Supplemental Guidance: None

Enhancements: None

PL-04: Rules of Behavior

Control Objective: The organization:[15]

- Develops usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.
- Verifies that the usage policies require acceptable uses for the technology.
- Verifies that the usage policies require acceptable network locations for the technology.
- Prohibits copy, move, and storage of sensitive data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need; and
- Establishes end-user messaging technologies restrictions.

Standard: Human Resources (HR) is responsible for developing usage policies for technologies and defining proper use of EAP Expert's technologies, ensuring:

(a) Systems can only be used after explicit approval is given by company management;
(b) User authentication must be enabled, when technically feasible;
(c) Acceptable uses of the technologies must be given; and
(d) Acceptable network locations must be clearly stated.

Supplemental Guidance: An investigation should take place when there is:

- A credible allegation or evidence of unethical or unlawful acts, fraud or gross misconduct, including but not limited to acts which could reasonably form the basis of a claim against EAP Expert for unlawful discrimination, harassment or retaliation; or
- A requirement to do so by law, regulation or policy.

Where law enforcement becomes involved in the subject of an internal investigation, EAP Expert shall cooperate with authorities consistent with its legal obligations to employees

Enhancements:

- PL-04(a) – Social Media & Social Networking Restrictions

[15] HIPAA 164.310(b) | PCI DSS 4.2, 12.3, 12.3.1, 12.3.2, 12.3.5-.6, 12.3.10 &12.4 | MA201CMR17 17.03(2)(b)(b)

PL-04(a): Rules Of Behavior | Social Media & Social Networking Restrictions

Control Objective: The organization includes in the rules of behavior, explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing system account information.

Standard: Human Resources (HR) is responsible for developing usage policies and guidance specifically for social media and social networking usage.

Supplemental Guidance: This control enhancement addresses rules of behavior related to use of social media and networking sites:

- When using such media and sites for official duties;
- When organizational information is involved in the social media/networking transactions; and
- When accessing social media /networking sites from organizational systems.

PL-05: Privacy Impact Assessment (PIA)

Control Objective: The organization conducts a privacy impact assessment on systems to evaluate privacy in systems.[16]

Standard: Asset custodians and data/process owners of new systems, systems under development, or systems undergoing major modifications are required to complete a Privacy Impact Assessment (PIA) to evaluate privacy for that system(s).

Supplemental Guidance: The PIA process does not have to be complex, but it can be complex is a business need exists. The process is designed to guide system owners and developers in assessing privacy through the early stages of development.

The PIA process is required to consist of gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval. Specifically:

- New Systems. New systems and systems under development or undergoing major modifications are required to complete a PIA.
- Legacy Systems. Legacy systems, as they exist today, do not have to complete a PIA. However, if the upgrading of these systems puts the data at risk, a PIA should be performed.
- Current Systems: Currently operational systems are not required to complete a PIA. However, if privacy is a concern, a PIA be completed.

The following websites offer examples of PIAs, with varying levels of complexity. It is up to the asset custodian and data owner to determine the proper level of complexity for the PIA:

- WISP Template 16: Privacy Impact Assessment (PIA)
- http://www.justice.gov/opcl/docs/doj-pia-template.pdf
- http://www.gsa.gov/portal/content/102237

Enhancements: None

PL-06: Security-Related Activity Planning

[Control Withdrawn – Incorporated Into PL-2]

PL-07: Security Concept Of Operations

Control Objective: The organization:

- Develops a security Concept of Operations (CONOPS) for systems containing at a minimum, how the organization intends to operate the systems from the perspective of cybersecurity; and
- Reviews and updates the CONOPS at least annually.

Standard: EAP Expert is responsible for developing and implementing a security Concept of Operations (CONOPS)

Supplemental Guidance: A COPNOPS is simply a documented understanding how EAP Expert intends to operate from the perspective of cybersecurity. The security CONOPS may be included in the security plan for the system or in other system development life cycle-related documents, as appropriate.

[16] NIST CSF ID.RA-4

Enhancements: None

PL-08: Security Architecture

Control Objective: The organization develops a cybersecurity architecture for systems that:[17]

- Describes the overall philosophy and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; and
- Describes how the security architecture is integrated into and supports the enterprise architecture.

Standard: EAP Expert is responsible for developing and implementing a security architecture process.

Supplemental Guidance: The cybersecurity architecture at the individual system level is consistent with and complements the more global, organization-wide cybersecurity architecture described in PM-07 that is integral to and developed as part of the enterprise architecture.

Enhancements: None

PL-09: Central Management

Control Objective: The organization centrally manages cybersecurity controls and related processes.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for managing cybersecurity controls and related processes.

Supplemental Guidance: Central management refers to the organization-wide management and implementation of selected cybersecurity controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring.

Enhancements: None

[17] NIST CSF ID.AM-3 & PR.IP-2

PROGRAM MANAGEMENT (PM)

Cybersecurity Program Management Policy: EAP Expert shall implement Cybersecurity program management controls to provide a foundation for EAP Expert's Cybersecurity Management System (ISMS).

Management Intent: The purpose of the Program Management (PM) policy is for EAP Expert to specify the development, implementation, assessment, authorization, and monitoring of the Cybersecurity program management. The successful implementation of security controls for organizational systems depends on the successful implementation of the organization's program management controls. The Cybersecurity Program Management (PM) controls are essential for managing the Cybersecurity program.

Supporting Documentation: Program Management (PM) control objectives & standards directly support this policy.

PM-01: CYBERSECURITY PROGRAM PLAN

Control Objective: The organization: [18]

- Develops and disseminates organization-wide cybersecurity standards that:
  - Provides an overview of the requirements for the cybersecurity program and a description of the controls in place, or planned, for meeting those requirements;
  - Provides sufficient information about controls to enable an implementation that is unambiguously compliant with the intent of the plan;
  - Includes roles, responsibilities, management commitment, and compliance;
  - Is approved by senior management with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations;
- Reviews standards for applicability; and
- Revises standards to address organizational changes and problems identified during implementation or security assessments.

Standard: EAP Expert's cybersecurity policies and standards shall be represented in a single document, the Written Cybersecurity Program (WISP) that shall be:

(a) Endorsed by executive management;
(b) Reviewed and updated at least annually; and
(c) Disseminated to the appropriate parties to ensure all EAP Expert personnel understand their applicable requirements.

Supplemental Guidance: The security plans for individual systems and the organization-wide cybersecurity program plan together, provide complete coverage for all security controls employed within the organization.

Enhancements: None

PM-02: ASSIGNED CYBERSECURITY RESPONSIBILITIES

Control Objective: The organization appoints an individual assigned with the mission and resources to coordinate, develop, implement, and maintain an organization-wide cybersecurity program.[19]

Standard: The authority and responsibility for managing the cybersecurity program are delegated to EAP Expert's Cybersecurity Officer (ISO and he/she is required to perform or delegate the following cybersecurity management responsibilities:

(a) Establish, document, and distribute security policies and procedures;
(b) Monitor and analyze security alerts and information;
(c) Distribute and escalate security alerts to appropriate personnel;
(d) Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
(e) Administer user accounts, including additions, deletions, and modifications; and

[18] HIPAA 164.308(a)(1)(i) & 164.316(a)-(b) | GLBA Sec 6801(b)(a) | PCI DSS 12.1 & 12.1.1 | MA201CMR17 17.03(1), 17.04 & 17.03(2)(b)(b) | NIST CSF ID.GV-1 & ID.GV-2 | DFARS 252.204-7008 | NY DFS 500.02 & 500.03

[19] HIPAA 164.308(a)(2) | GLBA Safeguards Rule | PCI DSS 12.5-12.5.5 | MA201CMR17 17.03(2)(a) | OR646A.622(2)(d)(A)(i) | NIST CSF ID.AM-6 & ID.GV-2 | NY DFS 500.04

(f) Monitor and control all access to data.

Supplemental Guidance: None

Enhancements: None

PM-03: Cybersecurity Resources

Control Objective: The organization addresses all capital planning and investment requests, including the resources needed to implement the cybersecurity program, and documents all exceptions to this requirement.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for managing and providing oversight for the cybersecurity-related aspects of the planning and service / tool selection process.

Supplemental Guidance: None

Enhancements: None

PM-04: Vulnerability Remediation Process

Control Objective: The organization implements a process for ensuring that vulnerabilities are properly identified, documents remediation actions and tracks vulnerabilities to mitigate risk to operations, assets, individuals, and other organizations. [20]

Standard: EAP Expert is required to use a Plan of Action & Milestones (POA&M), or some other company-approved method, as a key tool in documenting identified weaknesses, their status, and remediation steps.

Supplemental Guidance: POA&M-related issues shall be based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

Enhancements: None

PM-05: Information System Inventory

Control Objective: The organization develops and maintains an inventory of its systems. [21]

Standard: EAP Expert is required to maintain an inventory of its systems that includes, but is not limited to:

(a) A list of all such devices and personnel with access;
(b) A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices);
(c) List of company-approved products; and
(d) Update the inventory at necessary.

Supplemental Guidance: It is also possible that the owner and custodian of the hardware, software, and data are the same, but this needs to be identified and documented.

Enhancements: None

PM-06: Cybersecurity Measures of Performance

Control Objective: The organization develops, monitors, and reports on the results of cybersecurity measures of performance. [22]

Standard: The Cybersecurity Officer (ISO) is responsible for developing measures of performance or outcome-based metrics to measure the effectiveness or efficiency of the cybersecurity program and the security controls employed in support of the program.

---

[20] MA201CMR17 17.03(2)(j) | OR646A.622(2)(d)(B)(iii) | NIST CSF ID.RA-6
[21] PCI DSS 12.3.3, 12.3.4 & 12.3.7 | NIST CSF ID.AM-1 & ID.AM-2
[22] HIPAA 164.308(a)(8) | SOX Sec 404 | MA201CMR17 17.03(2)(j) | OR646A.622(2)(d)(A)(vi) & OR646A.622(2)(d)(B)(iii) | NIST CSF ID.AM-2 & PR.IP-7

Supplemental Guidance: Measures of performance are outcome-based metrics used by EAP Expert to measure the effectiveness or efficiency of the cybersecurity program and the security controls employed in support of the program.

Enhancements: None

PM-07: Enterprise Architecture

Control Objective: The organization develops an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and the resulting risk to organizational operations, organizational assets, individuals, other organizations.[23]

Standard: EAP Expert's enterprise architecture process shall be:

(a) Aligned with the industry-recognized leading practices; and
(b) Utilized in all system development and acquisition activities.

Supplemental Guidance: The integration of cybersecurity requirements and associated security controls into EAP Expert's enterprise architecture helps to ensure that security considerations are addressed early in the System Development Life Cycle (SDLC) and are directly and explicitly related to EAP Expert's mission/business processes. This also embeds into and links with the enterprise architecture, an integral cybersecurity architecture consistent with organizational risk management and cybersecurity strategies. In support of industry-recognized leading practices:

- Implementation of vendors' security best practices should be used when configuring a vendor's product unless there is a valid business or security requirement to deviate from the recommended best practices in deploying and operating those solutions; and
- If a best practice cannot be implemented, compensating controls should be addressed and documented accordingly.

Enhancements:

- PM-07(a) – Standardized Terminology

PM-07(a): Enterprise Architecture | Standardized Terminology

Control Objective: The organization uses standardized terminology to reduce confusion amongst groups and departments. [24]

Standard: EAP Expert shall use the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Cybersecurity Terms*, as the primary reference document to define common cybersecurity terms.

Supplemental Guidance: None

PM-08: Statutory, Regulatory & Contractual Compliance

Control Objective: The organization addresses cybersecurity issues in the development, documentation, implementation, and updating of a plan to protect its critical systems and sensitive data in accordance with applicable local, state, and federal laws, as well as non-regulatory requirements that the organization is contractually bound to address. [25]

Standard: Asset custodians and data/process owners are required to protect EAP Expert's critical systems and sensitive data in accordance with applicable US local, state, and Federal laws, as well as applicable international and other legal requirements that EAP Expert is contractually bound to address.

Supplemental Guidance: The requirements for defining critical infrastructure and key resources are found in applicable laws, regulations and contract requirements.

Enhancements: None

[23] PCI DSS 2.2
[24] NIST IR 7298 - http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
[25] HIPAA 164.308(a)(8) | GLBA Sec 6801(b)(c) | PCI DSS 12.1/ NV SB227 | NIST CSF ID.BE-2, ID.BE-4, ID.GV-3 & ID.RM-3

PM-09: Risk Management Strategy

Control Objective: The organization:[26]

- Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations associated with the operation and use of systems; and
- Implements that strategy consistently across the organization.

Standard: EAP Expert is required to use an organization-wide cybersecurity risk management strategy that includes:

(a) A formal risk assessment that is performed at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation);
(b) Identification of critical assets, current safeguards, effectiveness of safeguards, threats, and vulnerabilities;
(c) A review of all processes involving creating, receiving, maintaining and transmitting of sensitive data; and
(d) Assigning responsibility to validate security controls are enabled.

Supplemental Guidance: EAP Expert's cybersecurity-specific risk management strategy should include an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

Enhancements: None

PM-10: Security Authorization Process

Control Objective: The organization:

- Manages the security state of organizational systems through security authorization processes;
- Designates individuals to fulfill specific roles and responsibilities within the organization's risk management process; and
- Fully integrates the security authorization processes into an organization-wide risk management program.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for managing the state of EAP Expert's cybersecurity infrastructure.

Supplemental Guidance: Security authorization processes for systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework (RMF), and associated security standards and guidelines. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, and other organizations.

Enhancements: None

PM-11: Business Process Definition

Control Objective: The organization:[27]

- Defines business processes with consideration for cybersecurity and the resulting risk to organizational operations, organizational assets, individuals, and other organizations; and
- Determines information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Standard: Managers are required to work with asset custodians and data/process owners to formally document the established businesses processes to ensure that security considerations are addressed early in the System Development Life Cycle (SDLC), in order to integrate cybersecurity requirements and associated security controls into the enterprise architecture.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations through the compromise of information (e.g., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy.

---

[26] HIPAA 164.308(a)(1)(ii)(B) | SOX Sec 404 | GLBA Sec 6801(b)(b) | PCI DSS 12.2 | MA201CMR17 17.03(2)(b) | OR646A.622(2)(d)(A)(ii) | NIST CSF ID.GV-4, ID.RA-3, ID.RA-4, ID.RA-6, ID.RM-1, ID.RM-2 & ID.RM-3 | NY DFS 500.09

[27] NIST CSF ID.AM-6, ID.BE-3, ID.GV-4, ID.RA-4 & ID.RM-3

Enhancements: None

PM-12: Insider Threat Program

Control Objective: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.[28]

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for developing and implementing an insider threat program.

Supplemental Guidance: Organizations handling classified information are required to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of sensitive, but unclassified information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns.

Enhancements: None

PM-13: Cybersecurity Workforce

Control Objective: The organization establishes a cybersecurity workforce development and improvement program.[29]

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for developing and implementing a cybersecurity workforce development and improvement program.

Supplemental Guidance: Cybersecurity workforce development and improvement programs are complementary to organizational security awareness and training programs. Cybersecurity workforce development and improvement programs focus on developing and institutionalizing core cybersecurity capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

Cybersecurity workforce development and improvement programs include, for example:

- Defining the knowledge and skill levels needed to perform cybersecurity duties and tasks;
- Developing role-based training programs for individuals assigned cybersecurity roles and responsibilities; and
- Providing standards for measuring and building individual qualifications for incumbents and applicants for cybersecurity-related positions.

Enhancements: None

PM-14: Testing, Training & Monitoring

Control Objective: The organization:[30]

- Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational systems:
  - Are developed and maintained; and
  - Continue to be executed in a timely manner;
- Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for establishing and maintaining a process to:

(d) Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:
   i. Daily log reviews;
   ii. Firewall ruleset reviews;
   iii. Applying configuration standards to new systems;

[28] NIST CSF ID.RA-3
[29] NIST CSF PR.AT-1, PR.AT-2, PR.AT-4 & PR.AT-5 | NY DFS 500.14
[30] NIST CSF PR.IP-10, DE.DP-1, DE.DP-2, DE.DP-3 & DE.DP-5 | PCI DSS 12.11 & 12.11.1

iv. Responding to security alerts; and
v. Change management processes;

(e) Maintain documentation of quarterly review process to include:
i. Documenting results of the reviews; and
ii. Review and sign-off of results by personnel assigned responsibility for the compliance program.

Supplemental Guidance: This control ensures that oversight exists for security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. Testing, training, and monitoring plans and activities should be informed by current threat and vulnerability assessments.

Enhancements: None

PM-15: Contacts With Security Groups & Associations

Control Objective: The organization establishes and institutionalizes contact with selected groups and associations within the security community to: [31]

- Facilitate ongoing security education and training for organizational personnel;
- Maintain currency with recommended security practices, techniques, and technologies; and
- Share current security-related information including threats, vulnerabilities, and incidents.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for establishing and maintaining formal contact with selected groups and/or associations within the security community.

Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, but are not limited to, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations.

Enhancements: None

PM-16: Threat Awareness Program

Control Objective: The organization implements a threat awareness program that includes a cross-organization information-sharing capability. [32]

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for establishing and implementing a formal threat awareness program to make all personnel aware of the importance of cybersecurity.

Supplemental Guidance: Threat information sharing may be bilateral (e.g., government-commercial cooperatives, commercial-commercial cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

Enhancements: None

[31] HIPAA 164.308(a)(5)(ii) & (ii)(A) | PCI DSS 5.1.2 & 6.1 | NIST CSF ID.RA-2 & RS.CO-5 | NY DFS 500.10
[32] PCI DSS 12.6 | NIST CSF ID.RA-2, ID.RA-3 & ID.RA-5

RISK ASSESSMENT (RA)

Risk Assessment Policy: EAP Expert shall periodically assess the risk to operations, assets, and data, resulting from the operation of systems and the associated processing, storage, or transmission of data.

Management Intent: The purpose of the Risk Assessment (RA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to EAP Expert.

Supporting Documentation: Risk Assessment (RA) control objectives & standards directly support this policy.

RA-01: RISK ASSESSMENT POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates: [33]

- A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Processes to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Standard: EAP Expert is required to identify and document organization-wide security risk assessment controls that, at a minimum, include:

(a) A formal, documented security risk assessment policy; and
(b) Processes to facilitate the implementation of the security risk assessment policy, procedures, and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

RA-02: SECURITY CATEGORIZATION

Control Objective: The organization:[34]

- Categorizes systems and data in accordance with applicable local, state, and Federal laws;
- Documents the security categorization results (including supporting rationale) in the security plan for systems; and
- Ensures the security categorization decision is reviewed and approved by the asset owner.

Standard: Based on the System Criticality and Data Sensitivity of a system (see Appendix D), asset custodians and data/process owners are required to:

(a) Categorize the system and data; and
(b) Where applicable, document the security categorization results (including supporting rationale) in a System Security Plan (SSP) for the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts on organizational operations, organizational assets, and individuals if organizational information and systems are comprised through a loss of confidentiality, integrity, or availability. Security categorization processes carried out by business units, facilitates the development of inventories of information assets mappings to specific system components where information is processed, stored, or transmitted.

Enhancements: None

[33] MA201CMR17 17.03(2)(b) | NY DFS 500.09
[34] PCI DSS 9.6.1 | NIST CSF ID.AM-5, ID.RA-4 & ID.RA-5 | NY DFS 500.09

RA-03: Risk Assessment

Control Objective: The organization: [35]

- Conducts an annual assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information it processes, stores, or transmits;
- Documents risk assessment results in an organization-approved format; and
- Reviews risk assessment results.

Standard: At least once per year or upon significant changes to the networks, EAP Expert is required to conduct a formal cybersecurity risk assessment for the corporate network that, at the very least, covers the following:

(a) Identifies:
    i. Critical assets;
    ii. Potential natural and man-made threats;
    iii. Vulnerabilities;
(b) Documents known vulnerabilities in a formal risk assessment; and
(c) Assesses current cybersecurity controls affecting the confidentiality, integrity, and availability of critical data.

Supplemental Guidance: Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, and other organizations based on the operation and use of systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities).

Risk assessments (formal or informal) can be conducted at all three tiers in the risk management hierarchy (e.g., organization level, mission/business process level, or system level). RA-03 is noteworthy in that this control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework (RMF). Risk assessments can play an important role in security control selection processes particularly during the application of tailoring guidance, which includes security control supplementation.

Enhancements:

- RA-03(a) – Risk Ranking

RA-03(a): Risk Assessment | Risk Ranking

Control Objective: The organization will establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry-recognized leading practices. [36]

Standard: Asset custodians and data/process owners are required to rank vulnerabilities according to the National Vulnerability Database (NVD) Common Vulnerability Scoring System Support (CVSS) system.

Supplemental Guidance: The NVD provides severity rankings of "Low," "Medium," and "High" in addition to the numeric CVSS scores.

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

RA-04: Risk Assessment Update

Control Objective: The organization routinely updates its risk assessment and reacts accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information. [37]

Standard: EAP Expert is required to update risk assessments whenever there are significant changes to systems, the environment of operation, or other conditions that may impact the security state of the system.

Supplemental Guidance: None

Enhancements: None

---

[35] HIPAA 164.308(a)(1)(ii)(A) & (B) | GLBA Safeguards Rule | PCI DSS 12.2 | MA201CMR17 17.03(2)(b) | OR646A.622(b)(A)(ii) | NIST CSF ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, PR.IP-12, DE.AE-4 & RS.MI-3

[36] National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) http://nvd.nist.gov/cvss.cfm

[37] GLBA Safeguards Rule | PCI DSS 6.1 | MA201CMR17 17.03(2)(i) & 17.03(2)(b)(c) | OR646A.622(b)(A)(iv)

RA-05: Vulnerability Scanning

Control Objective: The organization: [38]

- Scans for vulnerabilities in systems and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting and making transparent, checklists and test procedures; and
  - Measuring vulnerability impact;
- Analyzes vulnerability scan reports and results from security control assessments;
- Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and
- Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other systems (e.g., systemic weaknesses or deficiencies).

Standard: EAP Expert's Cybersecurity personnel are responsible for the following vulnerability scanning-related activities:

(a) Perform ongoing scans for vulnerabilities in systems and hosted applications, as well as ad hoc scans when new vulnerabilities potentially affecting system(s)/application(s) are identified and reported;
(b) Utilize vulnerability scanning tools and techniques that promote:
  i. Enumerating platforms, software flaws, and improper configurations;
  ii. Formatting and making transparent, checklists and test procedures; and
  iii. Measuring vulnerability impact;
(c) Analyze vulnerability scan reports and results;
(d) Remediate legitimate vulnerabilities in accordance with a risk-based approach; and
(e) Share information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout EAP Expert to help eliminate similar vulnerabilities in other systems (e.g., systemic weaknesses or deficiencies).

Supplemental Guidance: Security categorization of systems guides the frequency and comprehensiveness of vulnerability scans. The organization determines the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches.

Enhancements:

- RA-05(a) – Update Tool Capability
- RA-05(b) – Update by Frequency / Prior to New Scan / When Identified
- RA-05(c) – Breadth / Depth of Coverage
- RA-05(d) – Privileged Access
- RA-05(e) – Automated Trend Analysis
- RA-05(f) – Review Historical Audit Logs
- RA-05(g) – External Vulnerability Assessment Scans for PCI DSS Compliance
- RA-05(h) – Internal Vulnerability Assessment Scans for PCI DSS Compliance

RA-05(a): Vulnerability Scanning | Update Tool Capability

Control Objective: The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.[39]

Standard: EAP Expert must employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

[38] PCI DSS 11.2 | OR646A.622(b)(B)(iii) & OR646A.622(b)(d(A)(iii) | NIST CSF ID.RA-1, PR.IP-12, DE.CM-8, DE.DP-4, DE.DP-5, RS.CO-3 & RS.MI-3 | NY DFS 500.04

[39] NY DFS 500.04

Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

RA-05(B): VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

Control Objective: The organization updates the information system vulnerabilities scanned according to:

- An organization-defined frequency;
- Prior to a new scan; or
- When new vulnerabilities are identified and reported.

Standard: EAP Expert must update the information system vulnerabilities scanned:

(a) Automatically (according to vendor settings);
(b) Prior to a new scan; and/or
(c) When new vulnerabilities are identified and reported.

Supplemental Guidance: None

RA-05(C): VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE

Control Objective: The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (e.g., information system components scanned and vulnerabilities checked).

Standard: EAP Expert must employ vulnerability scanning mechanisms that are capable of:

(a) Covering the appropriate scope of assets that require scanning; and
(b) Being able to identify known vulnerabilities on scanned assets.

Supplemental Guidance: None

RA-05(D): VULNERABILITY SCANNING | PRIVILEGED ACCESS

Control Objective: The information system implements privileged access authorization to organization-identified information system components for selected vulnerability scanning activities.

Standard: Where technically feasible, information systems must implement privileged access authorization for selected vulnerability scanning activities.

Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive, or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

RA-05(E): VULNERABILITY SCANNING | AUTOMATED TREND ANALYSIS

Control Objective: The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Standard: Where technically feasible, EAP Expert shall employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Supplemental Guidance: None

RA-05(F): VULNERABILITY SCANNING | REVIEW HISTORICAL AUDIT LOGS

Control Objective: The organization reviews historical audit logs to determine if a vulnerability identified in the information system has been previously exploited.

Standard: Where technically feasible, EAP Expert security personnel must review historical audit logs to determine if identified vulnerabilities were exploited on EAP Expert assets.

Supplemental Guidance: None

RA-05(G): VULNERABILITY SCANNING | EXTERNAL VULNERABILITY ASSESSMENT SCANS FOR PCI DSS COMPLIANCE

Control Objective: If required by the Payment Card Industry Data Security Standard (PCI DSS), the organization: [40]

- Performs quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).
- Verifies that the scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in the PCI DSS are resolved.

Standard: For assets within scope for PCI DSS, EAP Expert is required to perform external network vulnerability scans, via an Approved Scanning Vendor (ASV), at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all "High" vulnerabilities as defined in the PCI DSS are resolved.

Supplemental Guidance: Within PCI DSS, the term "significant change" includes, but is not limited to:

- Network topology changes;
- Firewall rule modifications; or
- Major product upgrades.

RA-05(H): VULNERABILITY SCANNING | INTERNAL VULNERABILITY ASSESSMENT SCANS FOR PCI DSS COMPLIANCE

Control Objective: If required by the Payment Card Industry Data Security Standard (PCI DSS), the organization: [41]

- Performs internal network vulnerability scans at least quarterly or after any significant change in the network (e.g., changes in network topology, firewall rule modifications, or major product upgrades).
- Verifies that the scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in the PCI DSS are resolved.

Standard: For assets within scope for PCI DSS, EAP Expert is required to perform internal network vulnerability scans at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all "High" vulnerabilities as defined in the PCI DSS are resolved.

Supplemental Guidance: Within PCI DSS, the term "significant change" includes, but is not limited to:

- Network topology changes;
- Firewall rule modifications; or
- Major product upgrades.

RA-06: TECHNICAL SURVEILLANCE COUNTERMEASURES SECURITY

Control Objective: The organization employs a technical surveillance countermeasures survey, when necessary.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are authorized to conduct or contract an outside organization to perform a technical surveillance countermeasures survey.

Supplemental Guidance: Technical surveillance countermeasures surveys are performed by qualified personnel to detect the presence of technical surveillance devices/hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities. Such surveys provide evaluations of the technical security postures through visual, electronic, and physical examinations in and about surveyed facilities. The surveys also provide useful input into risk assessments and organizational exposure to potential adversaries.

Enhancements: None

[40] PCI DSS 11.2, 11.2.2 & 11.2.3
[41] PCI DSS 11.2, 11.2.1 & 11.2.3

SYSTEM & SERVICE ACQUISITION (SA)

System & Services Acquisition Policy: EAP Expert shall allocate sufficient resources to adequately protect organizational systems by employing a System Development Life Cycle (SDLC) process that incorporate Cybersecurity considerations.

Management Intent: The purpose of the System & Services Acquisition (SA) policy is to ensure that systems employ a System Development Life Cycle (SDLC), where the security of systems and services are assessed throughout the operational life of the systems to reduce risks to EAP Expert.

Supporting Documentation: System & Service Acquisition (SA) control objectives & standards directly support this policy.

SA-01: SYSTEM & SERVICES ACQUISITION POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[42]

- A formal, documented system and services acquisition policy that includes cybersecurity considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Standard: EAP Expert is required to document organization-wide system and services acquisition controls that, at a minimum, include:

(a) A formal, documented system and services acquisition policy; and
(b) Processes to facilitate the implementation of the system and services acquisition policy, procedures, and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

SA-02: ALLOCATION OF RESOURCES

Control Objective: The organization:

- Includes a determination of cybersecurity requirements for systems in business process planning;
- Determines, documents, and allocates the resources required to protect systems as part of its capital planning and investment control process; and
- Establishes a discrete line item for cybersecurity in organizational programming and budgeting documentation.

Standard: EAP Expert is required to:

(a) Include cybersecurity requirements in business process planning; and
(b) Allocate resources required to protect its systems and data, as part of its capital planning process.

Supplemental Guidance: To apply needed security controls within the System Development Life Cycle (SDLC) (including the acquisition process), it requires a basic understanding of cybersecurity, threats, vulnerabilities, and risk to critical missions/business functions. The security engineering principles described in SA-08 cannot be properly applied if individuals that design, code, and test systems and system components (including information technology products that are used to build those systems/components) do not understand security. Therefore, EAP Expert should include qualified cybersecurity personnel in SDLC activities to ensure that security requirements are incorporated into organizational systems.

Enhancements: None

[42] NY DFS 500.11

SA-03: System Development Life Cycle (SDLC)

Control Objective: The organization:[43]

- Manages systems using a System Development Life Cycle (SDLC) methodology that includes cybersecurity considerations; and
- Defines and documents system security roles and responsibilities throughout the SDLC.

Standard: For all significant development and/or acquisitions, asset custodians and data/process owners are required to:

(a) Manage systems using a System Development Life Cycle (SDLC) that includes cybersecurity considerations; and
(b) Define and document cybersecurity roles and responsibilities throughout the SDLC.

Supplemental Guidance: The level of detail required in security-related documentation is based on the security category or classification level of the system and the degree to which organizations depend on the stated security capability to meet overall risk response expectations, as defined in the organizational risk management strategy.

Enhancements: None

SA-04: Acquisition Process

Control Objective: The organization includes the following requirements and/or specifications, explicitly or by reference, in system acquisitions based on an assessment of risk:[44]

- Security functional requirements/specifications;
- Security-related documentation requirements; and
- Developmental and evaluation-related security requirements.

Standard: Asset custodians and data/process owners are required to take security requirements into account when purchasing systems or outsourcing solutions.

Supplemental Guidance: None

Enhancements:

- SA-04(a) – Functional Properties of Security Controls
- SA-04(b) – Design & Implementation of Security Controls
- SA-04(c) – Development Methods
- SA-04(d) – Commercial Off-The-Shelf (COTS) Security Solutions
- SA-04(e) – Continuous Monitoring Plan
- SA-04(f) – Functions / Ports / Protocols / Services In Use
- SA-04(g) – Use of Approved PIV Products

SA-04(a): Acquisition Process | Functional Properties Of Security Controls

Control Objective: The organization requires, in acquisition documents, that vendors/contractors provide information describing the functional properties of the security controls to be employed within systems, system components, or system services in sufficient detail to permit analysis and testing of the controls.

Standard: Vendors are required to provide documentation describing the functional properties of the security controls employed within systems, system components, or system services in sufficient detail to permit analysis and testing of the controls.

Supplemental Guidance: Functional properties of security controls describe the functionality (e.g., security capability, functions, and mechanisms) visible at the interfaces of the controls and specifically exclude functionality and structures internal to the operation of the controls. The purpose of this control enhancement is to ensure that development processes produce a design that increases the likelihood of greater security strength.

SA-04(b): Acquisition Process | Design & Implementation of Security Controls

Control Objective: The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes detailed:

[43] NIST CSF PR.IP-2
[44] NIST CSF PR.IP-2 & DE.CM-6

- Security-relevant external system interfaces;
- High-Level Design (HLD);
- Low-Level Design (LLD);
- Source code;
- Hardware schematics; and
- Other organization-defined design/implementation information.

Standard: Developers, vendors and service providers are required to provide documentation describing the design and implementation the security controls employed within systems, system components, or system services in sufficient detail to permit analysis and testing of the controls.

Supplemental Guidance: The design and functional characteristics may be considered to be Controlled Unclassified Information (CUI) by the US Government.[45]

Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system.

SA-04(C): ACQUISITION PROCESS | DEVELOPMENT METHODS

Control Objective: The organization requires software vendors/manufacturers to demonstrate that their software development processes employ industry-recognized leading practices for secure programming, engineering methods, quality control processes, and validation techniques to minimize flawed or malformed software.

Standard: Software vendors are required to demonstrate that their software development processes employ:

(a) Industry-recognized leading practices for secure programming;
(b) Secure engineering methods;
(c) Quality control processes; and
(d) Testing processes to minimize flawed or malformed software.

Supplemental Guidance: None

SA-04(D): ACQUISITION PROCESS | COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS

Control Objective: The organization employs only Commercial Off-the-Shelf (COTS) cybersecurity products.

Standard: EAP Expert is required to use only Commercial Off-the-Shelf (COTS) products for cybersecurity requirements.

Supplemental Guidance: COTS cybersecurity products used to protect sensitive information by cryptographic means may be required to use approved key management.

SA-04(E): ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN

Control Objective: The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness.

Standard: Where technically feasible and justified by a valid business case, third-party developers of information system, system component, or information system service are required to produce a plan for the continuous monitoring of security control effectiveness.

Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations.

[45] National Archives - https://www.archives.gov/cui/registry/category-list

SA-04(F): ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

Control Objective: The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Standard: EAP Expert requires that developer of information systems, system components, or information system services to identify early in the system development life cycle, the functions, ports, protocols, and services intended that will be enabled for use in a production environment.

Supplemental Guidance: The identification of functions, ports, protocols and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented.

SA-04(G): ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

Control Objective: The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Standard: Where technically feasible, EAP Expert employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Supplemental Guidance: None

SA-05: INFORMATION SYSTEM DOCUMENTATION

Control Objective: The organization:[46]

- Obtains, protects as required, and makes available to authorized personnel, administrator documentation for systems that describes:
  - Secure configuration, installation, and operation of the system;
  - Effective use and maintenance of security features/functions; and
  - Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions; and
- Obtains, protects as required, and makes available to authorized personnel, user documentation for systems that describes:
  - User-accessible security features/functions and how to effectively use those security features/functions;
  - Methods for user interaction with systems, which enables individuals to use the system in a more secure manner; and
  - User responsibilities in maintaining the security of the information and system; and
- Documented attempts to obtain system documentation when such documentation is either unavailable or nonexistent.

Standard: Asset custodians and data/process owners are required to:

(a) Obtain administrator documentation for systems that describes:
  i. Secure configuration, installation, and operation of the system;
  ii. Effective use and maintenance of security features/functions; and
  iii. Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions;

(b) Obtain user documentation for systems that describes:
  i. User-accessible security features/functions and how to effectively use those security features/functions;
  ii. Methods for user interaction with the system, which enables individuals to use the system in a more secure manner; and
  iii. User responsibilities in maintaining the security of the information and system.

Supplemental Guidance: The purpose of this control is to help EAP Expert personnel understand the implementation and operation of security controls associated with systems. In contrast, documentation requirements in SA-04 help to ensure that system developers implement development processes that routinely produce such documentation and/or artifacts as inherent, essential

[46] NIST CSF ID.RA-1 | NY DFS 500.08

parts of those processes. Systems can include hardware, software, and firmware components. System developer is a general term that includes developers or manufacturers of information technology products (including hardware, software, and firmware), systems integrators, vendors, and product resellers.

The inability to obtain needed system documentation may occur, for example, due to the age of the systems or lack of support from developers and contractors. In those situations, organizations may need to recreate selected system documentation if such documentation is essential to the effective implementation and/or operation of security controls. The level of protection provided for selected system documentation is commensurate with the security category of the system. For example, documentation associated with a critical communications system would typically require stronger safeguards than a routine administrative system.

Enhancements:

- SA-05(a) – Functional Properties of Security Controls
- SA-05(b) – External System Interfaces
- SA-05(c) – High-Level Design
- SA-05(d) – Low-Level Design
- SA-05(e) – Source Code

SA-05(A): INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

Control Objective: The organization obtains developer documentation that describes the functional properties of the security controls employed within systems.

Standard: Developers are required to provide asset custodians documentation describing the functional properties of the security controls employed within systems, system components, or system services in sufficient detail to permit analysis and testing of the controls.

Supplemental Guidance: Functional properties of security controls describe the functionality (e.g., security functions, mechanisms) visible at the interfaces of the controls and specifically exclude functionality and structures internal to the operation of the controls.

SA-05(B): INFORMATION SYSTEM DOCUMENTATION | EXTERNAL SYSTEM INTERFACES

Control Objective: The organization obtains developer documentation that describes the security-relevant external interfaces to systems.

Standard: Developers are required to provide documentation describing external system interfaces (e.g., data connections) in sufficient detail to permit monitoring and testing.

Supplemental Guidance: None

SA-05(C): INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN

Control Objective: The organization obtains developer documentation that describes the high-level design of systems in terms of subsystems.

Standard: Developers are required to provide asset custodians documentation in sufficient detail to permit high-level analysis and an architectural review.

Supplemental Guidance: A system can be partitioned into multiple subsystems.

SA-05(D): INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN

Control Objective: The organization obtains developer documentation that describes the low-level design of systems in terms of modules.

Standard: Developers are required to provide asset custodians documentation in sufficient detail to permit detailed analysis and control testing.

Supplemental Guidance: Each subsystem within a system can contain one or more modules.

SA-05(E): INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE

Control Objective: The organization obtains the source code for custom-developed applications.

Standard: Developers are required to provide asset owners with source code for custom-developed applications.

Supplemental Guidance: Asset owners are responsible for securely maintaining the source code over the SDLC of systems / applications.

SA-06: Software Usage Restrictions

[Control Withdrawn – Incorporated Into CM-10 & SI-07]

SA-07: User-Installed Software

[Control Withdrawn – Incorporated Into CM-11 & SI-07]

SA-08: Security Engineering Principles

Control Objective: The organization applies industry-recognized leading practices engineering principles in the specification, design, development, implementation, and modification of systems.[47]

Standard: Asset custodians are required to implement configuration standards for all system components that address known security vulnerabilities and are consistent with industry-accepted system hardening standards (Appendix K: System Hardening).

Supplemental Guidance: EAP Expert applies security engineering principles primarily to new development systems or systems undergoing major upgrades. For legacy systems, security engineering principles must be applied to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example:

- Developing layered protections;
- Establishing sound security policy, architecture, and controls as the foundation for design;
- Incorporating security requirements into the system development life cycle;
- Delineating physical and logical security boundaries;
- Ensuring system developers are trained on how to build secure software;
- Tailoring security controls to meet organizational and operational needs;
- Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
- Reducing risk to acceptable levels, thus enabling informed risk management decisions.

Sources of industry-accepted system hardening standards include, but are not limited to:

- Center for Internet Security (CIS);
- International Organization for Standardization (ISO);
- SysAdmin Audit Network Security (SANS) Institute; and
- National Institute of Standards Technology (NIST)

Enhancements: None

SA-09: External Information System Services

Control Objective: If the organization outsources IT-related activities, the organization: [48]

- Conducts an organizational assessment of risk prior to the acquisition or outsourcing of services;
- Maintains and implements policies and procedures to manage service providers (e.g., Software-as-a-Service (SaaS), Web hosting companies, collocation providers, or email providers), through observation, review of policies and procedures, and review of supporting documentation. Including:
  - Maintaining a list of service providers.
  - Maintaining a written agreement that includes an acknowledgment that the service providers are responsible for the security of data the service providers possess.
  - Ensuring there is an established process for engaging service providers including proper due diligence prior to engagement.

[47] PCI DSS 2.2 | NIST CSF PR.IP-2 | NY DFS 500.08

[48] MA201CMR17 17.03(2)(f)(a) | OR646A.622(2)(d)(A)(v) | NIST CSF ID.AM-4, PR.AT-3 & DE.CM-6

- Maintains a program to monitor service providers' control compliance status at least annually.
- Requires that providers of external system services comply with organizational cybersecurity requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements;
- Defines and documents oversight and user roles and responsibilities with regard to external system services; and
- Conducts an organizational assessment of risk prior to the acquisition or outsourcing of services.

Standard: Asset custodians and data/process owners are required to:

(a) Maintain a comprehensive list of service providers, including all applicable Service Level Agreements (SLAs);
(b) Require that providers of external systems comply with EAP Expert cybersecurity requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements;
(c) Define oversight responsibilities with regard to external system services;
(d) Perform a review of the service provided for acceptable service levels;
(e) Conduct a risk assessment outsourcing of services; and
(f) Monitor security control compliance by external service providers.

Supplemental Guidance: External system services are services that are implemented outside of the authorization boundaries of EAP Expert's control. This includes services that are used by, but not a part of, EAP Expert's network. For services external to EAP Expert, a chain of trust requires that EAP Expert establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. External system services documentation includes service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Enhancements:

- SA-09(a) – Risk Assessments & Organizational Approvals
- SA-09(b) – Identification of Functions, Ports, Protocols & Services
- SA-09(c) – Business Partner Contracts
- SA-09(d) – Consistent Interests of Consumers and Providers
- SA-09(e) – Processing, Storage and Service Location
- SA-09(f) – Group Health Plans

SA-09(A): EXTERNAL INFORMATION SYSTEM SERVICES | RISK ASSESSMENTS & ORGANIZATIONAL APPROVALS

Control Objective: If the organization outsources technology-related activities, the organization:[49]

- Conducts an organizational assessment of risk prior to the acquisition or outsourcing of services;
- Maintains a list of service providers;
- Maintains and implements controls to manage security providers (e.g., backup tape storage facilities or security service providers), through observation, review of policies and procedures, and review of supporting documentation.
- Maintains a written agreement that includes an acknowledgment that service providers are responsible for the security of data the service providers possess;
- Maintains a program to monitor service providers' control compliance status, at least annually;
- Requires that providers of external system services comply with organizational cybersecurity requirements and employ appropriate security controls in accordance with all applicable laws and regulatory requirements; and
- Defines and documents oversight and user roles and responsibilities with regard to external system services.

Standard: Asset custodians and data/process owners are required to:

(a) Conduct a risk assessment outsourcing of services;
(b) Assume responsibility for any EAP Expert-owned or managed device used to connect EAP Expert's network to an external system service.
(c) Maintain a comprehensive list of service providers, including all applicable Service Level Agreements (SLAs);
(d) Require that providers of external systems comply with EAP Expert requirements and employ appropriate security controls in accordance with all applicable laws and regulatory requirements;
(e) Define oversight responsibilities with regard to external system services;
(f) Review affected client contracts/projects to determine if notification to the client is necessary if a service provider is terminated;

[49] HIPAA 164.308(a)(2)(a), 164.308(a)(4)(a) & 164.314(a) | GLBA Safeguards Rule | PCI DSS 2.4, 12.8- 12.8.4 | MA201CMR17 17.03(2)(f)(b) | OR646A.622(2)(d)(A)(v)

(g) Monitor security control compliance by external service providers; and
(h) Maintain information about which PCI DSS requirements are managed by each service provider and which are managed by EAP Expert, where applicable.

Supplemental Guidance: EAP Expert should insist on certain contract provisions with service providers that should, at a minimum, cover the following:

- Acceptable storage and transmission security controls;
- Appropriate end user training requirements;
- Breach notification procedures;
- Document destruction requirements;
- Contract performance measures;
- Contract termination process;
- Subcontractors must agree to implement equal protection measures; and
- Applicable laws and regulations.

SA-09(B): External Information System Services | Identification Of Functions, Ports, Protocols & Services

Control Objective: The organization requires asset owners to identify the functions, ports, protocols, and other services required for the use of such services.

Standard: Data/process owners, in conjunction with asset custodians, are required to develop documentation that describes the functions, ports, protocols, and services necessary for systems or applications to interact with EAP Expert's network.

Supplemental Guidance: This enables EAP Expert to maintain on-going situational awareness of the functions, ports, protocols, and services that are being employed in the system. This includes functions, ports, protocols, and services that are part of distributed systems, for example, service-oriented architectures or cloud-based systems. Such information can be useful when the need arises to understand the tradeoffs involved in blocking specific ports, protocols, or services or when requiring external service providers to do so.

SA-09(C): External Information System Services | Business Partner Contracts

Control Objective: If the organization permits a business partner to create, receive, maintain, or transmit sensitive information on the organization's behalf, the organization obtains satisfactory assurances from the business associate that appropriate safeguards are in place and enforced.[50]

Standard: EAP Expert is required to maintain written and executed agreements with business partners to ensure:

(a) Appropriate management, operational and technical control safeguards are in place to ensure the confidentiality, integrity, and availability of EAP Expert's sensitive data the business associate creates, receives, maintains, or transmits; and
(b) Service providers acknowledge in writing that they are responsible for the security of EAP Expert data (e.g., cardholder data) that the service provider possesses or otherwise stores, processes, or transmits on behalf of EAP Expert, or to the extent that they could impact the security of EAP Expert data environment.

Supplemental Guidance: Agreements, contracts, and other arrangements should specify:

- All sensitive information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- The service provider must be compliant with and maintain compliance with the protective conditions outlined in the contract;
- The service provider is liable to protect all sensitive information it stores and/or accesses;
- In the event of a security breach, due to its actions or inactions, the service provider shall bear all responsibility and expenses associated with the response to the security breach;
- The service provider must return or destroy all sensitive data received from EAP Expert, upon completion of the contract;
- Any violation of the service provider's security posture amounts to a material breach of contract and entitles EAP Expert to immediately terminate the contract without penalty;
- Auditing of the service provider's security posture and compliance is authorized at any time; and
- The contract's protective requirements shall survive any termination agreement.

Business unit management should periodically review and reevaluate the list of business partners to determine who has access to sensitive data in order to assess whether the list is complete and current.

[50] HIPAA 164.308(b)(a), 164.314(a)(1)(i)-(ii), 164.314(a)(1)(ii)(A)-(B), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(ii)(a)-(b) | PCI DSS 2.6 & 12.9

A business partner is not in compliance with cybersecurity requirements if the business partner knew of or knows of a pattern of activity or practice of the business partner that constituted a material breach or violation of its obligation under the contract or other arrangement, unless the business partner took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful.

SA-09(d): External Information System Services | Consistent Interests of Consumers and Providers

Control Objective: The organization employs security safeguards to ensure that the interests of external service providers are consistent with and reflect organizational interests.

Standard: Data/process owners are required to ensure appropriate security safeguards are implemented to ensure that the interests of external service providers are consistent with and reflect EAP Expert's interests.

Supplemental Guidance: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (e.g., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities.

SA-09(e): External Information System Services | Processing, Storage and Service Location

Control Objective: The organization restricts the location of information processing/storage based on business requirements.

Standard: Data/process owners are required to restrict the location of information processing and system services to locations, based on statutory, regulatory and/or contractual requirements.

Supplemental Guidance: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of cybersecurity breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.

SA-09(f): External Information System Services | Group Health Plans

Control Objective: If the organization sponsors a group health plan, the organization must ensure electronic Protected Health Information (ePHI) will be reasonably and appropriately safeguarded where it is created, received, maintained or transmitted.[51]

Standard: Asset custodians and data/process owners are required to ensure electronic Protected Health Information (ePHI) is reasonably and appropriately safeguarded when creating, receiving, maintaining or transmitting data on behalf of an employee, contractor or group health plan.

Supplemental Guidance: None

SA-10: Developer Configuration Management

Control Objective: The organization requires that system developers and integrators: [52]

- Perform configuration management during system design, development, implementation, and operation;
- Manage and control changes to systems;
- Implement only organization-approved changes;
- Document approved changes to systems; and
- Track security flaws and flaw resolution.

[51] HIPAA 164.314(b)(a)-(b) | PCI DSS 12.9

[52] MA201CMR17 17.03(2)(d)(B)(i) | NIST CSF PR.IP-1, PR.IP-2 & PR.IP-3

Standard: EAP Expert requires that system developers and integrators:

(a) Perform configuration management during system design, development, implementation, and operation;
(b) Manage and control changes to systems;
(c) Implement only company-approved changes;
(d) Document approved changes to systems; and
(e) Track security flaws and flaw resolution.

Supplemental Guidance: This control also applies to internal systems development and integration. System developer is a general term that includes developers or manufacturers of information technology products (including hardware, software, and firmware), systems integrators, vendors, and product resellers.

Enhancements:

- SA-10(a) – Developer Configuration Management | Software / Firmware Integrity Verification

SA-10(A): DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION

Control Objective: The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

Standard: Where technically and a business justification exists, asset owners will ensure File Integrity Monitoring (FIM) mechanisms exist and are configured to alert security personnel when unauthorized changes are made.

Supplemental Guidance: This allows EAP Expert to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

SA-11: DEVELOPER SECURITY TESTING

Control Objective: The organization requires that system developers/integrators, in consultation with associated security personnel:[53]

- Create and implement a security test and evaluation plan;
- Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- Document the results of the security testing/evaluation and flaw remediation processes.

Standard: Developers and system integrators are required to:

(a) Follow change control processes and procedures for all changes to system components that affect EAP Expert's production network;
(b) Remove test data and accounts before production systems become active / goes into production; and
(c) Ensure security functionality testing is conducted, prior to implementation.

Supplemental Guidance: The change control processes should include the following:

- Separate development/test and production environments;
- Separation of duties between development/test and production environments;
- Production data (live data) are not used for testing or development; and
- Removal of test data and accounts before production systems become active.

Security Test and Evaluation (ST&E) plans provide the specific activities that developers plan to carry out including the types of analyses, testing, and reviews of software and firmware components, the degree of rigor to be applied in the analyses, tests, and reviews, and the types of artifacts produced during those processes. Developmental security testing occurs at all post-design phases of the System Development Life Cycle (SDLC). Developer testing confirms that:

- Required security controls are implemented correctly and operating as intended; and
- The system(s) meets the established security requirements.

Enhancements:

[53] PCI DSS 6.4 & 6.4.4 | MA201CMR17 17.03(2)(d)(B)(i) | NIST CSF ID.RA-1 & PR.IP-2

- SA-11(a) – Static Code Analysis
- SA-11(b) – Threat Analysis & Flaw Remediation
- SA-11(d) – Dynamic Code Analysis

SA-11(A): DEVELOPER SECURITY TESTING | STATIC CODE ANALYSIS

Control Objective: The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.[54]

Standard: Developers and system integrators are required to perform a static code analysis of custom code prior to release to production or customers, in order to identify any potential coding vulnerability.

Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

SA-11(B): DEVELOPER SECURITY TESTING | THREAT ANALYSIS & FLAW REMEDIATION

Control Objective: The organization requires that system developers and integrators create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.[55]

Standard: Asset custodians and data/process owners are required to:

(a) Address new threats and vulnerabilities on an ongoing basis and ensures these applications are protected against known attacks by either of the following methods:
    i. Reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or
    ii. Installing an application firewall.
(b) Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:
    i. At least annually;
    ii. After any changes;
    iii. By an organization that specializes in application security;
    iv. That all vulnerabilities are corrected; and
    v. That the application is re-evaluated after the corrections

Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information technology products and systems prior to delivery are critical to the effective operation of those products and systems. Threat and vulnerability analyses at this phase of the life cycle help ensure that design or implementation changes have been accounted for and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated.

SA-11(C): DEVELOPER SECURITY TESTING | DYNAMIC CODE ANALYSIS

Control Objective: The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Standard: Developers and system integrators are required to employ dynamic code analysis tools to review custom code prior to release to production or customers, in order to identify any potential coding vulnerability.

Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data

[54] PCI DSS 6.3, 6.3.1 & 6.3.2
[55] PCI DSS 6.6

into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).

SA-12: Supply Chain Protection

Control Objective: The organization protects against supply chain threats as part of a comprehensive, defense-in-breadth cybersecurity strategy.[56]

Standard: Responsible parties within EAP Expert are required to conduct a due care review of suppliers prior to entering into contractual agreements to acquire system hardware, software, firmware, or services.

Supplemental Guidance: The scope of the due care review should cover all anticipated system components and spares over the life of the system. Systems, system components, and information technology products include hardware, software, and firmware. Supplier reviews include, for example:

- Analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support systems, products, and services; and
- Assessment of supplier training and experience in developing systems, components, products, or services with the required security capability.

These reviews provide EAP Expert with increased levels of visibility into supplier activities during the System Development Life Cycle (SDLC) to promote more effective supply chain risk management. Supplier reviews can also help determine whether primary suppliers have security safeguards in place and in practice for vetting second and third tier providers, and any other subcontractors.

Enhancements:

- SA-12(a) – Acquisition Strategies, Tools & Methods
- SA-12(b) – Supplier Reviews
- SA-12(c) – Liability From Harm
- SA-12(d) – Validate as Genuine & Not Altered
- SA-12(e) – Processes to Address Weaknesses of Deficiencies

SA-12(a): Supply Chain Protection | Acquisition Strategies, Tools & Methods

Control Objective: The organization employs tailored acquisition strategies, contract tools, and procurement methods for the purchase of systems, system components, or system service from suppliers.

Standard: For sensitive projects or for overseas locations, EAP Expert is required to tailor acquisition strategies, contract tools, and procurement methods to ensure the integrity of the system(s).

Supplemental Guidance: There are a number of different tools and techniques available, such as obscuring the end use of a system or system component, using blind or filtered buys. EAP Expert should also consider creating incentives for suppliers who:

- Implement required security safeguards;
- Promote transparency into their organizational processes and security practices;
- Provide additional vetting of the processes and security practices of subordinate suppliers, critical system components, and services;
- Restrict purchases from specific suppliers or countries; and
- Provide contract language regarding the prohibition of tainted or counterfeit components.

SA-12(b): Supply Chain Protection | Supplier Reviews

Control Objective: The organization conducts a supplier review prior to entering into a contractual agreement to acquire the system, system component, or system service.[57]

Standard: Responsible parties within EAP Expert are required to conduct supplier reviews prior to entering into a contractual agreement to acquire critical systems, system components, or system services.

[56] NIST CSF ID.BE-1 & PR.IP-2 | NY DFS 500.11

[57] NY DFS 500.11

Supplemental Guidance: Supplier reviews should include, for example:

- Analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support systems, system components, and system services; and
- Assessment of supplier training and experience in developing systems, components, or services with the required security capability.

These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and practices for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.

SA-12(C): SUPPLY CHAIN PROTECTION | LIABILITY FROM HARM

Control Objective: The organization employs security safeguards to limit harm from potential adversaries identifying and targeting the organizational supply chain.

Standard: Responsible parties within EAP Expert are required to employs safeguards to limit harm from cybersecurity threats to the supply chain.

Supplemental Guidance: Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example:

- Avoiding the purchase of custom configurations to reduce the risk of acquiring systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations;
- Employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain;
- Employing approved vendor lists with standing reputations in industry, and
- Using procurement carve outs (e.g., exclusions to commitments or obligations).

SA-12(D): SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE & NOT ALTERED

Control Objective: The organization employs security safeguards to validate those systems or system components received are genuine and have not been altered.

Standard: The responsible party for EAP Expert's technology infrastructure is required to validate critical systems or system components received are genuine and have not been altered or replaced with fraudulent versions.

Supplemental Guidance: For some system components, especially hardware, there are technical means to help determine if the components are genuine or have been altered. Security safeguards used to validate the authenticity of systems and system components include, for example, optical/nanotechnology tagging and side-channel analysis. For hardware, detailed bill of material information can highlight the elements with embedded logic complete with component and production location.

SA-12(E): SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES

Control Objective: The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

Standard: Responsible parties within EAP Expert are required to report weaknesses or deficiencies in supply chain elements as a cybersecurity incident, in accordance with the Incident Response Plan (IRP).

Supplemental Guidance: Supply chain elements may include supplier development processes and supplier distribution systems.

SA-13: TRUSTWORTHINESS

Control Objective: The organization:

- Describes the trustworthiness required in systems, system components, or system services supporting its critical missions/business functions; and
- Implements a process to achieve such trustworthiness.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for developing and implementing a process to ensure the trustworthiness of systems, system components, or system services supporting EAP Expert's critical missions/business functions.

Supplemental Guidance: This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing systems that are needed to conduct critical organizational missions/business functions. Trustworthy systems are important to mission/business success. Factors affecting the trustworthiness of systems include:

- Security functionality (e.g., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and
- Security assurance (e.g., the grounds for confidence that the security functionality is effective in its application).

Developers, implementers, operators, and maintainers of organizational systems can increase the level of trustworthiness by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings.

Enhancements: None

SA-14: Criticality Analysis

Control Objective: The organization identifies critical system components and functions by performing a criticality analysis for critical systems, system components, or system services at pre-defined decision points in the system development life cycle (SDLC).[58]

Standard: Responsible parties within EAP Expert are required to conduct criticality analysis during pre-defined decision points within the SDLC on critical system components in an effort to identify and remediate vulnerabilities.

Supplemental Guidance: Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities. System components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the system.

Enhancements: None

SA-15: Development Process, Standards & Tools

Control Objective: The organization: [59]

- Requires the developers of systems, system components, or system services to follow a documented development process that:
  - Explicitly addresses security requirements;
  - Identifies the standards and tools used in the development process;
  - Documents the specific tool options and tool configurations used in the development process; and
  - Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy security requirements.

Standard: EAP Expert requires the implementation of industry-recognized leading practices throughout the Software Development Life Cycle (SDLC):

(a) At least annually, developers are properly trained in current, secure coding techniques, including:
  i. How to avoid common coding vulnerabilities, and
  ii. Understanding how sensitive data is handled in memory; and

(b) Developers and system integrators are required to take steps to prevent common coding vulnerabilities in software development processes, to include the following:
  i. Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws;
  ii. Buffer overflow;
  iii. Insecure cryptographic storage;
  iv. Insecure communications;
  v. Improper error handling;
  vi. All “High” vulnerabilities identified in the vulnerability identification process;

[58] NIST CSF ID.AM-5, ID.BE-3, ID.BE-4, ID.BE-5, ID.RA-4 & ID.RM-3 | NY DFS 500.11
[59] PCI DSS 6.3, 6.5, 6.5.1-6.5.10 | NIST CSF PR.IP-2

vii. Cross-site scripting (XSS);
viii. Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal); and
ix. Cross-site request forgery (CSRF)

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

Enhancements:
- SA-15(a) – Use of Live Data

SA-15(A): DEVELOPMENT PROCESS, STANDARDS & TOOLS | USE OF LIVE DATA

Control Objective: The organization approves, documents, and controls the use of live data in development and test environments for the system, system component, or system service. [60]

Standard: The following "live" production data is prohibited from use in testing or development:
(a) Personally Identifiable Information (PII); and
(b) Primary Account Numbers (PANs)

Supplemental Guidance: The use of live data in preproduction environments can result in significant risk to EAP Expert. EAP Expert can minimize such risk by using test or dummy data during the development and testing of systems, system components, and system services.

SA-16: DEVELOPER-PROVIDED TRAINING

Control Objective: The organization requires the developers of systems, system components, or system services to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Standard: Developers are required to provide EAP Expert asset custodians with training on the correct use and operation of implemented security functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training.

Enhancements: None

SA-17: DEVELOPER SECURITY ARCHITECTURE & DESIGN

Control Objective: The organization requires the developers of systems, system components, or system services to produce a design specification and security architecture that:[61]
- Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;
- Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Standard: Developers are responsible for implementing security configuration standards that:
(a) Address known security vulnerabilities; and
(b) Are consistent with industry-accepted system hardening standards (Appendix K: System Hardening).

Supplemental Guidance: This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-08 is primarily directed at internal developers to help ensure that organizations develop a

[60] PCI DSS 6.4 & 6.4.3 | MA201CMR17 17.03(2)(d)(B)(i)
[61] NIST CSF PR.IP-2

cybersecurity architecture that is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when EAP Expert outsources the development of systems, system components, or system services to external entities, and there is a requirement to demonstrate consistency with EAP Expert's enterprise architecture and cybersecurity architecture.

Enhancements: None

SA-18: Tamper Resistance & Detection

Control Objective: The organization implements a tamper protection program for critical systems, system components, or system services.

Standard: The responsible party for EAP Expert's technology infrastructure is required to employ anti-tamper technologies and techniques throughout the multiple phases of the System Development Life Cycle (SDLC) including design, development, integration, operations, and maintenance.

Supplemental Guidance: Anti-tamper technologies and techniques provide a level of protection for critical systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems, components, and products during distribution and when in use.

Enhancements:

- SA-18(a) – Inspection of Information Systems, Components or Devices

SA-18(a): Tamper Resistance & Detection | Inspection of Information Systems, Components or Devices

Control Objective: The organization routinely inspects systems, system components, or devices to detect tampering. [62]

Standard: Asset custodians are required protect devices that store, process or transmit sensitive data from tampering and substitution by:

(a) Maintaining a list of authorized devices;
(b) Periodically inspecting devices to look for tampering or substitution; and
(c) Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

Supplemental Guidance: This control enhancement addresses both physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components are taken out of organization-controlled areas. Indications of the need for inspection include, for example, when individuals return from travel to high-risk locations.

SA-19: Component Authenticity

Control Objective: The organization:

- Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
- Reports counterfeit system components to law enforcement.

Standard: EAP Expert is required to perform due care and due diligence to detect and prevent counterfeits from entering into EAP Expert's networks.

Supplemental Guidance: Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include the FBI and US-CERT.

Enhancements:

- SA-19(a) – Anti-Counterfeit Training
- SA-19(b) – Component Disposal

[62] PCI DSS 9.1, 9.1.1, 9.9 & 9.9.1-9.9.3

SA-19(A): Component Authenticity | Anti-Counterfeit Training

Control Objective: The organization trains personnel to detect counterfeit system components (including hardware, software, and firmware).

Standard: Personnel who interact with systems that store, process or transmit sensitive data are required to receive training on how to detect counterfeit system components.

Supplemental Guidance: None

SA-19(B): Component Authenticity | Component Disposal

Control Objective: The organization disposes of system components using organization-defined techniques and methods.

Standard: The responsible party for EAP Expert's technology infrastructure is required to securely dispose of systems that store, process or transmit sensitive data.

Supplemental Guidance: Proper disposal of system components helps to prevent such components from entering the gray market.

SA-20: Customized Development of Critical Components

Control Objective: The organization custom develops critical system components.

Standard: Only when a strong business case exists and a risk assessment supports it are critical system components allowed to be custom developed.

Supplemental Guidance: In situations where no alternative sourcing is available and organizations choose not to re-implement or custom-developed critical system components, additional safeguards can be employed (e.g., enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.

Enhancements: None

SA-21: Developer Screening

Control Objective: The organization requires that the developers of systems, system components, or system services:

- Have appropriate access authorizations as determined by assigned duties; and
- Satisfy additional personnel screening criteria.

Standard: EAP Expert requires that developers of systems, system components, or system services satisfy all applicable screening criteria.

Supplemental Guidance: The degree of trust required of the developer may need to be consistent with that of the individuals accessing the system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed.

Enhancements: None

SA-22: Unsupported System Components

Control Objective: The organization:

- Replaces system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
- Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Standard: EAP Expert prohibits unsupported systems and system components from operating on any network, without first:

(a) Obtaining an approved waiver; and
(b) Implementing compensating controls, if applicable.

Supplemental Guidance: Support for system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components.

Enhancements:

- SA-22(a) – Alternate Sources for Continued Support

SA-22(A): UNSUPPORTED SYSTEM COMPONENTS | ALTERNATE SOURCES FOR CONTINUED SUPPORT

Control Objective: The organization provides in-house support or contracts external providers for support with unsupported system components.

Standard: EAP Expert authorizes alternate sources for support with unsupported systems and system components only if the following criteria are met:

(a) An approved waiver is obtained; and
(b) Compensating controls are implemented, if applicable.

Supplemental Guidance: This control enhancement addresses the need to provide continued support for selected system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations.

OPERATIONAL CONTROLS

Operational Controls are primarily focused on resource protection. Operational Controls generally focus on the means to control access to information and to protect the availability of that information. Management and Technical controls depend on proper Operational Controls being in place. A Management Control allowing only authorized personnel access to the data center does little good without some kind of Operational Control that addresses access.

AWARENESS & TRAINING (AT)

Awareness & Training Policy: EAP Expert shall ensure that users are made aware of the security risks associated with their roles and that users understand the applicable laws, policies, standards, and procedures related to the security of systems and data.

Management Intent: The purpose of the Awareness & Training (AT) policy is to provide guidance for broad security awareness and security training for EAP Expert users.

Supporting Documentation: Awareness & Training (AT) control objectives & standards directly support this policy.

AT-01: SECURITY AWARENESS & TRAINING POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates: [63]

- A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Standard: EAP Expert is required to document organization-wide security awareness and training controls that, at a minimum, include:

(a) A formal, documented security awareness and training policy; and
(b) Processes to facilitate the implementation of the security awareness and training policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

The security awareness and training program should include, at a minimum, the following components:

- Training goals;
- Target audience(s);
- Learning objectives;
- Deployment methods;
- Evaluation method to determine training effectiveness;
- Frequency;
- Duration;
- Deliverables or handouts; and
- Attendance tracking

Enhancements: None

AT-02: SECURITY AWARENESS

Control Objective: The organization provides basic security awareness training to all system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and thereafter as required.[64]

[63] NY DFS 500.14

[64] HIPAA 164.308(a)(5)(i) & 164.308(a)(5)(ii)(A) | PCI DSS 12.6 | MA201CMR17 17.04(8) & 17.03(2)(b)(a) | NIST CSF PR.AT-1 | NY DFS 500.14

Standard: EAP Expert's Cybersecurity personnel are responsible for developing and implementing a formal security awareness program to make all EAP Expert users aware of the importance of cybersecurity.

Supplemental Guidance: Organizations generally determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for cybersecurity and user actions to maintain security and to respond to suspected security incidents.

Enhancements:
- AT-02(a) – Practical Exercises
- AT-02(b) – Insider Threat

AT-02(A): SECURITY AWARENESS | PRACTICAL EXERCISES

Control Objective: The organization includes practical exercises in security awareness training that simulate actual cyber-attacks.

Standard: EAP Expert's Cybersecurity personnel are responsible for developing and implementing practical exercises in security awareness training that simulate actual cyber-attacks.

Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking malicious web links.

AT-02(B): SECURITY AWARENESS | INSIDER THREAT

Control Objective: The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Standard: EAP Expert's Cybersecurity personnel are required to implement security awareness training that includes how to identify and report potential indicators of insider threat.

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include concerning behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow colleagues, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, and/or practices.

AT-03: SECURITY TRAINING

Control Objective: The organization provides role-based security-related training:[65]
- Before authorizing access to the system or performing assigned duties;
- When required by system changes; and
- Annually thereafter.

Standard: For cybersecurity training:
(a) Human Resources (HR) and users' direct management shall provide initial security training to personnel upon hire; and
(b) EAP Expert's Cybersecurity personnel are required to provide training, at least annually, thereafter.

Supplemental Guidance: Initial orientation and ongoing security training should include the following topics:
- Cybersecurity basics
- Company cybersecurity policies
- Email policy
- Acceptable usage policy
- Data classification & handling
- Malicious software & spam
- Offsite security / security at home
- Wireless security
- Third party security (outsourced vendors)
- Visitor security procedures

[65] PCI DSS 12.6.1 | MA201CMR17 17.04(8) | OR646A.622(2)(d)(A)(iv) | NIST CSF PR.AT-2, PR.AT-4 & PR.AT-5 | NY DFS 500.10 & 500.14

- Incident response procedures
- Business continuity roles and procedures

Methods can vary depending on the role of the personnel and their level of access to sensitive data. For end-user training:

- All users must sign an acknowledgment form stating they have read and understood EAP Expert's requirements regarding cybersecurity policies, standards, procedures and guidelines prior to having access to EAP Expert systems or data.
- All new users must attend a security awareness training class within thirty (30) days of, being granted access to any system;
- All users shall undergo at least one (1) hour of security awareness training annually.
- All users must be provided with sufficient training and supporting reference materials to allow them to properly protect EAP Expert's systems and data; and
- EAP Expert's management must develop and maintain a communications process to be able to communicate new Cybersecurity program information, such as an informational security bulletin or email about security items of interest.

Enhancements:

- AT-03(a) – Awareness Training for Sensitive Information
- AT-03(b) – Vendor Security Training

AT-03(A): SECURITY TRAINING | AWARENESS TRAINING FOR SENSITIVE INFORMATION

Control Objective: The organization ensures that every user accessing a system processing, storing, or transmitting types of sensitive information is formally trained in handling procedures for all of the relevant types of information on the system. [66]

Standard: EAP Expert's management is required to ensure that every user accessing a system that processes, stores, or transmits sensitive information is formally trained in handling procedures for all of the relevant types of sensitive information.

Supplemental Guidance: None

AT-03(B): SECURITY TRAINING | VENDOR SECURITY TRAINING

Control Objective: The organization incorporates cybersecurity topics into all relevant vendor product, process and skills training.

Standard: EAP Expert is required to incorporate relevant security training to all employees and/or contractors that are involved in the deployment of cybersecurity-oriented solutions.

Supplemental Guidance: Training should focus on implementing best practices associated with the use of a vendor product or process. A record of this training should be saved as a log sheet or sign in sheet from the session or a certificate of completion from the vendor and documentation for specialized training should be maintained by individual supervisors.

AT-04: SECURITY TRAINING RECORDS

Control Objective: The organization: [67]

- Documents and monitors individual system security training activities including basic security awareness training and specific system security training; and
- Retains individual training records.

Standard: EAP Expert requires personnel to acknowledge in writing or electronically, at least annually, that they have read and understood EAP Expert's cybersecurity policies.

Supplemental Guidance: A record of the acknowledgment of Cybersecurity training shall be maintained by Human Resources (HR) as evidence of training.

Any security bulletins or awareness training information should be archived as evidence of training. If possible, the individuals who received training or distribution list recipients should be documented. A record of the acknowledgment of cybersecurity training shall be maintained by Human Resources (HR) as evidence of training.

Enhancements: None

[66] PCI DSS 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.9, 11.6, 12.6, 12.6.1, 12.6.2, 12.8.3 & 12.8.5, 12.10.4 | NY DFS 500.10
[67] PCI DSS 12.6.2 | NY DFS 500.14

AT-05: Security Industry Alerts & Notification Process

Control Objective: The organization establishes and institutionalizes contact with selected groups and associations within the security community:[68]

- To facilitate ongoing security education and training for organizational personnel;
- To stay up to date with the latest recommended security practices, techniques, and technologies; and
- To share current security-related information including threats, vulnerabilities, and incidents.

Standard: EAP Expert personnel responsible for incident response operations are required to subscribe to mailing lists or notification services to maintain awareness of security industry alerts.

Supplemental Guidance: There are five different mailing lists to select from the US-CERT subscription website (https://forms.us-cert.gov/maillists). However, the most applicable mailing lists are:

- Technical Cyber Security Alerts. Written for system administrators and experienced users, technical alerts provide timely information about current security issues, vulnerabilities, and exploits.
- Cyber Security Bulletins. Bulletins summarize information that has been published about new security issues and vulnerabilities for the week prior. They are published weekly and are written primarily for system administrators and other technical users.
- Cyber Security Alerts. Written for home, corporate, and new users, these alerts are published in conjunction with technical alerts when there are security issues that affect the general public.

Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations.

Enhancements: None

[68] HIPAA 164.308(a)(5)(ii) & (ii)(A) | PCI DSS 6.2

CONTINGENCY PLANNING (CP)

Contingency Planning Policy: EAP Expert shall establish, implement and maintain plans for the continuity of operations (COOP) in emergency situations to ensure the availability of critical information resources.

Management Intent: The purpose of Contingency Planning (CP) policy is to establish procedures that will help EAP Expert management to quickly determine the appropriate actions to be taken due to an interruption of service or disaster.

Supporting Documentation: Contingency Planning (CP) control objectives & standards directly support this policy.

CP-01: CONTINGENCY PLANNING POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates: [69]

- A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Standard: EAP Expert is required to document organization-wide contingency planning controls that, at a minimum, include:

(a) A formal, documented IT-specific contingency plan; and
(b) Processes to facilitate the implementation of the contingency plan, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

CP-02: CONTINGENCY PLAN

Control Objective: The organization:[70]

- Develops a contingency plan for systems that:
  - Identifies essential missions and business functions and associated contingency requirements;
  - Provides recovery objectives, restoration priorities, and metrics;
  - Addresses contingency roles, responsibilities, assigned individuals with contact information;
  - Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
  - Addresses eventual, full system restoration without deterioration of the security measures originally planned and implemented; and
  - Is reviewed and approved by designated officials within the organization;
- Distributes copies of the contingency plan to key contingency personnel;
- Coordinates contingency planning activities with incident handling activities;
- Reviews the contingency plan as required by the organization-defined frequency;
- Revises the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and
- Communicates contingency plan changes to key contingency personnel.

Standard: EAP Expert is required to establish, and implement as needed, procedures to enable the continuation of critical business processes while operating in other-than-normal conditions, that includes:

(a) Developing a contingency plan that:
  i. Identifies essential missions and business functions and associated contingency requirements;

[69] HIPAA 164.308(a)(7)(i) | 164.308(a)(7)(ii) | NIST CSF ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-5, PR.DS-4, PR.IP-7, PR.IP-9, DE.AE-4, RS.AN-2, RS.AN-4, RS.CO-1, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3
[70] HIPAA 164.308(a)(7)(ii)(C) & 164.312(a)(b)(ii)

ii. Provides recovery objectives, restoration priorities, and metrics;
iii. Addresses contingency roles, responsibilities, assigned individuals with contact information;
iv. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
v. Addresses eventual, full system restoration without deterioration of the security measures originally planned and implemented; and
vi. Is reviewed and approved by company management;

(b) Distributing copies of the contingency plan to key contingency personnel;
(c) Coordinating contingency planning activities with incident handling activities;
(d) Reviewing the contingency plan at least annually;
(e) Revising the contingency plan to address necessary changes;
(f) Communicating contingency plan changes to key contingency personnel; and
(g) Establishing procedures for obtaining access to sensitive data during other-than-normal or emergency conditions.

Supplemental Guidance: None

Enhancements:

- CP-02(a) – Coordinate with Related Plans
- CP-02(b) – Capacity Planning
- CP-02(c) – Resume Essential Missions / Business Functions
- CP-02(d) – Identify Critical Assets

CP-02(A): CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

Control Objective: The organization coordinates contingency plan development with organizational elements responsible for related plans.

Standard: Process owners must ensure coordinated contingency plan development with appropriate personnel responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

CP-02(B): CONTINGENCY PLAN | CAPACITY PLANNING

Control Objective: The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Standard: EAP Expert's management is required to conduct capacity planning so that necessary capacity for critical information processing, telecommunications, and environmental support exists during contingency operations.

Supplemental Guidance: Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber-attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

CP-02(C): CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

Control Objective: The organization plans for the resumption of essential missions and business functions within an organization-defined time period of contingency plan activation.

Standard: EAP Expert plans for the resumption of essential missions and business functions within the planned Recovery Time Objective (RTO) from the Contingency Plan.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for the resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

CP-02(D): CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

Control Objective: The organization identifies critical information system assets supporting essential missions and business functions.

Standard: Asset and process owners are required to identify critical information system assets that support essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets.

CP-03: CONTINGENCY TRAINING

Control Objective: The organization trains personnel in their contingency roles and responsibilities.[71]

Standard: Asset custodians and data/process owners are required to be trained in their contingency roles and responsibilities with respect to systems.

Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up systems at alternate processing and storage sites, and managers/senior leaders may receive more specific training on how to conduct mission essential functions in designated off-site locations and how to establish communications with other entities for purposes of coordination of contingency-related activities.

Enhancements: None

CP-04: CONTINGENCY PLAN TESTING

Control Objective: The organization tests the contingency plan for the information using organization-defined tests and/or exercises to determine the plan's effectiveness and the organization's readiness to execute the plan. [72]

Standard: Asset custodians and data/process owners are required to:

(a) Establish and implement periodic testing procedures;
(b) Test their contingency plan to determine the plan's effectiveness and the company's readiness to execute the plan; and
(c) Document the contingency plan test results.

Supplemental Guidance: Asset custodians and data/process owners are required to perform a full recovery and reconstitution of critical systems to a known state as part of contingency plan testing, at least once a year.

Enhancements:

- CP-04(a) – Coordinate with Related Plans

CP-04(A): CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

Control Objective: The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Standard: Process owners must ensure coordinated contingency plan testing with appropriate personnel responsible for related plans.

[71] NIST CSF RS.CO-1
[72] HIPAA 164.308(a)(7)(ii)(D)

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements.

CP-05: Contingency Plan Update

Control Objective: The organization reviews the contingency plan and any test/exercise results to initiates corrective actions.[73]

Standard: Asset custodians and data/process owners are required to:

(a) Review the entire contingency plan at least once a year;
(b) Review any test/exercise results; and
(c) Initiate corrective actions, as necessary.

Supplemental Guidance: None

Enhancements: None

CP-06: Alternate Storage Site

Control Objective: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of system backup information.[74]

Standard: The responsible party for EAP Expert's technology infrastructure is required to identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards, in the event of an area-wide disruption or disaster.

Supplemental Guidance: EAP Expert should determine who needs access to facilities and offices in the event of a disaster. Access should be restricted to business essential personnel until operations and facilities are returned to normal operating conditions.

- The organization ensures that the established alternate storage site is separated from the primary storage site to reduce susceptibility to the same hazards.
- The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.
- The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Enhancements:

- CP-06(a) – Separation from Primary Site
- CP-06(b) – Accessibility

CP-06(a): Alternate Storage Site | Separation from Primary Site

Control Objective: The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Standard: Asset and process owners must identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.

[73] HIPAA 164.308(a)(7)(ii)(E) | NIST CSF PR.IP-4 & PR.IP-10
[74] HIPAA 164.310(a)(b)(i) | NIST CSF PR.IP-4

CP-06(B): Alternate Storage Site | Accessibility

Control Objective: The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Standard: Asset and process owners must identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

CP-07: Alternate Processing Site

Control Objective: The organization:

- Identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards; and
- Ensures that the alternate processing site provides cybersecurity measures equivalent to that of the primary site.

Standard: The responsible party for EAP Expert's technology infrastructure is required to identify an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards, in the event of an area-wide disruption or disaster.

Supplemental Guidance: Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Alternate processing sites reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the disruption, compromise, or failure in organizational systems. Access should be restricted to business essential personnel until operations and facilities are returned to normal operating conditions.

Enhancements:

- CP-07(a) – Separation from Primary Site
- CP-07(b) – Accessibility
- CP-07(b) – Priority of Service

CP-07(A): Alternate Processing Site | Separation from Primary Site

Control Objective: The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Standard: Asset and process owners must identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.

CP-07(B): Alternate Processing Site | Accessibility

Control Objective: The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Standard: Asset and process owners must identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk.

CP-07(C): ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

Control Objective: The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Standard: EAP Expert must develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements.

Supplemental Guidance: Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.

CP-08: TELECOMMUNICATIONS SERVICES

Control Objective: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information for essential missions and business functions within the organization's defined time period when the primary telecommunications capabilities system operations are unavailable.[75]

Standard: The responsible party for EAP Expert's technology infrastructure is required to establish alternate telecommunications services, including necessary Service Level Agreement (SLA) to permit the resumption essential communication functions within an acceptable time period when the primary telecommunications capability is unavailable.

Supplemental Guidance: The responsible party for EAP Expert's technology infrastructure is required to obtain alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services.

Enhancements:

- CP-08(a) – Priority of Service Provisions
- CP-08(b) – Single Points of Failure

CP-08(A): TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

Control Objective: The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

Standard: The responsible party for EAP Expert's technology infrastructure is required to develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the business operations availability requirements.

Supplemental Guidance: None

CP-08(B): TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

Control Objective: The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Standard: EAP Expert must obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Supplemental Guidance: None

CP-09: INFORMATION SYSTEM BACKUP

Control Objective: The organization:[76]

- Conducts backups of user-level information contained in the systems;
- Conducts backups of system-level information contained in the systems;
- Conducts backups of system documentation including security-related documentation; and

[75] NIST CSF ID.BE-4 & PR.PT-4

[76] HIPAA 164.308(a)(7)(ii)(A) | NIST CSF PR.IP-4

- Protects the confidentiality and integrity of backup information at the storage location.

Standard: Asset custodians and data/process owners are responsible for:

(a) Conducting backups of user-level information contained in systems;
(b) Conducting backups of system-level information contained in systems;
(c) Conducting backups of system documentation including security-related documentation; and
(d) Protecting the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance: System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. It is necessary for orderly and efficient data backup and restoration. The individual responsible for data backups should fully document the following items for each generated data backup:

- Date of data backup;
- Type of data backup (e.g., differential, incremental, full, or copy);
- Generation (e.g., grandfather / father / son);
- Individual responsible for data backup;
- Extent of data backup (e.g., files/directories);
- Data media on which the operational data are stored;
- Data media on which the backup data are stored;
- Data backup hardware and software with version number(s);
- Data backup parameters (e.g., type of data backup etc.); and
- Storage location of backup copies.

Selecting the appropriate backup technology is a management decision. The level of risk will determine the level of data backup technologies and redundancies required. Regardless of the available technology solution, the following methods of data backup may be used:

Data Backup Methods:

- **Full**: A full backup is a backup of every file on a file system, whether that file has changed or not. The alternatives to a full backup are incremental backup and differential backup. A full backup takes longer to accomplish and requires the most storage space on the backup media, but it also provides the quickest restore times. A full backup should be performed weekly on production systems, along with daily differential or incremental backups. A full backup should also be performed before any major planned changes to a system.

- **Incremental**: An incremental backup image is a copy of all database data that has changed since the most recent, successful, full backup operation. This is also known as a cumulative backup image because a series of incremental backups taken over time will each have the contents of the previous incremental backup image. The predecessor of an incremental backup image is always the most recent successful full backup of the same object.

- **Differential (Delta):** A delta, or incremental delta, backup image is a copy of all database data that has changed since the last successful backup (full) of the data in question. This is also known as a differential, or non-cumulative, backup image. The predecessor of a delta backup image is the most recent full backup.

Depending on the available technology solution, the following procedures will be used:

Tape / Removable Hard Disk Drive (HDD) Cartridge Backups

The most commonly used tape / Hard Disk Drive (HDD) cartridge (tape) rotation schedule is called “Grandfather / Father / Son” (GFS). This rotation scheme operates on a five-day work week principle:

- “Son” tapes are for daily backups;
- “Father” tapes are for weekly backups; and
- “Grandfather” are for monthly backups

The monthly and annual tapes should be archived for storage. Daily and weekly tapes should be replaced every 6 months, due to wear and tear. The following steps show how to perform a simple GFS rotation method using 20 tapes:

- Obtain 20 tapes and label them as follows:
  - 4 daily tapes (sons) labeled “MONDAY” through “THURSDAY”
  - 4 weekly tapes (fathers) labeled “WEEK 1” through “WEEK 4”
  - 12 monthly tapes (grandfathers) labeled with the month and year
- If a full backup exceeds the capacity of one tape, create tape sets

- Beginning on a Friday, perform a full backup on the "WEEK 1" tape. Store the Week tapes off-site.
- Beginning on the following Monday, perform daily differential or incremental backups on the "MONDAY" through "THURSDAY" tapes. Store the daily backup tapes off-site.
- On Friday, perform another full backup on the "WEEK 2" tape.
- Continue with this rotation method until the last business day of the month.
- On the last business day (no matter what the day of the week it is), perform a full backup on the first monthly (grandfather) tape. Label the tape with the current date and store it off-site.

Continuous Data Protection (CDP) Backups
Continuous Data Protection (CDP), also called continuous backup or disk-to-disk (D2D), refers to backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves. It allows the user or administrator to restore data to any point in time.

CDP backups should be used in conjunction with archiving backups, such as tape or HDD cassette backups. This rationale is due to the need to have archived "snapshots" of the data in case the current and CDP data become corrupted.

Internet-Based Backups
The preferred method for data backups is through utilizing both a local copy of a backup, be it tape, HDD cassette, or CDP device, as well as an automated Internet-based data backup provider. Internet-based backups help eliminate human error associated with manually producing tape backups and can be scheduled each day, without human intervention.

Just as with traditional tape backups, care must be taken to ensure all data is captured in the backup set. Data not selected to be transmitted off-site will not be backed up remotely, so regular testing is required regardless of the backup technology used.

Enhancements:
- CP-09(a) – Testing for Reliability & Integrity
- CP-09(b) – Separate Storage for Critical Information

CP-09(A): Information System Backup | Testing for Reliability & Integrity
Control Objective: The organization tests backup information at an organization-defined frequency to verify media reliability and information integrity.

Standard: At least annually, asset owners and custodians must test backup information to verify media reliability and information integrity.

Supplemental Guidance: None

CP-09(B): Information System Backup | Separate Storage for Critical Information
Control Objective: The organization stores backup copies of critical information system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall store backup copies of critical information system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system.

Supplemental Guidance: Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.

CP-10: Information System Recovery & Reconstitution
Control Objective: The organization provides for the recovery and reconstitution of systems to a known state after a disruption, compromise, or failure.[77]

[77] HIPAA 164.308(a)(7)(ii)(B) | NIST CSF RS.RP-1 & RC.RP-1

Standard: EAP Expert's IT department is required to provide for the recovery and reconstitution of systems to a known state after a disruption, compromise, or failure. This includes but is not limited to:

a. Conducting backups;
b. Maintaining backup solutions and media; and
c. Periodically testing backup solutions to validate that successful recovery is possible.

Supplemental Guidance: Recovery is executing system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, potential system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures.

Enhancements:

- CP-10(a) – Transaction Recovery
- CP-10(b) – Failover Capability
- CP-10(c) – Backup & Restoration Hardware Protection
- CP-10(d) – Electronic Discovery
- CP-10(e) – Information System Imaging

CP-10(A): Information System Recovery & Reconstitution | Transaction Recovery

Control Objective: The organization implements transaction recovery for systems that are transaction-based.

Standard: For critical systems, asset custodians and data/process owners are required to provide for transaction recovery of systems that are transaction-based.

Supplemental Guidance: Transaction-based systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

CP-10(B): Information System Recovery & Reconstitution | Failover Capability

Control Objective: The organization provides real-time or near-real-time failover capability for systems.

Standard: For critical systems, asset custodians and data/process owners are required to provide real-time or near-real-time failover capability for critical systems.

Supplemental Guidance: None

CP-10(C): Information System Recovery & Reconstitution | Backup & Restoration Hardware Protection

Control Objective: The organization protects backup and restoration hardware and software.

Standard: For critical systems, asset custodians and data/process owners are required to provide for backup and restoration hardware and software.

Supplemental Guidance: None

CP-10(D): Information System Recovery & Reconstitution | Electronic Discovery (eDiscovery)

Control Objective: The organization provides for electronic discovery (eDiscovery) for its active and archived communication transactions.

Standard: EAP Expert's IT department is required to provide for electronic discovery (eDiscovery) for communication transactions, covering both active and archived communications data.

Supplemental Guidance: None

CP-10(E): INFORMATION SYSTEM RECOVERY & RECONSTITUTION | INFORMATION SYSTEM IMAGING

Control Objective: The organization provides the capability to reimage system components from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

Standard: EAP Expert's IT department is required to provide the capability to re-image systems from configuration-controlled and integrity-protected disk images representing a secure, operational state for the system.

Supplemental Guidance: The process of re-imaging should be used since it has several key benefits, including:

- Fast recovery time for a complete OS;
- Ability to load one image on multiple like-systems; and
- Reduces troubleshooting by being able to quickly reload an OS, while keeping data intact.

CP-11: ALTERNATE COMMUNICATIONS PROTOCOLS

Control Objective: Systems provide the capability to employ alternative communications protocols in support of maintaining continuity of operations.[78]

Standard: For critical systems, asset custodians and data/process owners are required to provide the capability to employ alternative communications protocols in support of maintaining continuity of operations.

Supplemental Guidance: Contingency plans and the associated training and testing for those plans, incorporate an alternate communications protocol capability as part of increasing the resilience of organizational systems. Alternate communications protocols include, for example, switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications, and therefore, the potential side effects of introducing alternate communications protocols are analyzed prior to implementation.

Enhancements: None

CP-12: SAFE MODE

Control Objective: Systems, when an organization-defined condition is detected, enter a safe mode of operation with organization-defined restrictions of safe mode of operation.

Standard: For critical systems, asset custodians and data/process owners are required to provide the capability to enter into a safe mode of operations.

Supplemental Guidance: The safe mode of operation, which can be activated automatically or manually, restricts the types of activities or operations systems could execute when those conditions are encountered. Restrictions includes, for example, allowing only certain functions that could be carried out under limited power or with reduced communications bandwidth.

Enhancements: None

CP-13: ALTERNATIVE SECURITY MEASURES

Control Objective: The organization employs alternative or supplemental security mechanisms for satisfying security functions when the primary means of implementing the security function is unavailable or compromised.

Standard: For critical systems, asset custodians and data/process owners are required to provide the capability to employ alternative or supplemental security mechanisms for satisfying security functions when the primary means of implementing the security function is unavailable or compromised.

Supplemental Guidance: This control supports system resiliency and contingency planning/continuity of operations. These mechanisms may be less effective than the primary mechanisms (e.g., not as easy to use, not as scalable, or not as secure). Given the cost and level of effort required to provide such alternative capabilities, this control would typically be applied only to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue to

[78] NIST CSF ID.BE-5

senior executives and system administrators one-time pads in case multifactor tokens, the EAP Expert's standard means for secure remote authentication, is compromised.

Enhancements: None

INCIDENT RESPONSE (IR)

Incident Response Policy: EAP Expert shall establish an actionable Cybersecurity incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

Management Intent: The purpose of Incident Response (IR) policy is to establish a protocol to guide EAP Expert's response to a cyber-security incident.

Supporting Documentation: Incident Response (IR) control objectives & standards directly support this policy.

IR-01: INCIDENT RESPONSE POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[79]

- A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Standard: EAP Expert is required to document organization-wide incident response controls that, at a minimum, include:

(a) A formal, documented incident response policy; and
(b) Processes to facilitate the implementation of the incident response policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

IR-02: INCIDENT RESPONSE TRAINING

Control Objective: The organization:

- Trains personnel in their incident response roles and responsibilities with respect to systems; and
- Provides refresher training.

Standard: EAP Expert management and IT staff are required to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Supplemental Guidance: Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Enhancements: None

IR-03: INCIDENT RESPONSE TESTING

Control Objective: The organization tests and/or exercises the incident response capability for systems using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results.[80]

[79] HIPAA 164.308(a)(6)(i) | NY DFS 500.16
[80] NIST CSF PR.IP-10 & RS.CO-1 | PCI DSS 12.10.2

Standard: EAP Expert management and IT staff are required to perform annual tests and/or exercises of its incident response capability to formally determine incident response effectiveness and make corrections, based on any deficiencies.

Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Enhancements:

- IR-03(a) – Coordination with Related Plans

IR-03(A): INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

Control Objective: The organization coordinates incident response testing with organizational elements responsible for related plans.

Standard: Process owners must ensure coordinated incident response testing is conducted with appropriate personnel responsible for related plans.

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

IR-04: INCIDENT HANDLING

Control Objective: The organization: [81]

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Standard: EAP Expert management and IT staff are required:

(a) Identify the severity and classification of incidents; and
(b) Define appropriate actions to take in response to ensure the continuation of business functions.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

Enhancements:

- IR-04(a) – Automated Incident Handling Processes
- IR-04(b) – Identity Theft Protection Program

IR-04(A): INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Control Objective: The organization employs automated mechanisms to support the incident handling process.

Standard: Where technically feasible, EAP Expert shall employ automated mechanisms to support the incident handling process.

[81] PCI DSS 12.5.3 | NIST CSF DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.MI-1, RS.MI-2, RS.RP-1, RC.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3 | NY DFS 500.16

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

IR-04(B): INCIDENT HANDLING | IDENTITY THEFT PROTECTION PROGRAM (ITPP)

Control Objective: The organization maintains a program to prevent identity theft from occurring.[82]

Standard: EAP Expert is required to maintain an Identity Theft Protection Program (ITPP) that is focused on preventing identity theft incidents. EAP Expert shall take precautions to detect, prevent, and mitigate identity theft through the following means:

(a) Identify relevant patterns, practices, and specific forms of activity that signal possible identity theft and incorporate those warnings into the ITPP:
    i. Alerts, notifications or warnings from a Consumer Reporting Agency;
    ii. Suspicious documents;
    iii. Suspicious personal identifying information;
    iv. Unusual use of, or suspicious activity related to, the covered account; and
    v. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.
(b) Detect Red Flags that have been incorporated into the ITPP;
(c) Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
(d) Ensure the ITPP is updated periodically to reflect changes in risks from identity theft

Supplemental Guidance: As applicable, EAP Expert staff is required to identify Red Flags that are relevant to detecting a possible risk of identity theft to customers through the following means:

- Verify the identity of persons opening accounts;
- Detect the Red Flags that the financial institution or creditor identifies as relevant in connection with the opening of an account or any existing account;
- Assess whether the Red Flags detected evidence a risk of identity theft;
- Mitigate the risk of identity theft, commensurate with the degree of risk posed;
- Train staff to implement the ITPP; and
- Oversee service provider arrangements.

Fair and Accurate Credit Transactions Act (FACTA) rules and guidelines implemented in Section 114 of FACTA specify five categories of Red Flags which illustrate the types of identity theft-related activities that need to be identified:

- Alerts, notifications or warnings from a Consumer Reporting Agency;
- Suspicious documents;
- Suspicious personal identifying information;
- Unusual use of, or suspicious activity related to, the covered account; and
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

The definition of a Red Flag is a pattern, practice, or specific activity that indicates the possible risk of identity theft. In developing Red Flag guidelines, organizations must identify patterns, practices, and specific forms of activity that indicate "the possible existence" of identity theft. In simple terms, a Red Flag must be an indicator of the possible existence of a fraud attempted or committed using the identifying information of another person without authority.

The Red Flag guidelines require each financial institution and creditor that holds any consumer account or another account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (ITPP) for combating identity theft in connection with new and existing accounts. The ITPP must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities, and be flexible to address changing identity theft risks as they arise.

IR-05: INCIDENT MONITORING

Control Objective: The organization tracks and documents system security incidents. [83]

Standard: EAP Expert management and IT staff are responsible for managing and documenting security incidents.

---

[82] Fair and Accurate Credit Transactions Act (FACTA)

[83] PCI DSS 12.5.2 | NIST CSF DE.AE-3, DE.AE-5, RS.AN-1 & RS.AN-4

Supplemental Guidance: Documenting system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Enhancements: None

IR-06: INCIDENT REPORTING

Control Objective: The organization:[84]

- Requires personnel to report suspected security incidents to organizational incident response personnel within organization-defined time-periods; and
- Reports security incident information to designated authorities.

Standard: Users are responsible for reporting system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to EAP Expert's Cybersecurity personnel.

Supplemental Guidance: If a breach occurs, breach notification procedures should occur without unreasonable delay, except:

- When a law enforcement agency has determined that notification will impede a criminal investigation; or
- In order to discover the complete scope of the breach and restore the integrity of the system.

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports and the designated reporting authorities reflect applicable laws, policies, regulations, standards, and guidance.

In terms of incident reporting, the definition of a security breach is when an individual's unencrypted Personally Identifiable Information (PII) is reasonably believed to have been acquired by an unauthorized person or process. Good faith acquisition of PII by an authorized user or authorized agent for EAP Expert purposes does not constitute a security breach, provided that the PII is not used or subject to further unauthorized disclosure.

Enhancements:

- IR-06(a) – Automated Reporting
- IR-06(b) – Cyber Incident Reporting for Covered Defense Information (CDI)

IR-06(A): INCIDENT REPORTING | AUTOMATED REPORTING

Control Objective: The organization employs automated mechanisms to assist in the reporting of security incidents.

Standard: Where technically feasible, EAP Expert shall employ automated mechanisms to assist in the reporting of security incidents.

Supplemental Guidance: None

IR-06(B): INCIDENT REPORTING | CYBER INCIDENT REPORTING FOR COVERED DEFENSE INFORMATION (CDI)

Control Objective: The organization reports cyber security incidents in a timely manner. [85]

Standard: Upon discovery of a cyber incident that affects a Covered Contractor Information System (CCIS) or the Covered Defense Information (CDI) residing therein, or that affects EAP Expert's ability to perform the requirements of the contract that are designated as operationally critical support, EAP Expert shall:

(a) Conduct a review of evidence of compromise of CDI, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts.
    i. This review shall also include analyzing CCIS(s) that were part of the cyber incident, as well as other information systems on EAP Expert's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect EAP Expert's ability to provide operationally critical support; and

[84] HIPAA 164.308(a)(6)(ii) | PCI DSS 12.8.3 | MA201CMR17 17.03(2)(j) | OR646A.604(1)-(5) | CA SB1386 SEC2-Section 1798.29 | NIST CSF RS.CO-2 | NY DFS 500.16 & 500.17

[85] DFARS 252.204-7012

ii. Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(b) The cyber incident report shall be treated as information created by or for Department of Defense (DoD) and shall include, at a minimum, the required elements at http://dibnet.dod.mil;

(c) If applicable, submit identified and contained malicious software in accordance with instructions provided by the DoD Contracting Officer;

(d) Preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least ninety (90) days from the submission of the cyber incident report to allow DoD to request the media or decline interest; and

(e) Upon request by DoD, provide DoD with:

i. Access to additional information or equipment that is necessary to conduct a forensic analysis; and

ii. All of the damage assessment information gathered.

Supplemental Guidance: None

IR-07: Incident Reporting Assistance

Control Objective: The organization provides an incident response support resource that offers advice and assistance to users of systems for the handling and reporting of security incidents.[86]

Standard: EAP Expert management and IT staff are required to establish a direct, cooperative relationship between its incident response capability and stakeholders (internal & external).

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required.

Enhancements:

- IR-07(a) – Automation Support of Availability of Information / Support
- IR-07(b) – Coordination With External Providers

IR-07(a): Incident Reporting Assistance | Automation Support of Availability of Information / Support

Control Objective: The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Standard: Where technically feasible, EAP Expert shall employ automated mechanisms to increase the availability of incident response-related information and support.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

IR-07(b): Incident Reporting Assistance | Coordination With External Providers

Control Objective: The organization:[87]

- Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
- Identifies organizational incident response team members to the external providers.

Standard: The Cyber Security Incident Response Team (CSIRT):

(a) Is EAP Expert's integrated digital security analysis team; and

(b) Designates incident response personnel to:

1. Be available on a 24/7 basis to respond to potential incidents; and
2. Assign personnel to establish and maintain direct, cooperative relationships with applicable external providers.

[86] NY DFS 500.16

[87] NY DFS 500.16

Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

IR-08: INCIDENT RESPONSE PLAN (IRP)

Control Objective: The organization: [88]

- Develops an incident response plan that:
  - Provides the organization with a roadmap for implementing its incident response capability;
  - Describes the structure and organization of the incident response capability;
  - Provides a high-level approach for how the incident response capability fits into the overall organization;
  - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
  - Defines reportable incidents;
  - Provides metrics for measuring the incident response capability within the organization.
  - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
  - Is reviewed and approved by designated officials within the organization;
- Distributes copies of the incident response plan to incident response personnel (identified by name and/or by role) and organizational elements;
- Reviews the incident response plan on an organization-defined frequency;
- Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
- Communicates incident response plan changes to incident response personnel (identified by name and/or by role) and organizational elements.

Standard: EAP Expert management and IT staff are required to:

(a) Be prepared to respond immediately to cybersecurity-related incidents;
(b) Create the Incident Response Plan (IRP) to be implemented in the event of a system breach.
(c) Test the IRP at least annually;
(d) Designate specific personnel to be available on a 24/7 basis to respond to alerts;
(e) Provide appropriate training to staff with security breach response responsibilities;
(f) Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems;
(g) Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments; and
(h) Ensure the plan addresses the following, at a minimum:
    i. Roles, responsibilities, and communication and contact strategies in the event of a compromise;
    ii. Specific incident response procedures;
    iii. Business recovery and continuity procedures;
    iv. Data backup processes;
    v. Analysis of legal requirements for reporting compromises;
    vi. Coverage and responses of all critical system components; and
    vii. Reference or inclusion of incident response procedures from legal or contractual sources, if applicable.

Supplemental Guidance: It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational systems.

National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the data and/or system.

Enhancements: None

[88] HIPAA 164.308(a)(6)(ii) | PCI DSS 12.8.3, 12.10, 12.10.1-12.10.6 | OR646A.622(2)(d)(B)(iii) | NIST CSF PR.IP-7, PR.IP-9, DE.AE-3, DE.AE-5, RS.AN-4, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.RP-1, RC.RP-1, RC.IM-1 & RC.IM-2 | NY DFS 500.16

IR-09: Information Spillage Response

Control Objective: The organization responds to information spills by:

- Identifying the specific information causing system contamination;
- Alerting organization-defined personnel of the information spill using a secure method of communication;
- Isolating the contaminated system;
- Eradicating the information from the contaminated system; and
- Identifying other systems that may have been subsequently contaminated.

Standard: EAP Expert is required to respond to information spillage in accordance with its Incident Response Plan (IRP).

Supplemental Guidance: Information spillage refers to instances where sensitive information (e.g., classified information, export controlled information) is inadvertently placed on systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to a system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system.

Enhancements:

- IR-09(a) – Responsible Personnel
- IR-09(b) – Training
- IR-09(c) – Post-Spill Operations
- IR-09(d) – Exposure to Unauthorized Personnel

IR-09(a): Information Spillage Response | Responsible Personnel

Control Objective: The organization assigns personnel or roles with responsibility for responding to information spills.

Standard: EAP Expert shall assign personnel or roles with responsibility for responding to information spills.

Supplemental Guidance: None.

IR-09(b): Information Spillage Response | Training

Control Objective: The organization provides information spillage response training at an organization-defined frequency.

Standard: Standard: EAP Expert shall provide information spillage response training at least annually.

Supplemental Guidance: None.

IR-09(c): Information Spillage Response | Post-Spill Operations

Control Objective: The organization implements procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

Standard: EAP Expert shall publish and implement procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

Supplemental Guidance: Correction actions for information systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business.

IR-09(d): Information Spillage Response | Exposure to Unauthorized Personnel

Control Objective: The organization employs security safeguards for personnel exposed to information, not within assigned access authorizations.

Standard: EAP Expert shall employ security safeguards for personnel exposed to information, not within assigned access authorizations.

Supplemental Guidance: Security safeguards include, for example, making personnel exposed to spilled information aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.

IR-10: Integrated Cybersecurity Analysis Team

Control Objective: The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel. [89]

Standard: The Computer Incident Response Team (CIRT) is EAP Expert's integrated cybersecurity analysis team.

Supplemental Guidance: Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat in order to implement defensive measures that will enable organizations to deter intrusions more effectively.

Enhancements: None

[89] PCI DSS 12.10.3 | NY DFS 500.16

MEDIA PROTECTION (MP)

Media Protection Policy: EAP Expert shall protect system media, both hardcopy and digital, by limiting access to authorized users and sanitizing or destroying media so that unauthorized data recovery is technically infeasible.

Management Intent: The purpose of the Media Protection (MP) policy is to ensure that access to both paper and digital media is limited to authorized individuals.

Supporting Documentation: Media Protection (MP) control objectives & standards directly support this policy.

MP-01: MEDIA PROTECTION POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[90]

- A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Standard: EAP Expert is required to document organization-wide media protection controls that, at a minimum, include:

(a) A formal, documented media protection policy; and
(b) Processes to facilitate the implementation of the media protection policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

MP-02: MEDIA ACCESS

Control Objective: The organization restricts access to types of digital and non-digital media authorized individuals using organization-defined security measures.[91]

Standard: Asset custodians and data/process owners are required to restrict access to digital and non-digital media to authorized individuals.

Supplemental Guidance: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls may provide adequate protection.

Enhancements:

- MP-02(a) – Automated Restricted Access
- MP-02(b) – Disclosure of Information

MP-02(A): MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS

Control Objective: The organization maps data to data/process owners and restricts access using organization-defined security safeguards.

Standard: Asset custodians and data/process owners are required to assign Role-Based Access Control (RBAC) to the specific data that is under their care or line of business to limit access to authorized personnel.

[90] HIPAA 164.308(a)(4)(ii)(B) | MA201CMR17 17.03(2)(c)
[91] HIPAA 164.308(a)(4)(ii)(C) | NIST CSF PR.PT-2

Supplemental Guidance: Data owner should review Role-Based Access Controls (RBAC) on a quarterly basis to verify only users with business justification are able to access that data.

MP-02(B): Media Access | Disclosure of Information

Control Objective: The organization limits the disclosure of information to authorized parties. [92]

Standard: EAP Expert personnel, including EAP Expert subcontractors, are prohibited from releasing any information, regardless of medium (e.g., film, tape, document), pertaining to any part of a contract or any program related to a contract to anyone outside the EAP Expert. The only exceptions are if:

(a) The project's contracting officer has given prior written approval; or
(b) The information is otherwise in the public domain before the date of release.

Supplemental Guidance: None.

MP-03: Media Marking

Control Objective: The organization marks media in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings required, if any.

Standard: EAP Expert users are required to mark media in accordance with Appendix A: Data Classification & Handling Guidelines.

Supplemental Guidance: The following labeling procedures should be followed to classify the sensitivity level of information contained within hard copy materials:

- Hard copy reports containing Confidential or Restricted information should be clearly marked on every page with an indication of the sensitivity level of the most sensitive information contained in the report, and include page numbers;
- A cover page should be attached to all documents classified as Restricted, with the Information Owner's name, date, and department; and
- Reports marked as containing Restricted information should be reviewed annually to ensure the marking is appropriate to the protection required for the information.

The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within systems (see AC-16). System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media to be publicly releasable.

Enhancements: None

MP-04: Media Storage

Control Objective: The organization: [93]

- Physically controls and securely stores digital and non-digital media within controlled areas using organization-defined security measures; and
- Protects system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Standard: EAP Expert users are required to:

(a) Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility;
(b) Review the location's security at least annually;
(c) Physically secure all media;
(d) Maintain strict control over the storage and accessibility of media; and
(e) Maintain strict control over the internal or external distribution of any kind of media, including the following:
    i. Classify media so the sensitivity of the data can be determined.
    ii. Send the media by secured courier or another delivery method that can be accurately tracked.

[92] DFARS 252.204-7000
[93] HIPAA 164.310(d)(b)(iv) | PCI DSS 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.7 & 9.9 | MA201CMR17 17.03(2)(c) | OR646A.620 & ORS646A.622(2)(d)(C)(i) | NIST CSF PR.PT-2

Supplemental Guidance: System media includes both digital and non-digital media. Digital media includes, for example:

- Portable electronic devices (e.g., laptops, tablets, smartphones, etc.);
- Diskettes;
- Magnetic tapes;
- External/removable hard drives;
- Flash drives; and
- CDs/DVDs.

Enhancements:

- MP-04(a) – Cryptographic Protection (Encrypting Data at Rest)
- MP-04(b) – Sensitive Data Inventories

MP-04(A): MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION (ENCRYPTING DATA AT REST)

Control Objective: The organization employs cryptographic mechanisms to protect information in storage on organization-defined digital media.[94]

Standard: EAP Expert users are required to render sensitive data unreadable anywhere it is stored by using strong cryptography with associated key-management processes and procedures.

Supplemental Guidance: Storage includes but is not limited to portable digital media, backup media, and in logs.

MP-04(B): MEDIA STORAGE | SENSITIVE DATA INVENTORIES

Control Objective: The organization maintains inventory logs of all sensitive media and conduct sensitive media inventories at least annually.[95]

Standard: Asset custodians and data/process owners of sensitive data are required to:

(a) Maintain an inventory log of all media; and
(b) Conduct media inventories at least annually.

Supplemental Guidance: None

MP-05: MEDIA TRANSPORTATION

Control Objective: The organization:[96]

- Protects and controls digital and non-digital media during transport outside of controlled areas using organization-defined security measures;
- Maintains accountability for system media during transport outside of controlled areas; and
- Restricts the activities associated with transport of such media to authorized personnel.

Standard: EAP Expert users are required to ensure:

(a) Digital and non-digital media is protected during transport outside of EAP Expert-controlled areas using available security measures;
(b) Management must approve any sensitive media that is moved from a secured area;
(c) Accountability is maintained for system media during transport outside of EAP Expert-controlled areas; and
(d) Activities associated with transport of sensitive media are restricted to authorized personnel.

Supplemental Guidance: System media includes both digital and non-digital media. Non-digital media includes, for example, diskettes, magnetic tapes, removable hard drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas.

Enhancements:

- MP-05(a) – Custodians

[94] PCI DSS 3.4, 3.4.1 & 9.8.2 | NY DFS 500.15
[95] PCI DSS 9.7.1
[96] HIPAA 164.310(d)(a) | PCI DSS 9.6, 9.6.2, 9.6.3 & 9.7 | MA201CMR17 17.03(2)(c) | OR646A.620 | NIST CSF PR.PT-2

- MP-05(b) – Cryptographic Protection (Encrypting Data in Storage Media)
- MP-05(c) – Ad-Hoc Transfers

MP-05(A): MEDIA TRANSPORTATION | CUSTODIANS

Control Objective: The organization employs an identified custodian throughout the transport of system media.

Standard: Data/process owners are required to ensure a dedicated custodian is identified throughout the transport of system media.

Supplemental Guidance: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

MP-05(B): MEDIA TRANSPORTATION | CRYPTOGRAPHIC PROTECTION (ENCRYPTING DATA IN STORAGE MEDIA)

Control Objective: The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.[97]

Standard: Asset custodians and data/process owners are required to employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Supplemental Guidance: This standard also applies to mobile devices. Mobile devices include

- Portable storage media:
  - USB memory sticks; and
  - External hard disk drives
- Portable computing and communications devices with storage capability:
  - Notebook computers;
  - Personal Digital Assistants (PDAs); and
  - Cellular / smart telephones.

MP-05(C): MEDIA TRANSPORTATION | AD-HOC TRANSFERS

Control Objective: The organization employs a technology-based method for securely exchanging large files with external parties.

Standard: Unscheduled, infrequent and one-time file transfers that contain sensitive data are required to be performed through encrypted transport protocols.

Supplemental Guidance: Encrypted transport protocols may include Secure FTP or HTTPS. Examples include Dropbox, Box and ShareFile for secure, large file transfer to unique recipients.

MP-06: MEDIA SANITIZATION

Control Objective: The organization:[98]

- Sanitizes system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
- Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

Standard: Media must be sanitized when it is no longer needed for business or legal reasons. EAP Expert asset custodians and data/process owners are required to destroy system media that cannot be sanitized, as follows:

(a) Shred, incinerate, or pulp hardcopy materials so that data cannot be reconstructed; or
(b) Render data on electronic media unrecoverable so that data cannot be reconstructed.

Supplemental Guidance: This control applies to all digital and non-digital media subject to disposal or reuse to include media found in devices such as scanners, copiers, and printers. The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

Enhancements:

---

[97] NY DFS 500.15

[98] HIPAA 164.310(d)(b)(i) | PCI DSS 9.8, 9.8.1 & 9.8.2 | OR646A.622(2)(d)(C)(i) & OR646A.622(2)(d)(C)(iv) | NIST CSF PR.DS-3 & PR.IP-6

- MP-06(a) – Media Sanitization Documentation
- MP-06(b) – Equipment Testing

MP-06(A): MEDIA SANITIZATION | MEDIA SANITIZATION DOCUMENTATION

Control Objective: The organization tracks, documents, and verifies media sanitization and disposal actions. [99]

Standard: Asset custodians and data/process owners are required to:

(a) Track, document, and verify media sanitization and disposal actions;
(b) Assign one individual or department responsible for coordinating data disposal and reuse of equipment; and
(c) Train staff members on the security risks associated with the reuse of equipment that stored or processed sensitive data.

Supplemental Guidance: None

MP-06(B): MEDIA SANITIZATION | EQUIPMENT TESTING

Control Objective: The organization tests sanitization equipment and procedures on an organization-defined frequency to verify that the intended sanitization is being achieved.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall test sanitization equipment and procedures, at least annually.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).

MP-07: MEDIA USE

Control Objective: The organization restricts the use of organization-defined types of digital and/or non-digital media on systems or system components using security safeguards. [100]

Standard: Asset custodians and data/process owners are required to employ technical and non-technical safeguards to restrict the insecure use of mobile computing and communications devices with information storage capability.

Supplemental Guidance: System media includes both digital and non-digital media. This control also applies to mobile computing and communications devices that include notebook computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices.

Enhancements:

- MP-07(a) – Prohibit Use Without Owner
- MP-07(b) – Limitations on Use

MP-07(A): MEDIA USE | PROHIBIT USE WITHOUT OWNER

Control Objective: The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Standard: EAP Expert prohibits the use of portable storage devices in EAP Expert-owned or managed systems when such devices have no identifiable owner.

Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).

MP-07(B): MEDIA USE | LIMITATIONS ON USE

Control Objective: The organization restricts the use and distribution of sensitive data. [101]

Standard: To protect sensitive information, including, but not limited to Controlled Technical Information (CTI) and Covered Defense Information (CDI), EAP Expert personnel shall:

[99] HIPAA 164.310(d)(b)(ii) | PCI DSS 9.7.1
[100] NIST CSF PR.PT-2
[101] DFARS 252.204-7009

(a) Only access and use sensitive information for intended purposes;
(b) Protect against unauthorized release or disclosure; and
(c) Ensure applicable third parties implement mechanisms to restrict the use and distribution of sensitive data, in accordance with EAP Expert cybersecurity requirements.

Supplemental Guidance: None

MP-08: Media Downgrading

Control Objective: The organization:

- Establishes a system media downgrading process that includes employing downgrading mechanisms with organization-defined strength and integrity;
- Ensures that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
- Identifies organization-defined system media requiring downgrading; and
- Downgrades the identified system media using the established process.

Standard: To ensure sensitive data is not inadvertently released, management approval is required to downgrade the classification of media.

Supplemental Guidance: This control applies to all system media, digital and non-digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. The downgrading of media includes redacting information to enable wider release and distribution. The downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information.

Enhancements: None

PERSONNEL SECURITY (PS)

Personnel Security Policy: EAP Expert shall ensure that published rules of behavior are followed by users and employ a method of formal sanctions for personnel who fail to comply with Cybersecurity policies and standards.

Management Intent: The purpose of the Personnel Security (PS) policy is to ensure that EAP Expert performs due care and due diligence in its personnel management of procedures.

Supporting Documentation: Personnel Security (PS) control objectives & standards directly support this policy.

PS-01: PERSONNEL SECURITY POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[102]

- A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Standard: EAP Expert is required to document organization-wide personnel security controls that, at a minimum, include:

(d) A formal, documented personnel security policy; and
(e) Processes to facilitate the implementation of the personnel security policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

PS-02: POSITION RISK DESIGNATION (POSITION CATEGORIZATION)

Control Objective: The organization:[103]

- Assigns a risk designation to all positions;
- Establishes screening criteria for individuals filling those positions; and
- Reviews and revises position risk designations.

Standard: Human Resources (HR) is responsible for assigning risk to job positions. Assigned risk is required to:

(a) Be consistent with HR policy and guidance;
(b) Include explicit cybersecurity role appointment requirements (e.g., training, responsibilities, etc.); and
(c) Prevent personnel who do not have access to sensitive data from obtaining access to sensitive data.

Supplemental Guidance: Appendix E: Cybersecurity Roles & Responsibilities provides a detailed description of Cybersecurity roles and responsibilities.

Enhancements:

- PS-02(a) – Users With Elevated Privileges
- PS-02(b) – Security-Related Positions

PS-02(A): POSITION RISK CATEGORIZATION | USERS WITH ELEVATED PRIVILEGES

Control Objective: The organization ensures that every user accessing a system processing, storing, or transmitting classified information is cleared and indoctrinated to the highest classification level of the information on the system.

Standard: EAP Expert is required to diligently manage individuals with elevated privileges through the following methods:

---

[102] NIST CSF PR.IP-11
[103] HIPAA 164.308(a)(3)(i) & (ii) & (A) | NIST CSF PR.IP-11 | PCI DSS 12.4 & 12.4.1

(a) Privileged access must be based on a legitimate need to have system access (e.g., "need to know" or "need to use"), and be re-evaluate at least annually;
(b) Users with privileged access must be provided with periodic security awareness briefings and trained to fulfill their security responsibilities; and
(c) A process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.) and immediately for individuals being separated for adverse reasons just prior to notifying them of the pending action.

Supplemental Guidance: Managers should ensure that all personnel with elevated privileges take at least one (1) contiguous week of vacation annually since studies have found that mandatory vacations:

- Prevent workers from concealing fraud or other illegal or abusive acts; and
- Serve to alleviate stress, helping them maintain the level of diligence needed to perform their job functions.

PS-02(b): Position Risk Categorization | Security-Related Positions

Control Objective: The organization ensures that all security-related positions are staffed by qualified individuals and those individuals have the skill set necessary to perform the cybersecurity-related job functions.[104]

Standard: EAP Expert is required to assess individual skill sets for all individuals that are responsible for cybersecurity functions. Only individuals meeting or exceeding EAP Expert's cybersecurity skills requirement are allowed to perform cybersecurity-related functions.

Supplemental Guidance: None

PS-03: Personnel Screening

Control Objective: The organization:[105]

- Screens individuals prior to authorizing access to the system; and
- Rescreens individuals, if necessary, based on organizational concerns.

Standard: Human Resources (HR) is responsible for screening potential personnel prior to hiring in an effort to minimize the risk of compromise from internal sources.

Supplemental Guidance: Approved methods of screening procedures include:

- Previous employment history verification;
- Criminal history record check;
- Department of Motor Vehicles (DMV) history check;
- Credit history; and
- Personal/professional reference checks.

Enhancements:

- PS-03(a) – Information With Special Protection Measures

PS-03(a): Personnel Screening | Information With Special Protection Measures

Control Objective: The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

- Have valid access authorizations that are demonstrated by assigned official government duties; and
- Satisfy organization-defined additional personnel screening criteria.

Standard: EAP Expert management is required to ensure authorized users meet personnel screening criteria.

Supplemental Guidance: Organizational information requiring special protection includes, for example, Controlled Unclassified Information (CUI) and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.

[104] NY DFS 500.10
[105] HIPAA 164.308(a)(3)(ii) & (B) | PCI DSS 12.7 | NIST CSF PR.DS-5 & PR.IP-11

PS-04: Personnel Termination

Control Objective: The organization, upon termination of individual employment:[106]

- Terminates system access;
- Conducts exit interviews;
- Retrieves all security-related organizational system-related property; and
- Retains access to organizational information and systems formerly controlled by the terminated individual.

Standard: EAP Expert is required to ensure that upon termination of an individual's employment:

(a) System access accounts are disabled with twenty-four (24) hours of the termination action;
(b) Exit interviews are conducted, if possible;
(c) All company-related property is recovered; and
(d) All company-owned information the terminated employee was responsible for is identified and accounted for.

Supplemental Guidance: The objective of this control is to remove user access as soon as possible. If a user resigns or is terminated, the following should be accomplished as soon as possible, but no longer than twenty-four (24) hours from notification of a change in a user's status:

- The user's privileges and access must be revoked;
- The user's passwords must be changed or the accounts disabled to preclude access;
- All shared passwords known by the user on all applicable systems must be changed;
- All privileged account passwords known by the user must be changed;
- Incoming mail for the user should be re-directed as directed by the user's supervisor;
- After thirty (30) days, incoming mail should be disabled for the account, unless deemed necessary;
- All files owned by the user should be identified and either archived or changed to a valid user;
- All automated scripts/ batch jobs previously requested or previously submitted should be reviewed; and
- All EAP Expert property should be collected, including but not limited to:
    - Keys, lock combinations and identification badges;
    - Sensitive data and documentation;
    - Operator procedures;
    - Program documentation;
    - Company-owned equipment, pagers, notebook computers and tools; and
    - Phone contact lists.

Enhancements:

- PS-04(a) – Asset Collection
- PS-04(b) – High-Risk Terminations

PS-04(a): Personnel Termination | Asset Collection

Control Objective: The organization, upon termination of individual employment, ensures for the collection of organization-owned assets prior to the individual's departure.

Standard: The direct manager of a terminated user is responsible for inventorying and accounting for all EAP Expert-issued assets, prior to the individual's departure.

Supplemental Guidance: Depending on applicable labor laws, this may require withholding the final paycheck from the terminated individual until the company-issued assets are returned. Human Resources must be informed of any missing or damaged company assets that were the responsibility of the terminated individual.

PS-04(b): Personnel Termination | High-Risk Terminations

Control Objective: The organization, upon termination of an individual deemed to be a "high risk" to the organization, ensures for the expedited process of removing the individual's access to organizational systems and data.

Standard: Human Resources (HR) is required to immediately notify EAP Expert's Cybersecurity personnel to revoke the user's IDs, privileges, and authorizations for a "high risk" employee or contractor termination.

Supplemental Guidance: The objective of this control is to remove the user's access without delay. If the situation warrants it, a backup or image of the individual's systems (e.g., workstation, laptop, smart phone, etc.) may be required. If a backup is intended

[106] HIPAA 164.308(a)(3)(ii) & (C) | PCI DSS 9.3 | MA201CMR17 17.03(2)(e) | NIST CSF PR.IP-11

for possible punitive action against the individual, the backup must be in accordance with forensic investigation procedures to ensure chain of custody and unassailable data copies.

PS-05: Personnel Transfer

Control Objective: The organization reviews logical and physical access authorizations to systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates organization-defined transfer or reassignment actions within an organization-defined time period following the formal transfer action.[107]

Standard: EAP Expert managers are required to:

(a) Review the logical and physical access authorizations to systems/facilities when personnel are reassigned or transferred to other positions within the company; and
(b) Initiate company-defined transfer or reassignment actions within seven (7) days following the formal transfer action.

Supplemental Guidance: None

Enhancements: None

PS-06: Access Agreements

Control Objective: The organization:[108]

- Ensures that individuals requiring access to organizational information and systems sign appropriate access agreements prior to being granted access; and
- Reviews/updates the access agreements.

Standard: EAP Expert is required to ensure that access to information with special protection measures is granted only to individuals who:

(a) Have a valid access authorization; and
(b) Satisfy associated personnel security criteria.

Supplemental Guidance: Prior to granting any access to EAP Expert systems or data, a Non-Disclosure Agreement (NDA) should be signed by the employee, contractor, service provider or partner requiring access. This NDA should be maintained on-file, in accordance with document retention guidelines.

Enhancements: None

PS-07: Third-Party Personnel Security

Control Objective: The organization:[109]

- Establishes personnel security requirements including security roles and responsibilities for third-party providers;
- Documents personnel security requirements; and
- Monitors provider compliance.

Standard: EAP Expert is required to ensure third-party personnel access is granted only to individuals who:

(a) Have a valid access authorization;
(b) Satisfy associated personnel security criteria;
(c) Have read, understand, and signed a Non-Disclosure Agreement (NDA); and
(d) Have read, understand, and signed an acknowledgment that he or she understands and will abide by EAP Expert's policies, procedures, standards, and guidelines.

Supplemental Guidance: None

Enhancements: None

---

[107] NIST CSF PR.IP-11
[108] HIPAA 164.308(a)(4)(i) | NIST CSF PR.DS-5 & PR.IP-11
[109] NIST CSF ID.AM-6, ID.GV-2, PR.AT-3 & PR.IP-11

PS-08: Personnel Sanctions

Control Objective: The organization employs a formal sanctions process for personnel failing to comply with established cybersecurity policies and procedures. [110]

Standard: Human Resources (HR) is required to manage and operate its personnel sanctions process consistent with applicable laws, regulations, policies and standards.

Supplemental Guidance: The personnel sanctions process is included as part of the general personnel policies and procedures managed by EAP Expert HR. EAP Expert reserves the right to examine its property at any time, including property in the possession, control, custody of or in use by any employee. EAP Expert may utilize a tiered structure of sanctions that takes into consideration the magnitude of harm caused by the actions or inactions of the individual under sanction.

EAP Expert may utilize a tiered structure of sanctions that takes into consideration the magnitude of harm caused by the actions or inactions of the individual under sanction.

Enhancements:

- PS-08(a) – Workplace Investigations

PS-08(a): Personnel Sanctions | Workplace Investigations

Control Objective: The organization establishes guidelines for employee misconduct investigations.[111]

Standard: EAP Expert is required to follow established guidelines for employee misconduct investigations:

(a) All applicable laws concerning misconduct investigations will be adhered to;
(b) Employees who become the subject of an internal investigation will be treated with dignity and respect, and will be provided with timely information about the outcome of the investigation, although EAP Expert reserves the right to restrict access to the investigation report and related documentation; and
(c) Communications and work products relative to an investigation will be limited to parties with a legitimate need to know.

Supplemental Guidance: The Federal Trade Commission (FTC) requires that when an employer investigates an employee's conduct on the job, including investigations of employee misconduct, the Fair Credit Reporting Act (FCRA) governs. However, the FCRA does not apply to investigations conducted by EAP Expert's in-house personnel. In addition, FCRA does not apply when a third-party, who is not in the business of providing such reports, does the investigation (e.g., contractors who do such investigations, but not as their principal business).

If EAP Expert uses a third-party to investigate an employee, the employee shall be notified "clearly and conspicuously" in writing. Employees must give their permission to have the investigative consumer report completed. If EAP Expert disciplines the employee based upon the report, EAP Expert is required to provide the employee with:

- Notice of the disciplinary action;
- Name, address and phone number of the third-party that furnished the report; and
- A free copy of the report and can request EAP Expert to state why the discipline was taken.

These investigations may be conducted by a third-party if EAP Expert suspects a user of:

- Misconduct relating to employment;
- A violation of local, state, Federal, or international laws or regulations;
- A violation of any preexisting, written EAP Expert policy; or
- Noncompliance with the rules of a self-regulatory organization.

[110] HIPAA 164.308(a)(1)(ii)(C) | MA201CMR17 17.03(2)(d) | NIST CSF PR.IP-11
[111] Fair & Accurate Credit Transaction Act (FACTA) | Fair Credit Reporting Act (FCRA)

PHYSICAL & ENVIRONMENTAL PROTECTION (PE)

Physical & Environmental Protection Policy: EAP Expert shall implement or require physical access controls to limit access to systems, equipment, and the respective operating environments to authorized individuals. EAP Expert shall provide appropriate environmental controls in facilities containing systems. When applicable, this policy only applied to EAP Expert systems used for online services at designated third party hosting facilities.

Management Intent: The purpose of the Physical & Environmental Protection (PE) policy is to minimize risk to EAP Expert systems and data by addressing applicable physical security and environmental concerns.

Supporting Documentation: Physical & Environmental Protection (PE) control objectives & standards directly support this policy.

PE-01: PHYSICAL & ENVIRONMENTAL PROTECTION POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[112]

- A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Standard: EAP Expert is required to document organization-wide physical and environmental controls that, at a minimum, include:

(a) A formal, documented physical and environmental policy; and
(b) Processes to facilitate the implementation of the physical and environmental policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

PE-02: PHYSICAL ACCESS AUTHORIZATIONS

Control Objective: The organization: [113]

- Develops and keeps current a list of personnel with authorized access to the facility where the system resides (except for those areas within the facility officially designated as publicly accessible);
- Issues authorization credentials; and
- Reviews and approves the access list and removes from the access list personnel no longer requiring access.

Standard: EAP Expert is required to:

(a) Develop and keeps current a list of personnel with authorized access to its facilities, except for those areas within the facility officially designated as publicly accessible;
(b) Issue authorization credentials for physical access; and
(c) Review and approve the access list and remove personnel no longer requiring access.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including the level of forge-proof badges, smart cards, or identification cards) consistent with standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.

Enhancements:

- PE-02(a) – Role-Based Physical Access

[112] HIPAA 164.310(a)(a)
[113] HIPAA 164.310(a)(b)(ii) | PCI DSS 9.2 | NIST CSF PR.AC-2

- PE-02(b) – Identification Requirement
- PE-02(c) – Restrict Unescorted Access

PE-02(A): PHYSICAL ACCESS AUTHORIZATIONS | ROLE-BASED PHYSICAL ACCESS

Control Objective: The organization authorizes physical access to the facility where the system resides, based on the position or role of a user. [114]

Standard: EAP Expert is required to authorize physical access to its facilities based on position or role.

Supplemental Guidance: EAP Expert should restrict physical access to systems that process sensitive information to authorized personnel with the appropriate roles and access authorizations. Roles for physical access include, but are not limited to:

- Employees
- Contractors
- Vendors
- Partners
- Guests
- Maintenance Personnel
- Cleaning / Janitorial

PE-02(B): PHYSICAL ACCESS AUTHORIZATIONS | IDENTIFICATION REQUIREMENT

Control Objective: The organization requires at least one form of government-issued photo identification to gain access to the facility where the system resides. [115]

Standard: EAP Expert requires at least one (1) form of government-issued photo identification to gain access.

Supplemental Guidance: Acceptable forms of government photo identification include, for example:

- Passports;
- Personal Identity Verification (PIV) cards; and
- Drivers' licenses.

In the case of gaining access to facilities using automated mechanisms, organizations may use personal identity verification cards, key cards, PINs, and biometrics.

PE-02(C): PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

Control Objective: The organization restricts unescorted access to the facility where the system resides to personnel with required security clearances, formal access authorizations, and validated the need for access. [116]

Standard: EAP Expert is required to restrict physical access to the systems equipment and records storage.

Supplemental Guidance: None

PE-03: PHYSICAL ACCESS CONTROL

Control Objective: The organization:[117]

- Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the system resides (excluding those areas within the facility officially designated as publicly accessible);
- Verifies individual access authorizations before granting access to the facility;
- Controls entry to the facility containing the system using physical access devices and/or guards;
- Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
- Secures keys, combinations, and other physical access devices; and
- Changes combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

---

[114] HIPAA 164.310(a)(b)(iii)
[115] PCI DSS 9.4 & 9.4.1
[116] PCI DSS 9.3
[117] HIPAA 164.310(a)(b)(iv) | PCI DSS 9.1, 9.1.1, 9.1.2, 9.2, 9.4.2 & 9.4.3 | MA201CMR17 17.03(2)(g) | OR646A.622(2)(d)(C)(ii) | NIST CSF PR.AC-2, DE.CM-2, DE.CM-7 & DE.DP-3

Standard: EAP Expert is required to:

(a) Use video cameras and/or access control mechanisms to limit and monitor physical access to the facility and systems;
(b) Enforce physical access authorizations for all physical access points (including designated entry/exit points) to company-owned or operated facilities;
(c) Verify individual access authorizations before granting access to the facility;
(d) Control access to areas based on the physical security zone requirements;
(e) Secure keys, combinations, and other physical access devices;
(f) Change combinations and keys and when keys are lost, when combinations are compromised, or when individuals are transferred or terminated; and
(g) Issue visitors a physical token (e.g., a badge or access device) that:
    i. Identifies the visitors as not onsite personnel;
    ii. Must be surrendered before leaving the facility or at the date of expiration; and
    iii. Expires through automated or visual means (e.g., different color for each day)

Supplemental Guidance: EAP Expert should perform physical penetration testing, includes unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility. This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, isolating selected systems/components in secured areas. Components of systems (e.g., workstations, computer terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

Enhancements:

- PE-03(a) – Lockable Physical Casings
- PE-03(b) – Laptop Storage In Automobiles
- PE-03(c) – Workstation Security
- PE-03(d) – Physical Access Logs

PE-03(A): Physical Access Control | Lockable Physical Casings

Control Objective: The organization uses lockable physical casings to protect organization-defined system components from unauthorized physical access.

Standard: EAP Expert is required to protect sensitive systems from physical tampering or alteration of hardware components by utilizing lockable physical casings.

Supplemental Guidance: Lockable physical casings are primarily associated with rack-mounted hardware.

PE-03(B): Physical Access Control | Laptop Storage In Automobiles

Control Objective: The organization requires protection of mobile systems away from organizational premises.

Standard: When traveling with EAP Expert-issued laptops and mobile devices, users are required to:

(a) Lock the device(s) in the trunk of a user's automobile; or
(b) Maintain physical control and not leave the device(s) in the automobile.

Supplemental Guidance: A EAP Expert laptop or other mobile devices must never be left in the passenger compartment of an unattended vehicle.

The primary concern with storage in a vehicle's trunk is damage due to extreme temperature. The average storage temperature range for laptop computers is -40 degrees Fahrenheit to +140 degrees Fahrenheit, so if the trunk exceeds this temperature range, the device should not be left in the vehicle for risk of damage to both the device and the automobile.

PE-03(C): Physical Access Control | Workstation Security

Control Objective: The organization requires protection of workstations to restrict access to authorized users.

Standard: EAP Expert requires the following workplace security precautions:

(a) Physical media must be properly disposed of, in accordance with document destruction policies;
(b) All work areas must be cleared of all media containing sensitive data when not occupied;
(c) Filing cabinets, lockable drawers / overhead cabinets, storage rooms, and any other storage unit containing sensitive data will be locked when not in use; and
(d) Whiteboards, dry-erase boards, cork boards, writing tablets, and similar common shared work areas will be sanitized (e.g., erased, removed, or shredded) when not in use.

Supplemental Guidance: Physical security zones should be used to determine which areas are more vulnerable to unauthorized use, theft, or viewing of data and appropriate physical safeguards should be implemented.

PE-03(D): PHYSICAL ACCESS CONTROL | PHYSICAL ACCESS LOGS

Control Objective: The physical access control system generates a log entry for each access.

Standard: EAP Expert is required to configure access control systems to log the following information:
(a) Physical location of the access;
(b) Direction of access, if possible (e.g., ingress or egress);
(c) Identity of the person accessing the location; and
(d) Indication of success or failure.

Supplemental Guidance: Access control systems include card / badge readers and keypad readers.

PE-04: ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control Objective: The organization controls physical access to system distribution and transmission lines within organizational facilities.[118]

Standard: EAP Expert management is required to limit physical access to transmission medium to only authorized personnel.

Supplemental Guidance: Physical security safeguards applied to system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Transmission medium includes but are not limited to:
- Publicly accessible network jacks;
- Wireless Access Points (WAPs)
- Border protection devices (including firewalls & routers);
- Networking/communications hardware; and
- Telecommunication lines.

Protective measures to control physical access to system distribution and transmission lines include:
- Locked wiring closets;
- Disconnected or locked spare jacks; and
- Protection of cabling by conduit or cable trays.

Enhancements: None

PE-05: ACCESS CONTROL FOR OUTPUT DEVICES

Control Objective: The organization controls physical access to system output devices to prevent unauthorized individuals from obtaining the output.[119]

Standard: Physical access to system output devices must be limited to authorized personnel to prevent unauthorized individuals from obtaining access to unsecured data.

Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only; and placing output devices in locations that can be monitored by organizational personnel. Transmission medium includes but are not limited to:
- Printers;

[118] PCI DSS 9.1.2 & 9.1.3 | OR646A.622(2)(d)(C)(ii) | NIST CSF PR.AC-2
[119] OR646A.622(2)(d)(C)(ii) | NIST CSF PR.AC-2

- Plotters;
- Facsimile (Fax) machines; and
- Photocopiers.

Enhancements: None

PE-06: Monitoring Physical Access

Control Objective: The organization: [120]

- Monitors physical access to the system to detect and respond to physical security incidents;
- Reviews physical access logs; and
- Coordinates results of reviews and investigations with the organization's incident response capability.

Standard: EAP Expert is responsible for:

(a) Investigating and responding to detected physical security incidents, according to documented procedures;
(b) Performing security checks at the physical boundary of the facility or system for unauthorized exfiltration of information or system components;
(c) Using video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas;
(d) Reviewing collected data and correlate with other entries; and
(e) Retaining physical access data for at least three (3) months, unless otherwise restricted by law.

Supplemental Guidance: None

Enhancements:

- PE-06(a) – Intrusion Alarms / Surveillance Equipment

PE-06(a): Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment

Control Objective: The organization monitors physical intrusion alarms and surveillance equipment.

Standard: Where technically feasible, potential physical ingress and egress points will be monitored with physical intrusion alarms and surveillance equipment.

Supplemental Guidance: None

PE-07: Visitor Control

[Withdrawn: Incorporated into PE-2 and PE-3]

PE-08: Access Records

Control Objective: The organization:[121]

- Maintains visitor access records to the facility where the system resides (except for those areas within the facility officially designated as publicly accessible); and
- Reviews visitor access records.

Standard: EAP Expert is required to:

(a) Use a visitor log to maintain a physical audit trail of visitor activity;
(b) At a minimum, document the visitor's name, the company represented, and the onsite personnel authorizing physical access; and
(c) Retain this log for a minimum of three months, unless otherwise restricted by law.

Supplemental Guidance: Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

[120] HIPAA 164.310(c) | OR646A.622(2)(d)(C)(ii) | PCI DSS 9.1 & 9.1.1 | NIST CSF PR.AC-2, DE.CM-2, DE.CM-7, RS.AN-1 & RS.CO-3
[121] PCI DSS 9.4.4 | OR646A.622(2)(d)(C)(ii)

Enhancements: None

PE-09: Power Equipment & Power Cabling

Control Objective: The organization protects power equipment and power cabling for the system from damage and destruction.[122]

Standard: Asset custodians are required to protect power equipment and power cabling from damage, tampering, and destruction.

Supplemental Guidance: None

Enhancements:

- PE-09(a) – Automatic Voltage Controls

PE-09(a): Power Equipment & Power Cabling | Automatic Voltage Controls

Control Objective: The organization employs automatic voltage controls for critical system components.

Standard: Asset custodians are required to employ automatic voltage controls for critical system components.

Supplemental Guidance: Automatic voltage controls may take the form of Uninterruptable Power Supply (UPS) units or built-in voltage regulating systems, native to the electrical distribution system of the facility.

PE-10: Emergency Shutoff

Control Objective: The organization:[123]

- Provides the capability of shutting off power to the system or individual system components in emergency situations;
- Places emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and
- Protects emergency power shutoff capability from unauthorized activation.

Standard: In data center environments, asset custodians are required to:

(a) Provide the capability of shutting off power to systems in emergency situations;
(b) Place emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and
(c) Protect emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies to facilities containing concentrations of system resources including, for example, data centers, server rooms, and mainframe computer rooms. This control applies to facilities containing concentrations of system resources, such as data centers, server rooms, and mainframe computer rooms.

Enhancements: None

PE-11: Emergency Power

Control Objective: The organization provides a long-term alternate power supply for the system that is self-contained and not reliant on external power generation.[124]

Standard: In data center environments, asset custodians are required to provide for a long-term alternate power supply for critical systems that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Supplemental Guidance: Long-term alternate power supplies for the system may be either manually or automatically activated.

Enhancements: None

[122] NIST CSF ID.BE-4 & PR.AC-2
[123] NIST CSF PR.IP-5
[124] NIST CSF ID.BE-4

PE-12: Emergency Lighting

Control Objective: The organization employs and maintains automatic emergency lighting for the system that activates in the event of a power outage or disruption, and that covers emergency exits and evacuation routes within the facility.[125]

Standard: In data center environments, asset custodians are required to provide emergency lighting for all areas within the facility supporting essential missions and business functions.

Supplemental Guidance: None

Enhancements: None

PE-13: Fire Protection

Control Objective: The organization employs and maintains fire suppression and detection devices/systems for the system that are supported by an independent energy source.[126]

Standard: In data center environments, asset custodians are required to ensure that its facilities undergo annual fire marshal inspections and promptly resolve identified deficiencies.

Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Enhancements:

- PE-13(a) – Fire Detection Devices
- PE-13(b) – Fire Suppression Devices
- PE-13(c) – Automatic Fire Suppression

PE-13(a): Fire Protection | Fire Detection Devices

Control Objective: The organization employs fire detection devices/systems for the system that activate automatically and notify organizational personnel and emergency responders in the event of a fire.

Standard: In data center environments, asset custodians are required to employ fire detection devices that activate automatically and notify organizational personnel and emergency responders in the event of a fire.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

PE-13(b): Fire Protection | Fire Suppression Devices

Control Objective: The organization employs fire suppression devices/systems for the system that provide automatic notification of any activation to organizational personnel and emergency responders.

Standard: Where technically feasible, EAP Expert shall employ fire suppression devices/systems that provide automatic notification of any activation.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

PE-13(c): Fire Protection | Automatic Fire Suppression

Control Objective: The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall employ an automatic fire suppression capability.

---

[125] NIST CSF PR.IP-5

[126] NIST CSF PR.IP-5

Supplemental Guidance: None

PE-14: Temperature & Humidity Controls

Control Objective: The organization:[127]

- Maintains temperature and humidity levels within the facility where the system resides; and
- Monitors temperature and humidity levels.

Standard: In data center environments, asset custodians are required to employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Supplemental Guidance: Temperature and humidity controls typically apply to facilities containing concentrations of system resources, for example, data centers, server rooms, and mainframe computer rooms.

Enhancements:

- PE-14(a) – Monitoring with Alarms / Notifications

PE-14(a): Temperature & Humidity Controls | Monitoring with Alarms / Notifications

Control Objective: The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Standard: Where technically feasible, EAP Expert shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Supplemental Guidance: None

PE-15: Water Damage Protection

Control Objective: The organization protects the system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.[128]

Standard: In data center environments, asset custodians are required to employ mechanisms that, without the need for manual intervention, protect systems from water damage in the event of a water leak.

Supplemental Guidance: Isolation values can be employed in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

Enhancements: None

PE-16: Delivery & Removal

Control Objective: The organization authorizes, monitors, and controls types of system components entering and exiting the facility and maintains records of those items.[129]

Standard: Systems are prohibited from being removed from EAP Expert facilities without prior, management authorization.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and possibly isolating the areas from the system and media libraries.

Prior to the removal of the system, the following information needs to be captured:

- Make / model / serial # of the asset
- Owner of the asset
- Reason the asset is being removed from the facility
- Company and name of representative removing the asset

[127] NIST CSF PR.IP-5
[128] NIST CSF PR.IP-5
[129] OR646A.622(2)(d)(C)(ii) | NIST CSF PR.DS-3

- Estimated return date for the asset, if applicable

Enhancements: None

PE-17: Alternate Work Site

Control Objective: The organization:

- Employs organization-defined management, operational, and technical system security controls at alternate work sites;
- Assesses as feasible, the effectiveness of security controls at alternate work sites; and
- Provides a means for employees to communicate with cybersecurity personnel in case of security incidents or problems.

Standard: EAP Expert management is required to develop plans regarding alternate work sites that include:

(a) System security controls at alternate work sites;
(b) The effectiveness of security controls at alternate work sites; and
(c) The approved means for employees to communicate with administrative personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, commercial facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. This control supports the contingency planning activities of organizations and the telework initiative.

Enhancements: None

PE-18: Location of Information System Components

Control Objective: The organization positions system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.[130]

Standard: Asset custodians and data/process owners are required to:

(a) Plan the location where systems reside with regard to physical and environmental hazards; and
(b) Consider the physical and environmental hazards in its risk mitigation strategy.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to systems and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).

Enhancements: None

PE-19: Information Leakage

Control Objective: The organization protects the system from information leakage due to electromagnetic signals emanations.[131]

Standard: Asset custodians are required to assess facilities to reduce the chance of information leakage due to electromagnetic signals emanations through:

(a) The proper placement of Wireless Access Points (WAPs);
(b) Limiting the output / transmission power of the WAPS; and
(c) Ensuring monitors are positioned to minimize the risk of unauthorized individuals being able to intentionally or inadvertently view the screen.

Supplemental Guidance: Security categories or classifications of systems (with respect to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations. When in use, portable or hand-held devices should be held in a manner so as to avoid visual access by unauthorized individuals and privacy screens (e.g., polarizing / anti-glare) should be utilized, when applicable.

[130] NIST CSF PR.IP-5
[131] NIST CSF PR.DS-5

Enhancements: None

PE-20: Asset Monitoring & Tracking

Control Objective: The organization:[132]

- Employs asset location technologies to track and monitor the location and movement of assets within controlled areas; and
- Ensures that asset location technologies are employed in accordance with applicable laws, regulations, policies, standards, and guidance.

Standard: EAP Expert's requirements for property accountability include:

(a) All persons entrusted with EAP Expert property are responsible for its proper use, care, custody, safekeeping, and disposition. Responsibility for items will be assigned in writing;
(b) Persons will not be assigned to a duty that will prevent them from exercising proper care and custody over the property for which they are responsible;
(c) When a person assumes accountability for property that is remotely located, records must be maintained to show the location of the property and the persons charged with its care and safekeeping;
(d) EAP Expert property will not be used for any private purpose except as authorized by EAP Expert management;
(e) No EAP Expert property will be sold, given as a gift, loaned, exchanged, or otherwise disposed of unless specifically authorized by EAP Expert management; and
(f) Property documents shall identify the manufacturer's make, model, and serial number.

Supplemental Guidance: EAP Expert should employ an automated mechanism to help maintain an up-to-date, complete, accurate, and readily available inventory of system components.

Enhancements: None

[132] NIST CSF DE.CM-2 & DE.CM-7

TECHNICAL CONTROLS

Technical controls are primarily technical in nature. These controls, such as devices, processes, protocols, and other measures, are used to protect the confidentiality, integrity, and availability of the organization's technology assets and data.

ACCESS CONTROL (AC)

Access Control Policy: EAP Expert shall implement logical access controls to limit access to systems and processes to authorized users.

Management Intent: The purpose of the Access Control (AC) policy is to ensure that EAP Expert limits access to its systems and data to authorized users.

Supporting Documentation: Access Control (AC) control objectives & standards directly support this policy.

AC-01: ACCESS CONTROL POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[133]

- A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Standard: EAP Expert is required to document organization-wide access control controls that, at a minimum, include:

(a) A formal, documented access control policy; and
(b) Processes to facilitate the implementation of the access control policy, procedures and associated controls.

Supplemental Guidance: None

Enhancements: None

AC-02: ACCOUNT MANAGEMENT

Control Objective: The organization manages system accounts, including: [134]

- Identifying account types (e.g., individual, group, system, application, guest/anonymous, and temporary);
- Establishing conditions for group membership;
- Identifying authorized users of the system and specifying access privileges;
- Requiring appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling, and removing accounts;
- Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when system users are terminated, transferred, or system usage or need-to-know/need-to-share changes;
- Deactivating accounts that are no longer required;
- Granting access to the system based on a valid access authorization; and
- Reviewing accounts on a regular basis.

Standard: EAP Expert's IT department is responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(a) Control addition, deletion, and modification of user IDs, credentials, and other identifier objects to ensure authorized use is maintained;
(b) Verify user identity before issuing initial passwords or performing password resets;
(c) Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use;
(d) Immediately revoke access for any terminated users;
(e) Remove/disable inactive user accounts within ninety (90) days;

[133] HIPAA 164.312(a)(a) | PCI DSS 8.1 & 8.4
[134] HIPAA 164.312(d) | PCI DSS 8.1.3-8.1.5, 8.2.2, 8.5, 8.5.1, 8.6 & 8.7 | MA201CMR17 17.04(1(a) | NIST CSF PR.AC-1, PR.AC-4, DE.CM-1 & DE.CM-3

(f) Limit repeated access attempts by locking out the user ID after not more than six (6) attempts;
(g) Set the lockout duration to a minimum of thirty (30) minutes or until administrator enables the user ID;
(h) Establish and administer accounts in accordance with a role-based access scheme that organizes system and network privileges into roles;
(i) Track and monitors role assignments for privileged user accounts;
(j) Automatically terminate access for temporary and emergency accounts after the accounts are no longer needed;
(k) Enable accounts used by vendors for remote access only during the time period needed and monitor vendor remote access accounts when in use;
(l) Minimize the use of group, shared, or generic accounts and passwords;
(m) Default user IDs and accounts are disabled or removed;
(n) Service providers with remote access to EAP Expert's premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer; and
(o) Restrict user direct access or queries to databases to database administrators, including.
    i. Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);
    ii. Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators; and
    iii. Review database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes.

Supplemental Guidance:
- Access privileges granted to general users should be reviewed by information owners every six (6) months to determine if access rights are commensurate with the user's job duties.
- Evidence of account and privilege reviews that documents the review occurred, who conducted the review, and what action (if any) was taken should be maintained for a period of twelve (12) months.
- Asset custodians and data/process owners are required to promptly report all changes in user duties or employment status for the User IDs associated with the involved personnel and administrators should promptly revoke all unnecessary access privileges

Enhancements:
- AC-02(a) – Automated System Account Management
- AC-02(b) – Removal of Temporary / Emergency Accounts
- AC-02(c) – Disable Inactive Accounts
- AC-02(d) – Automated Audit Actions
- AC-02(e) – Inactivity Logout
- AC-02(f) – Roles Based Schemes (Role-Based Access Control (RBAC))
- AC-02(g) – Restrictions on Shared Groups / Accounts
- AC-02(h) – Shared / Group Account Credential Termination

AC-02(A): Account Management | Automated System Account Management

Control Objective: The organization employs automated mechanisms to support the management of information system accounts.

Standard: Where technically feasible, automated mechanisms are required to be configured to automatically alert appropriate personnel for security-related changes in account status.

Supplemental Guidance: The use of automated mechanisms can include, for example:
- Using email or text messaging to automatically notify account managers when users are terminated or transferred;
- Using the information system to monitor account usage; and
- Using telephonic notification to report atypical system account usage.

AC-02(B): Account Management | Removal of Temporary / Emergency Accounts

Control Objective: The information system automatically disables or removes temporary and emergency accounts after an organization-defined time period for each type of account.

Standard: Where technically feasible, automated mechanisms are required to disable temporary / emergency accounts after twenty-four (24) hours.

Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.

AC-02(C): ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

Control Objective: The information system automatically disables inactive accounts after an organization-defined time period.

Standard: Where technically feasible, automated mechanisms are required to disable inactive accounts after ninety (90) days.

Supplemental Guidance: None

AC-02(D): ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

Control Objective: The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies organization-defined personnel or roles.

Standard: Where technically feasible, automated mechanisms are required to alert asset custodians when accounts are created, modified, enabled, disabled, and/or removed.

Supplemental Guidance: None

AC-02(E): ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

Control Objective: The organization requires that users log out after an organization-defined time period of expected inactivity.

Standard: If a session has been idle for more than sixty (60) minutes, the user must be logged out and required to re-authenticate to re-activate the session.

Supplemental Guidance: None

AC-02(F): ACCOUNT MANAGEMENT | ROLE BASED SCHEMES (ROLE-BASED ACCESS CONTROL (RBAC))

Control Objective: The organization: [135]

- Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
- Monitors privileged role assignments; and
- Takes actions when privileged role assignments are no longer appropriate.

Standard: EAP Expert is required to establish Role-Based Access Control (RBAC) access enforcement via Active Directory (AD) that:

(a) Covers all system components;
(b) Assigns privileges to individuals based on job classification and function; and
(c) Restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Supplemental Guidance: RBAC is a type of Discretionary Access Control (DAC).

AC-02(G): ACCOUNT MANAGEMENT | RESTRICTIONS ON SHARED GROUPS / ACCOUNTS

Control Objective: The organization only permits the use of shared/group accounts that meet conditions for establishing shared/group accounts.

Standard: Only when justified by a valid business case, EAP Expert permits the use of shared/group accounts.

Supplemental Guidance: None

AC-02(H): ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION

Control Objective: The information system terminates shared/group account credentials when members leave the group.

Standard: When members no longer need access to a shared/group account, permissions are changed on all affected information systems in a timely manner.

Supplemental Guidance: None

[135] HIPAA 164.308(a)(4(ii)(A) & (B) & (C) | PCI DSS 7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3

AC-03: Access Enforcement

Control Objective: Systems enforce approved authorizations for logical access to the system in accordance with applicable policy.[136]

Standard: EAP Expert is required to limit access to systems and sensitive data to only those individuals whose job requires such access.

Enhancements: Access limitations should include the following:

- Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities;
- Assignment of privileges is based on individual personnel's job classification and function;
- Requirement for a documented approval by authorized parties specifying required privileges; and
- Implementation of an automated access control system.

AC-04: Information Flow Enforcement – Access Control Lists (ACLs)

Control Objective: Systems enforce approved authorizations for controlling the flow of information within a system and between interconnected systems in accordance with applicable policy.[137]

Standard: Network administrators are required to enforce information flow control using:

(a) Access Control Lists (ACL) as a basis for flow control decisions;
(b) Documented business justification for the use if all services, protocols, and ports allowed;
(c) Explicit security attributes on information, source, and destination objects as a basis for flow control decisions;
(d) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [138]
(e) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [139]
(f) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [140]
(g) Unauthorized outbound traffic to the Internet is prohibited; [141]
(h) Stateful inspection (dynamic packet filtering) must be implemented; [142]
(i) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [143] and
(j) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [144]

Supplemental Guidance: None

Enhancements:

- AC-04(a) – Object Security Attributes
- AC-04(b) – Content Check for Encrypted Data
- AC-04(c) – Embedded Data Types
- AC-04(d) – Metadata
- AC-04(e) – Human Reviews
- AC-04(f) – Physical / Logical Separation for Information Flows

AC-04(a): Information Flow Enforcement | Object Security Attributes

Control Objective: The information system uses security attributes associated with information, source, and destination objects to enforce defined information flow control policies as a basis for flow control decisions.

---

[136] HIPAA 164.308(a)(4(i) & (ii) | PCI DSS 7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3 | MA201CMR17 17.04(1)(b) & 17.04(b)(a) | OR646A.622(2)(d)(C)(iii) | NIST CSF PR.AM-3, PR.AC-4 & PR.PT-3
[137] PCI DSS 1.1.6, 1.3.3 & 1.3.5 | OR646A.622(2)(d)(C)(iii) | NIST CSF PR.AC-5, PR.DS-5, PR.PT-4 & DE.AE-1
[138] PCI DSS 1.3.1
[139] PCI DSS 1.3.2
[140] PCI DSS 1.3.3
[141] PCI DSS 1.3.4
[142] PCI DSS 1.3.5
[143] PCI DSS 1.3.6
[144] PCI DSS 1.3.7

Standard: Data/process owners and asset custodians are required to use security attributes associated with information, source, and destination objects to enforce defined information flow control policies as a basis for flow control decisions.

Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled Secret would be allowed to flow to a destination object labeled Secret, but an information object labeled Top Secret would not be allowed to flow to a destination object labeled Secret. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information.

AC-04(B): Information Flow Enforcement | Content Check For Encrypted Data

Control Objective: Systems prevent encrypted data from bypassing content-checking mechanisms.

Standard: When necessary for business purposes, EAP Expert's Cybersecurity personnel are authorized to implement steps to block encrypted data that cannot be analyzed by content-checking mechanisms.

Supplemental Guidance: None

AC-04(C): Information Flow Enforcement | Embedded Data Types

Control Objective: Systems enforce limitations on embedding data types within other data types.

Standard: When necessary for business purposes, EAP Expert's Cybersecurity personnel are authorized to block embedded data types.

Supplemental Guidance: Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes, for example, inserting executable files as objects within word processing files or inserting references or descriptive information into a media file.

AC-04(D): Information Flow Enforcement | Metadata

Control Objective: Systems enforces information flow control based on metadata.

Standard: When necessary for business purposes, EAP Expert's Cybersecurity personnel are authorized to implement steps to block data based on metadata tags as part of EAP Expert's Data Loss Prevention (DLP) program.

Supplemental Guidance: Metadata is information used to describe the characteristics of data. Metadata can include structural metadata describing data structures (e.g., data format, syntax, and semantics) or descriptive metadata describing data contents (e.g., age, location, telephone number). Enforcing allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata with regard to data integrity (e.g., protecting against unauthorized changes to metadata tags) and the binding of metadata to the data payload (e.g., ensuring sufficiently strong binding techniques with appropriate levels of assurance).

AC-04(E): Information Flow Enforcement | Human Reviews

Control Objective: Systems enforce the use of human reviews for information flows, firewall and router rule sets on a routine basis.[145]

Standard: EAP Expert management is responsible for implementing a review of firewall and router rule sets at least once every six (6) months to ensure least privileges and best practices are being followed.

Supplemental Guidance: Human reviews regarding information flow enforcement decisions are necessary when systems are not capable of making such flow control decisions or when organizations deem human reviews necessary. Business units are responsible for defining policy filters for all cases where automated flow control decisions are not possible or deemed to be not sufficient.

AC-04(F): Information Flow Enforcement | Physical / Logical Separation for Information Flows

Control Objective: The information system separates information flows logically or physically using mechanisms and/or techniques to accomplish separations by types of information.

[145] PCI DSS 1.1.7

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall separate information flows logically or physically using mechanisms and/or techniques to accomplish separations by types of information.

Supplemental Guidance: Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.

AC-05: Separation of Duties

Control Objective: The organization: [146]

- Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
- Documents separation of duties; and
- Implements separation of duties through assigned system access authorizations.

Standard: In sensitive environments, EAP Expert management is required to:

(a) Separate duties of individuals, as necessary, to prevent malevolent activity without collusion;
(b) Document any separation of duties; and
(c) Where technically feasible, implement separation of duties through assigned system access authorizations.

Supplemental Guidance: None

Enhancements: None

AC-06: Least Privilege

Control Objective: The organization employs the concept of least privilege, allowing only authorized accesses for users and processes which are necessary to accomplish assigned tasks in accordance with organizational business functions. [147]

Standard: EAP Expert follows the "principle of least privilege," [148] which states that only the minimum access necessary to perform an operation should be granted. Access will be granted only for the minimum:

(a) Levels of permissions necessary to perform the job function; and
(b) Time required.

Supplemental Guidance: EAP Expert employs the concept of least privilege for specific duties and systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions. EAP Expert considers the creation of additional processes, roles, and system accounts as necessary to achieve least privilege. EAP Expert also applies least privilege concepts to the design, development, implementation, and operations of systems.

Enhancements:

- AC-06(a) – Authorize Access to Security Functions
- AC-06(b) – Non-Privileged Access for Non-Security Functions
- AC-06(c) – Privileged Accounts
- AC-06(d) – Auditing Use of Privileged Functions
- AC-06(e) – Prohibit Non-Privileged Users from Executing Privileged Functions

AC-06(a): Least Privilege | Authorize Access to Security Functions

Control Objective: The organization explicitly authorizes access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.

Standard: Only explicitly-authorized personnel are permitted to have access to security functions and security-related information.

---

[146] PCI DSS 6.4.2 | NIST CSF PR.AC-4 & PR.DS-5
[147] OR646A.622(2)(d)(C)(iii) | NIST CSF PR.AC-4 & PR.DS-5
[148] Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems." Proceedings of the IEEE 63, 9 (September 1975): 1278-1308.

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

AC-06(B): LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS

Control Objective: The organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions.

Standard: Users must use accounts with the least functionality necessary to perform their job functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

AC-06(C): LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Control Objective: The organization restricts privileged accounts on the information system to organization-defined personnel or roles.

Standard: Assignment of privileged accounts must be limited to users who have:

(a) A valid business justification;
(b) Received security awareness training commensurate with the level of risk from having privileged access; and
(c) Demonstrated technical competence specific to the environment where privileged access is being granted.

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information.

AC-06(D): LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

Control Objective: The information system audits the execution of privileged functions. [149]

Standard: EAP Expert is required to establish a process for linking all access to systems, including administrative privileged accounts (e.g., root or administrator) to each individual user.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT).

AC-06(E): LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Control Objective: The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Standard: Where technically feasible, information systems must be configured to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

[149] PCI DSS 10.2 & 10.2.1-10.2.7

AC-07: Unsuccessful Login Attempts

Control Objective: Systems shall: [150]

- Enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period; and
- Automatically locks the account when the maximum number of unsuccessful attempts is exceeded.

Standard: EAP Expert's IT department is required to configure:

(a) Systems to automatically lock the accounts until released by an administrator when the maximum number of unsuccessful attempts is exceeded; and
(b) The maximum number of consecutive, unsuccessful access attempts is six (6) attempts.

Supplemental Guidance: This control applies regardless of whether the login occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined time period established by organizations.

Enhancements:

- AC-07(a) – Mobile Device Purging

AC-07(a): Unsuccessful Login Attempts | Mobile Device Purging

Control Objective: Mobile devices purge information based on organization-defined purging requirements/techniques after a defined number of consecutive, unsuccessful device login attempts.

Standard: Where technically feasible, mobile devices are required to be configured to be automatically purged after no more than ten (10) consecutive, unsuccessful login attempts to the mobile device.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a login occurs (e.g., personal digital assistants and smart phones).

AC-08: System Use Notification (Logon Banner)

Control Objective: Systems:

- Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices; and
- Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the system.

Standard: Where technically feasible, system use notifications are required to be presented to users on systems.

Supplemental Guidance: System use notifications can be implemented using warning banners displayed when individuals log in to systems. System use notifications are only used for access via interactive login interfaces with human users and are not required when interactive login interfaces do not exist.

Enhancements:

- AC-08(a) – Standardized Microsoft Windows Banner
- AC-08(b) – Truncated Banner

AC-08(a): System Use Notification | Standardized Microsoft Windows Banner

Control Objective: The Microsoft Windows system displays an approved logon banner before granting access to the system that provides privacy and security notices.

Standard: The standard banner is for Microsoft Windows-based workstation & server logons, which is presented every time a user logs onto a workstation or server:

WARNING: You are accessing a protected computer system that is provided for authorized use only.

Your continued use of this protected computer system consents to the following conditions:

[150] PCI DSS 8.1.6 & 8.1.7 | MA201CMR17 17.04(1)(e)

- You have no expectation of privacy on this protected computer system or network. Communications are routinely intercepted and monitored for authorized purposes including, but not limited to vulnerability testing, communications monitoring, network operations, and personnel misconduct investigations.
- At any time, data on this protected computer system, or any attached device, may be seized and inspected. By using this protected computer system, you consent to interception and seizure of all communications and data for any authorized purpose.
- Whether any particular communication or data qualifies for the protection by a privilege or is covered by a duty of confidentiality, is determined in accordance with established legal standards. You are strongly encouraged to seek personal legal counsel on such matters prior to using a protected computer system if you intend to rely on the protections of a privilege or confidentiality.
- Misuse will be prosecuted to the full extent of the law.

Supplemental Guidance: The standard banner is designed to be distributed via Group Policy Object (GPO) in Active Directory.

AC-08(b): System Use Notification | Truncated Banner

Control Objective: Systems not capable of displaying a logon banner from a centralized source, such as Active Directory, displays an approved logon banner before granting access to the system that provides privacy and security notices.

Standard: The truncated banner is for network devices, and non-Microsoft Windows workstation & server logons presented every time a user logs onto a firewall, router, Unix/Linux server, intranet portal, or any other internal system that accepts a logon banner:

This is a protected computer system for authorized use only. Continued use constitutes permission to monitor with no expectation of privacy. Misuse will be prosecuted to the full extent of the law.

Supplemental Guidance: None

AC-09: Previous Logon Notification

Control Objective: Systems notify the user, upon successful logon or system access, of the date and time of the last logon or access.

Standard: Where technically feasible, asset custodians are required to configure systems that process, store or transmit sensitive data to notify the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

Supplemental Guidance: This control is intended to cover both traditional logons to systems and accesses to systems that occur in other types of architectural configurations (e.g., service-oriented architectures).

Enhancements: None

AC-10: Concurrent Session Control

Control Objective: Systems limit the number of concurrent sessions for each system account.

Standard: EAP Expert requires that concurrent sessions are limited to users, based on the role of the account:

(a) Users: Standard user accounts should be configured to have no more than two (2) concurrent sessions; and
(b) Administrators: Privileged user accounts should be configured to have no more than five (5) concurrent sessions.

Supplemental Guidance: Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission critical applications. This control addresses concurrent sessions for system accounts and does not address concurrent sessions by single users via multiple system accounts.

Enhancements: None

AC-11: Session Lock

Control Objective: Systems:

- Prevent further access to systems by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user; and
- Retain the session lock until the user reestablishes access using established identification and authentication procedures.

Standard: Systems are required to enforce a session lock mechanism after sixty (60) minutes of inactivity.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of systems, for example, if organizations require users to log out at the end of workdays. Publicly viewable patterns can include, for example, screen saver patterns, photographic images, solid colors, or a blank screen, so long as none of those patterns convey sensitive information.

Enhancements:
- AC-11(a) – Pattern-Hiding Displays

AC-11(a): Session Lock | Pattern-Hiding Displays
Control Objective: The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Standard: Where technically feasible, information systems must be configured to conceal, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

AC-12: Session Termination
Control Objective: Systems automatically log out users at the end of the session or after an organization-defined time period of inactivity.[151]

Standard: Systems are required to be configured to automatically log users off and require the user to re-authenticate to re-activate the terminal or session if a session has been idle for more than sixty (60) minutes.

Supplemental Guidance: Configure systems to terminate sessions and require users to re-authenticate to re-activate a terminal or session if a session has been idle for more than sixty (60) minutes.

Enhancements: None

AC-13: Supervision & Review
Control Objective: The organization: [152]
- Requires that users log out when no longer using a system;
- Determines normal time-of-day and duration usage for system accounts;
- Monitors for atypical usage of system accounts; and
- Reports atypical usage to designated organizational officials.

Standard: EAP Expert requires asset custodians to:
(a) Determine normal time-of-day and duration usage for system accounts;
(b) Monitor for atypical usage of system accounts; and
(c) Report of atypical usage in accordance with incident escalation procedures.

Supplemental Guidance: None

[151] HIPAA 164.312(a)(b)(iii) | PCI DSS 8.1.8
[152] PCI DSS 10.6, 10.6.1 & 10.6.2

Enhancements: None

AC-14: Permitted Actions Without Identification or Authorization

Control Objective: The organization:

- Identifies specific user actions that can be performed on the system without identification or authentication; and
- Documents and provides supporting rationale in the security plan for the system, user actions not requiring identification and authentication.

Standard: EAP Expert prohibits system configurations that do not require identification or authentication, without a documented and justifiable business requirement.

Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational systems. EAP Expert may allow a limited number of user actions without identification or authentication (e.g., when individuals access public websites) and only to the extent necessary to accomplish mission/business objectives. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred.

Enhancements: None

AC-15: Automated Marking

Control Objective: The organization marks, in accordance with organizational policies and procedures, system media and system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information to aide Data Loss Prevention (DLP) and Network Access Control (NAC).

Standard: Asset custodians are required to configure systems to mark metadata in environments where Data Loss Prevention (DLP) and Network Access Control (NAC) technology is being used.

Supplemental Guidance: Automated marking or "tagging" of data can aid in controlling the distribution and containment of data.

Enhancements: None

AC-16: Security Attributes

Control Objective: Systems support and maintain the binding of organization-defined security attributes to information in storage, process, and transmission.[153]

Standard: Systems are required to be configured to display security attributes in human-readable form on each object output.

Supplemental Guidance: Objects output from the system include, but are not limited to, log files, screens, or printouts. Output devices include, but are not limited to, printers and video displays on computer terminals, monitors, screens on notebook/laptop computers and personal digital assistants.

Enhancements: None

AC-17: Remote Access

Control Objective: The organization:[154]

- Documents allowed methods of remote access to the system;
- Establishes usage restrictions and implementation guidance for each allowed remote access method;
- Monitors for unauthorized remote access to the system;
- Authorizes remote access to the system prior to connection; and
- Enforces requirements for remote connections to the system.

[153] NIST CSF PR.AC-4

[154] PCI DSS 12.3.8 & 12.3.9 | NIST CSF PR.AC-3 & PR.PT-4

Standard: EAP Expert's Cybersecurity personnel are responsible for:

(a) Documenting allowed methods of remote access to the system;
(b) Establishing usage restrictions and implementation guidance for each allowed remote access method;
(c) Monitoring for unauthorized remote access to systems;
(d) Authorizing remote access to systems prior to connection;
(e) Enforcing requirements for remote connections to systems;
(f) Using cryptography to protect the confidentiality and integrity of remote access sessions;
(g) Automatically disconnecting remote access sessions after a period of inactivity; and
(h) Immediately deactivating vendor and business partner remote access when it is no longer needed.

Supplemental Guidance: Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Virtual Private Networks (VPNs), when adequately provisioned with appropriate security controls, are considered internal networks.

Enhancements:

- AC-17(a) – Automated Monitoring / Control
- AC-17(b) – Protection of Confidentiality / Integrity Using Encryption
- AC-17(c) – Managed Access Control Points
- AC-17(d) – Privileged Commands & Access
- AC-17(e) – Disconnect / Disable Access
- AC-17(f) – Telecommuting
- AC-17(g) – Monitoring Vendor Usage

AC-17(A): Remote Access | Automated Monitoring / Control

Control Objective: The information system monitors and controls remote access methods.

Standard: Where technically feasible, information systems must monitor and control remote access methods.

Supplemental Guidance: Automated monitoring and control of remote access sessions allow organizations to detect cyber-attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

AC-17(B): Remote Access | Protection of Confidentiality / Integrity Using Encryption

Control Objective: The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.[155]

Standard: Where technically feasible, information systems must implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information.

AC-17(C): Remote Access | Managed Access Control Points

Control Objective: The information system routes all remote accesses through managed network access control points.

Standard: Where technically feasible, information systems must route all remote accesses through EAP Expert-managed network access control points.

Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections.

AC-17(D): Remote Access | Privileged Commands & Access

Control Objective: The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the system.

[155] NY DFS 500.15

Standard: EAP Expert authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.

Supplemental Guidance: None

AC-17(E): Remote Access | Disconnect / Disable Remote Access

Control Objective: The organization provides the capability to expeditiously disconnect or disable remote access to the information system within an organization-defined time period.

Standard: The Identity and Access Management (IAM) team must implement mechanisms to disconnect or disable remote access within sixty (60) minutes of notice.

Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.

AC-17(F): Remote Access | Telecommuting

Control Objective: The organization authorizes remote access to systems for remote workers.

Standard: EAP Expert authorizes remote users / teleworkers to connect to the internal network only if the following criteria for the remote system are met:

(a) Software patch status is current; and
(b) Anti-malware software is enabled and current.

Supplemental Guidance: None

AC-17(G): Remote Access | Monitoring Vendor Usage

Control Objective: The organization manages accounts used by vendors to access, support, or maintain system components via remote access as follows: [156]

- Vendor accounts are enabled only during the time period needed and disabled when not in use;
- Vendor account usage is monitored when in use.

Standard: Asset custodians and data/process owners are responsible for managing vendor remote access accounts, as follows:

(a) Vendor accounts may only be enabled only during the time period needed and must be disabled when not in use;
(b) Vendor account usage must be monitored when in use.

Supplemental Guidance: Allowing vendors to have 24/7 access to the network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-available external entry point into your network. Enabling access only for the time periods needed, and disabling it as soon as it is no longer needed, helps prevent misuse of these connections.

AC-18: Wireless Access

Control Objective: The organization:[157]

- Establishes usage restrictions and implementation guidance for wireless access;
- Monitors for unauthorized wireless access to the system;
- Authorizes wireless access to the system prior to connection; and
- Enforces requirements for wireless connections to the system.

Standard: EAP Expert's IT department is responsible for:

(a) Establishing usage restrictions and implementation guidance for wireless access;
(b) Monitoring for unauthorized wireless access to the system;
(c) Authorizing wireless access to systems prior to connection; and
(d) Enforcing requirements for wireless connections to systems.

[156] PCI DSS 8.1.5
[157] NIST CSF PR.PT-4

Supplemental Guidance: Wireless technologies include, but are not limited to:

- Microwave;
- Satellite;
- Packet radio (UHF/VHF);
- 802.11x; and
- Bluetooth.

Enhancements:

- AC-18(a) – Authentication & Encryption
- AC-18(b) – Disable Wireless Networking
- AC-18(c) – Restrict Configuration By Users
- AC-18(d) – Configure Wireless Communications

AC-18(a): Wireless Access | Authentication & Encryption

Control Objective: Systems protect wireless access using authentication and encryption.[158]

Standard: EAP Expert is required to ensure wireless networks use industry-recognized leading practices to implement strong encryption for authentication and transmission, commensurate with the sensitivity of the data being transmitted.

Supplemental Guidance: Refer to vendor documentation for the proper security configurations of Wireless Access Points (WAPs) and supported encryption strength.

AC-18(b): Wireless Access | Disable Wireless Networking

Control Objective: The organization disables, when not intended for use, wireless networking capabilities internally embedded within system components prior to issuance and deployment.

Standard: In sensitive environments, asset custodians are required to disable wireless networking capabilities in systems that do not have a legitimate need to have wireless network access.

Supplemental Guidance: Disabling wireless connectivity may be through least privileges in the operating system environment or through password protecting the system BIOS. Similar restrictions may be used to restrict access to only authorized networks.

AC-18(c): Wireless Access | Restrict Configuration By Users

Control Objective: The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Standard: In sensitive environments, users are prohibited from independently configuring the wireless networking capabilities of their assigned systems.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational systems.

AC-18(d): Wireless Access | Configure Wireless Communications

Control Objective: The organization confines wireless communications to organization-controlled boundaries.

Standard: Asset custodians are required to attempt to confine the wireless transmission boundary to within the geographic confines of EAP Expert's facilities through:

(a) Proper placement of Wireless Access Points (WAPs); and
(b) Limiting the output / transmission power of the WAPS.

Supplemental Guidance: Actions that may be taken by EAP Expert to confine wireless communications to organization-controlled boundaries include, for example:

- Reducing the power of wireless transmissions such that the transmissions cannot transit physical perimeters of organizations;
- Employing measures to control wireless emanations (e.g., TEMPEST); and

[158] PCI DSS 4.1.1

- Configuring wireless accesses such that the accesses are point-to-point in nature.

AC-19: Access Control For Mobile Devices

Control Objective: The organization:[159]

- Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;
- Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational systems;
- Monitors for unauthorized connections of mobile devices to organizational systems;
- Enforces requirements for the connection of mobile devices to organizational systems;
- Disables system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
- Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk; and
- Applies inspection measures to mobile devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.

Standard: For EAP Expert-owned mobile devices, the following is required:

(a) Loss / Theft. Immediately notify EAP Expert management if a mobile device is lost or stolen and the user must alert management to the circumstance of the loss and the data contained on the mobile device;
(b) Conduct. Users must conduct themselves in accordance with EAP Expert's Acceptable Use parameters (Appendix H);
(c) Passwords. A password or PIN with a minimum of four (4) characters must be used to log onto the device
(d) Lockout. The mobile device must be set to delete all data or lock internally after ten (10) unsuccessful attempts to enter a password or PIN.
(e) Encryption. The data on the mobile device must be encrypted.
(f) Message Storage Limits. Users may not store more than two hundred (200) messages or fourteen (14) days of messages on a mobile device.
(g) Data Backups. If the user backs up the data from the mobile device to another device that is not encrypted (e.g., backing up a tablet using an unencrypted computer), then the backup data must be encrypted.
(h) Software Protections. Applications that create, store, access, send or receive ePHI must meet EAP Expert security standards and custom developed applications used on mobile devices must undergo a security design review.
(i) Anti-malware. Anti-malware software must be installed on mobile devices that are capable of running such software:
    i. Android: Android devices are required to have anti-malware software installed.
    ii. Windows: Windows devices are required to have anti-malware software installed.
    iii. Apple: The Apple iOS is not currently capable of running anti-malware software, since no such software exists, based on the design of the iOS.
(j) Updates. Mobile device and installed applications must be kept updated with the latest vendor software releases:
    i. Operating Systems: The most recent operating system available for the mobile data device must be used.
    ii. Applications: Available security updates for any applications must be applied in a regular and timely manner unless instructed otherwise by EAP Expert IT staff.
(k) Rooting: Users must not circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., "jailbreaking") and users must not tamper with the mobile device by using unauthorized software, hardware, or other methods.
(l) Wireless: Users are required to utilize good judgment when connecting the mobile device to other devices and networks:
    i. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.
    ii. WiFi: Users may use only secure (e.g., WPA2) WiFi networks known to be trustworthy.
    iii. Cellular: EAP Expert is not responsible for overages or data plans for cellular usage.

Supplemental Guidance: Mobile devices include, but are not limited to:

- Laptop computers;
- Palmtop computers;
- Smart phones;
- Personal Digital Assistants (PDAs);
- FireWire devices;
- Universal Serial Bus (USB) devices;

[159] NIST CSF PR.AC-3

- CDs & DVDs;
- Flash drives;
- Modems;
- Handheld wireless devices;
- Wireless networking cards;
- Portable music players; and
- Any other existing or future mobile computing or storage device is defined as Personal Electronic Device (mobile device)

Enhancements:
- AC-19(a) – Full Device / Container-Based Encryption
- AC-19(b) – Centralized Management of Mobile Devices
- AC-19(c) – Remote Purging
- AC-19(d) – Personally Owned Devices
- AC-19(e) – Tamper Protection & Detection

AC-19(A): Access Control For Mobile Devices | Full Device / Container-Based Encryption

Control Objective: The organization employs full-device or container encryption to protect the confidentiality and integrity of information on organization-defined mobile devices.[160]

Standard: Where technically feasible, information systems must employ full-device or container encryption to protect the confidentiality and integrity of information on EAP Expert-owned or managed mobile devices.

Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields.

AC-19(B): Access Control For Mobile Devices | Central Management Of Mobile Devices

Control Objective: The organization centrally manages mobile devices.

Standard: Where technically feasible, EAP Expert requires mobile devices to be:
(a) Centrally managed; and
(b) Have passwords enabled in accordance with EAP Expert's existing password standards.

Supplemental Guidance: This control enhancement applies to mobile devices that are organization-controlled and excludes portable storage media.

AC-19(C): Access Control For Mobile Devices | Remote Purging

Control Objective: The organization provides the capability to remotely purge information from mobile devices.

Standard: Where technically feasible, EAP Expert requires mobile devices must be able to be remotely wiped when the mobile device is reported as lost or stolen.

Supplemental Guidance: This control enhancement protects information on mobile devices if the devices are obtained by unauthorized individuals. The remote kill / remote erase command must be executed upon notification of the missing status of the mobile device. Once an initial search is complete for the mobile device and it is reasonable to assume the device is either lost or stolen, it is imperative to immediately notify EAP Expert's Service Desk so that a remote kill command can be issued to the device.

AC-19(D): Access Control For Mobile Devices | Personally Owned Devices

Control Objective: The organization restricts the connection of personally-owned, mobile devices to organizational systems.

Standard: EAP Expert assumes that all mobile devices are untrusted unless EAP Expert has properly secured the mobile device. When approved by EAP Expert management, users are allowed to use personally -owned mobile devices, only if the following conditions are met:
(a) Conduct: Users must conduct themselves in accordance with EAP Expert's Acceptable Use parameters (Appendix H);
(b) Passwords: A password or PIN with a minimum of four (4) characters must be used to log onto the device
(c) Lockout. The mobile device must be set to delete all data or lock internally after ten (10) unsuccessful attempts to enter a password or PIN.

[160] NY DFS 500.15

(d) Encryption: The data on the mobile device must be encrypted.
(e) Message Storage Limits. Users may not store more than two hundred (200) messages or fourteen (14) days of messages on a mobile device.
(f) Data Backups: If the user backs up the data from the mobile device to another device that is not encrypted (e.g., backing up a tablet using an unencrypted computer) then the backup data must be encrypted.
(g) Software Protections: Applications that create, store, access, send or receive ePHI must meet EAP Expert security standards and custom developed applications used on mobile devices must undergo a security design review.
(h) Anti-malware: Anti-malware software must be installed on mobile devices that are capable of running such software:
    i. Android: Android devices are required to have anti-malware software installed.
    ii. Windows: Windows devices are required to have anti-malware software installed.
    iii. Apple: The Apple iOS is not currently capable of running anti-malware software, since no such software exists, based on the design of the iOS.
(i) Updates: Mobile device and installed applications must be kept updated with the latest vendor software releases:
    i. Operating Systems: The most recent operating system available for the mobile data device must be used.
    ii. Applications: Available security updates for any applications must be applied in a regular and timely manner unless instructed otherwise by EAP Expert IT staff.
(j) Rooting: Users must not circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., "jailbreaking") and users must not tamper with the mobile device by using unauthorized software, hardware, or other methods.
(k) Wireless: Users are required to utilize good judgment when connecting the mobile device to other devices and networks:
    i. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.
    ii. WiFi: Users may use only secure (e.g., WPA2) WiFi networks known to be trustworthy.
    iii. Cellular: EAP Expert is not responsible for overages or data plans for cellular usage.
(l) Storing EAP Expert data outside of EAP Expert-approved, encrypted containers on the mobile device.

Supplemental Guidance: This control addresses the Bring Your Own Device (BYOD) initiative. Mobile devices, particularly those that are personally owned are not necessarily trustworthy. These mobile devices lack the root of trust features (e.g., Trusted Platform Modules (TPMs)) that are increasingly built into laptops and other types of hosts. There is also frequent "jailbreaking" and "rooting" of mobile devices, which means that the built-in restrictions on security and the operating system have been bypassed.

AC-19(E): Access Control For Mobile Devices | Tamper Protection & Detection

Control Objective: The organization inspects mobile devices upon return from locations of concern to detect tampering.

Standard: Users are required to:
(a) Physically examine their mobile devices upon return from travel to locations of concern for signs of physical or logical tampering; and
(b) Immediately report any possible tampering to EAP Expert.

Supplemental Guidance: This control enhancement addresses both physical and logical tampering to counter state-sponsored intelligence operations that target Western companies.

Specially configured mobile devices may be needed, and these include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Additional, specific safeguards may be required for the device after travel is completed before the device is allowed to connect to EAP Expert's internal network.

AC-20: Use of External Information Systems

Control Objective: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:[161]

- Access the system from the external systems; and
- Process, store, and/or transmit organization-controlled information using the external systems.

Standard: EAP Expert permits the use of external information systems to process, store and/or transmit EAP Expert data only when:
(a) A valid business reason exists for the external trust relationship;
(b) A formal risk assessment of the third-party has been conducted;

[161] NIST CSF ID.AM-4 & PR.AC-3

(c) Risks identified in the risk assessment have been adequately addressed, if applicable; and
(d) A formal contract exists, including Non-Disclosure Agreements (NDAs).

Supplemental Guidance: This control addresses the use of internal and external systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud-based systems and services (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)) from EAP Expert systems.

Enhancements:
- AC-20(a) – Limits of Authorized Use
- AC-20(b) – Portable Storage Devices

AC-20(A): USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS OF AUTHORIZED USE

Control Objective: The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
- Verifies the implementation of required security controls on the external system as specified in the organization's cybersecurity policy and security plan; or
- Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Standard: EAP Expert permits authorized individuals to use external information systems to access the EAP Expert systems or to process, store, or transmit EAP Expert-controlled information only when EAP Expert verifies the implementation of required security controls on the external system as specified in EAP Expert's cybersecurity policies and standards.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

AC-20(B): USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES

Control Objective: The organization restricts or prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Standard: EAP Expert:
(a) Restricts the use of EAP Expert-controlled portable storage devices by authorized individuals on external information systems; and
(b) Prohibits personally-owned portable storage devices on external information systems.

Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

AC-21: INFORMATION SHARING

Control Objective: The organization:[162]
- Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information sharing circumstances where user discretion is required; and
- Employs a process to assist users in making information sharing/collaboration decisions.

Standard: While it is the user's responsibility to exercise sound judgment if information should be shared, asset custodians and data/process owners are required to:
(a) Facilitate information sharing by enabling authorized users to use authorized technology (e.g., SharePoint, a blog, or a wiki page); and
(b) Employ a process to assist users in making information sharing/collaboration decisions.

[162] NIST CSF PR.IP-8

Supplemental Guidance: This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information, information related to special access programs/compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or classification level.

Enhancements: None

AC-22: Publicly Accessible Content

Control Objective: The organization:

- Designates individuals authorized to post information onto an organizational system that is publicly accessible;
- Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto organizational system;
- Reviews the content on the publicly accessible organizational system for nonpublic information; and
- Removes nonpublic information from the publicly accessible organizational system, if discovered.

Standard: Asset custodians and data/process owners are required to:

(a) Designate select individuals to be authorized to post information onto publicly accessible websites;
(b) Train the authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
(c) Review the proposed content of publicly accessible information for nonpublic information prior to posting onto publicly accessible websites;
(d) Review the content on the publicly accessible websites for nonpublic information; and
(e) Remove nonpublic information from the publicly accessible websites, if discovered.

Supplemental Guidance: This addresses systems that are accessible to the general public, typically without identification or authentication. In accordance with EAP Expert policies and standards, the general public is not authorized to access to nonpublic information.

Enhancements: None

AC-23: Data Mining Protection

Control Objective: The organization implements data mining and data harvesting techniques for data storage objects to adequately protect against data mining and data harvesting.

Standard: Asset custodians and data/process owners are required to implement best practices for the development, configuration, and maintenance of public facing websites, services, and applications to mitigate the risk associated with data mining.

Supplemental Guidance: This control can be employed by EAP Expert to reduce the effectiveness of information harvesting from social networking sites, thus, limiting the amount of information that can be obtained from those sites. Data storage objects include, for example, databases, database records, and database fields. Data mining and data harvesting techniques include, for example, limiting the types of responses provided to database queries or limiting the number or frequency of database queries to increase the work factor required to determine the contents of databases.

Enhancements: None

AC-24: Access Control Decisions

Control Objective: The organization establishes procedures to ensure access control decisions are applied to each access request prior to access enforcement.

Standard: Asset custodians and data/process owners are required to ensure access control decisions are applied to each access request prior to access enforcement.

Supplemental Guidance: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when systems enforce access control decisions.

Enhancements: None

AC-25: Reference Monitor

Control Objective: Systems implement a reference monitor, for access control policies, that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

Standard: When necessary, asset custodians and data/process owners are required to configure critical systems to a reference monitor.

Supplemental Guidance: The tamperproof property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The always invoked property prevents adversaries from bypassing the mechanism and hence violating the security policy. The smallness property helps to ensure the completeness of the analysis and testing of the mechanism to detect weaknesses or deficiencies (e.g., latent flaws) that would prevent the enforcement of the security policy.

Enhancements: None

AUDIT & ACCOUNTABILITY (AU)

Audit & Accountability Policy: EAP Expert shall create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity by ensuring that the actions of individual users and systems can be uniquely traced.

Management Intent: The purpose of the Audit & Accountability (AU) policy is to ensure that EAP Expert creates and maintains appropriate scope and totality of audit records.

Supporting Documentation: Audit & Accountability (AU) control objectives & standards directly support this policy.

AU-01: AUDIT & ACCOUNTABILITY POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[163]

- A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Standard: EAP Expert is required to document organization-wide audit and accountability controls that, at a minimum, include:

(a) A formal, documented audit and accountability policy;
(b) Processes to facilitate the implementation of the audit and accountability policy, procedures and associated controls;
(c) Name a person or role as the responsible party for the overall audit process and its results;
(d) Determine the appropriate scope of audit controls that are necessary to protect organizational resources and ensure compliance requirements are met;
(e) Determine what data will need to be captured by the audit controls and logs; and
(f) Implement hardware, software, and procedural controls that record and examine activity.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

AU-02: AUDITABLE EVENTS

Control Objective: The organization:[164]

- Determines, based on a risk assessment and mission/business needs that the system must be capable of auditing events;
- Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
- Provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.

Standard: Asset custodians are required to configure all systems, devices, and applications to implement automated audit trails for all system components to reconstruct the following events:

(a) All individual accesses to sensitive data (e.g., cardholder data and SSNs);
(b) All actions taken by any individual with root or administrative privileges;
(c) Invalid logical access attempts;
(d) Use of identification and authentication mechanisms; and
(e) Creation and deletion of system-level objects.

[163] HIPAA 164.312(b) | PCI DSS 10.1 & 10.8 | NIST CSF PR.PT-1 | NY DFS 500.06
[164] MA201CMR17 17.04(4) | OR646A.622(2)(d)(B)(iii) | NIST CSF PR.PT-1 | NY DFS 500.06

Supplemental Guidance: EAP Expert identifies events which need to be auditable as significant and relevant to the security of systems and the environments in which those systems operate in order to meet specific/ongoing audit needs. For example, EAP Expert may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. Selecting the right level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes of problems.

Enhancements:

- AU-02(a) – Reviews & Updates

AU-02(A): AUDITABLE EVENTS | REVIEWS & UPDATES

Control Objective: The organization reviews and updates the audited events by an organization-defined frequency.[165]

Standard: EAP Expert is required to establish a daily process for linking access to systems and resources, including administrative privileged accounts (e.g., root or administrator).

Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

AU-03: CONTENT OF AUDIT RECORDS

Control Objective: Systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.[166]

Standard: Asset custodians are required to ensure the content of audit records generated by systems includes, at least, the following data fields for each event:

(a) User identification;
(b) Type of event;
(c) Date and time;
(d) Success or failure indication;
(e) Origination of event; and
(f) Identity or name of affected data, system component, or resource.

Supplemental Guidance: None

Enhancements:

- AU-03(a) – Additional Audit Information

AU-03(A): CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

Control Objective: The organization protects sensitive data contained in log files.

Standard: Asset owners and custodians are required to protect, and where required encrypt, log files that may contain sensitive data:

(a) Passwords in the clear;
(b) Social Security Numbers (SSN) or country-specific identification numbers;
(c) Payment card numbers (e.g. credit or debit card); or
(d) Financial account numbers.

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full-text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

[165] NY DFS 500.06

[166] PCI DSS 10.3 & 10.3.1-10.3.6 | NIST CSF PR.PT-1 | NY DFS 500.06

AU-04: Audit Storage Capacity

Control Objective: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.[167]

Standard: Asset custodians are required to allocate sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: Asset owners must consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Enhancements:

- AU-04(a) – Transfer to Alternate Storage

AU-04(a): Audit Storage Capacity | Transfer To Alternate Storage

Control Objective: The system off-loads audit records based on an organization-defined frequency onto a different system or media than the system being audited.

Standard: Asset custodians for critical systems are required to forward security-related event logs to a centralized log collection server.

Supplemental Guidance: This control enhancement addresses systems that lack the capacity to store audit records for long periods of time. Off-loading is the process of moving audit records from the primary system to a secondary or alternate system. It is a common process in systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred. The transfer process is designed to preserve the integrity and confidentiality of audit records.

AU-05: Response To Audit Processing Failures

Control Objective: Systems:[168]

- Alert designated organizational officials in the event of an audit processing failure; and
- Take actions to remedy the audit processing failure.

Standard: Asset custodians are required to ensure critical systems are configured to:

(a) Alert designated personnel in the event of an audit processing failure; and
(b) Take actions to remedy the audit processing failure.

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Enhancements:

- AU-05(a) – Real-Time Alerts

AU-05(a): Response To Audit Processing Failures | Real-Time Alerts

Control Objective: Systems provide a real-time alert to select personnel when the audit failure event requires real-time alerts.

Standard: EAP Expert's IT staff is responsible for managing a 24x7x365 alerting process for critical systems.

Supplemental Guidance: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (e.g., the time from event detection to alert occurs in seconds or less).

AU-06: Audit Review, Analysis & Reporting

Control Objective: The organization:[169]

[167] NIST CSF PR.DS-4 & PR.PT-1
[168] NIST CSF PR.PT-1
[169] NIST CSF PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.AN-1 & RS.CO-2

- Reviews and analyzes system audit records for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
- Adjusts the level of audit review, analysis, and reporting within the system when there is a change in risk to organizational operations, organizational assets, individuals, or other organizations based on law enforcement information, intelligence information, or other credible sources of information.

Standard: Asset custodians are required to:

(a) Review and analyze system audit records for indications of inappropriate or unusual activity, and report the findings in accordance with incident handling procedures;
(b) Adjust the level of audit review, analysis, and reporting within the system when there is a change in risk to operations, assets, individuals, or other organizations based on credible sources of information;
(c) Develop processes for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: [170]
    i. Firewalls;
    ii. IDS/IPS;
    iii. FIM;
    iv. Anti-malware;
    v. Physical access controls;
    vi. Logical access controls;
    vii. Audit logging mechanisms; and
    viii. Segmentation controls (if used); and
(d) Responding to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: [171]
    i. Restoring security functions;
    ii. Identifying and documenting the duration (date and time start to end) of the security failure;
    iii. Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause;
    iv. Identifying and addressing any security issues that arose during the failure;
    v. Performing a risk assessment to determine whether further actions are required as a result of the security failure;
    vi. Implementing controls to prevent cause of failure from reoccurring; and
    vii. Resuming monitoring of security controls.

Supplemental Guidance: EAP Expert operations centralize the review and analysis of audit records from multiple components in order to provide increased awareness of activities across the network. Audit review, analysis, and reporting covers all auditing performed by EAP Expert including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the system boundaries, use of mobile code, and use of VoIP.

Enhancements:

- AU-06(a) – Process Integration
- AU-06(b) – Correlate Audit Repositories
- AU-06(c) – Full-Text Analysis of Privileged Commands

AU-06(A): AUDIT REVIEW, ANALYSIS & REPORTING | PROCESS INTEGRATION

Control Objective: The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Standard: Where technically feasible, EAP Expert employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and audits.

[170] PCI DSS 10.8
[171] PCI DSS 10.8.1

AU-06(B): AUDIT REVIEW, ANALYSIS & REPORTING | CORRELATE AUDIT REPOSITORIES

Control Objective: The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Standard: Where technically feasible, EAP Expert analyzes and correlates audit records across different repositories to gain enterprise-wide situational awareness.

Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness.

AU-06(C): AUDIT REVIEW, ANALYSIS & REPORTING | FULL-TEXT ANALYSIS OF PRIVILEGED COMMANDS

Control Objective: The organization performs a full-text analysis of audited privileged commands in a physically distinct component or subsystem of the system, or another system that is dedicated to that analysis.

Standard: Where technically feasible, full-text analysis of privileged commands is required to be implemented to properly audit privileged actions performed on critical systems.

Supplemental Guidance: Full-text analysis refers to analysis that considers the full text of privileged commands (e.g., commands and all parameters) as opposed to analysis that only considers the name of the command. Full-text analysis includes, for example, the use of pattern matching and heuristics.

AU-07: AUDIT REDUCTION & REPORT GENERATION

Control Objective: Systems provide an audit reduction and report generation capability.[172]

Standard: Asset custodians and data/process owners are required to provide the resources to automatically process audit records for events of interest, based on selectable event criteria and generate reports that allow asset custodians and data/process owners to review potentially significant issues and/or incidents on the system generating the event.

Supplemental Guidance: Audit reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities conducting auditing activities.

Enhancements:

- AU-07(a) – Automatic Processing

AU-07(A): AUDIT REDUCTION & REPORT GENERATION | AUTOMATIC PROCESSING

Control Objective: The information system provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records.

Standard: Where technically feasible, information systems must provide the capability to process audit records for events of interest based on EAP Expert-defined audit fields within audit records.

Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.

AU-08: TIME STAMPS

Control Objective: Systems use internal system clocks to generate time stamps for audit records.[173]

Standard: Asset custodians are required to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time:

[172] NIST CSF PR.PT-1 & RS.AN-3

[173] PCI DSS 10.4 & 10.4.1-10.4.5 | NIST CSF PR.PT-1

(a) Critical systems have the correct and consistent time;
(b) Time data is protected; and
(c) Time settings are received from industry-accepted time sources.

Supplemental Guidance: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.
NTP is an Internet standard protocol which enables client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.[174]

Enhancements:
- AU-08(a) – Synchronization With Authoritative Time Source

AU-08(A): TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

Control Objective: The system synchronizes internal system clocks based on an organization-defined frequency with an authoritative time source.

Standard: The official NIST or USNO Internet Time Service (ITS) required to be used for system time synchronization include, but are not limited to:
(a) time.nist.gov 192.43.244.18 [primary]; and
(b) time-nw.nist.gov 131.107.13.100 [alternate]

Supplemental Guidance: This control enhancement provides uniformity of time stamps for systems with multiple system clocks and systems connected to a network.

AU-09: PROTECTION OF AUDIT INFORMATION

Control Objective: Systems: [175]
- Protect audit information and audit tools from unauthorized access, modification, and deletion:
- Authorize access to management of audit functionality to only a limited subset of privileged users; and
- Protect the audit records of non-local accesses to privileged accounts and the execution of privileged functions.

Standard: Asset custodians and data/process owners are required to:
(a) Secure audit trails so they cannot be altered;
(b) Limit viewing of audit trails to those with a job-related need;
(c) Protect audit trail files from unauthorized modifications;
(d) Promptly back up audit trail files to a centralized log server or media that is difficult to alter;
(e) Write logs for external-facing technologies onto a log server on the internal LAN;
(f) Use file-integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts, although new data being added should not cause an alert;
(g) Identify all approved users with the ability to alter or destroy data; and
(h) Ensure approved users are properly trained to handle sensitive data.

Supplemental Guidance: This control focuses on technical protection of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit system activity.

Enhancements:
- AU-09(a) – Audit Backup on Separate Physical Systems / Components
- AU-09(b) – Access by Subset of Privileged Users

AU-09(A): PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS

Control Objective: The information system backs up audit records onto a physically different system or system component than the system or component being audited.

Standard: Where technically feasible, EAP Expert shall back up audit records onto a physically different system or system component than the system or component being audited.

[174] http://tycho.usno.navy.mil/ntp.html
[175] HIPAA 164.312(c)(a) | PCI DSS 10.5 & 10.5.1-10.5.5 | NIST CSF PR.PT-1

Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records.

AU-09(B): Protection of Audit Information | Access by Subset of Privileged Users

Control Objective: The organization authorizes access to management of audit functionality to only organization-defined subset of privileged users.

Standard: EAP Expert restricts access to the management of audit functionality to users who have:

(a) A valid business justification;
(b) Received security awareness training commensurate with the level of risk from having privileged access; and
(c) Demonstrated technical competence specific to the environment where privileged access is being granted.

Supplemental Guidance: Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access is further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

AU-10: Non-Repudiation

Control Objective: The organization protects against an individual falsely denying having performed a particular action.[176]

Standard: Asset custodians and data/process owners are required to implement electronic mechanisms to corroborate that sensitive data has not been altered in an unauthorized manner.

Supplemental Guidance: Non-repudiation services can be used to determine if information originated from a particular individual or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by:

- Authors of not having authored particular documents;
- Senders of not having transmitted messages;
- Receivers of not having received messages; or
- Signatories of not having signed documents.

Enhancements: None

AU-11: Audit Record Retention

Control Objective: The organization retains audit records for an organization-defined time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. [177]

Standard: Asset custodians and data/process owners are required to retain audit records as necessary by legal or contractual requirements to provide support for investigations of incidents and to meet data retention requirements. In general, logs must be retained according to EAP Expert's record retention schedule:

(a) For critical or sensitive systems:
    i. Log entries must be immediately available for a minimum of 90 days (online);
    ii. Log entries must be available for 365 days (online or offline storage);
(b) All logs must be exportable or transferable in an automated fashion;
(c) Once logs are offloaded to a EAP Expert-approved log collector, the local logs may be removed from the reporting system or application.

[176] HIPAA 164.312(c)(b) | NIST CSF PR.PT-1
[177] PCI DSS 10.7 | NIST CSF PR.PT-1 | NY DFS 500.13

Supplemental Guidance: EAP Expert should retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. Appendix C: Data Retention Periods contains guidance on specific types of records and their retention requirements.

Enhancements: None

AU-12: Audit Generation

Control Objective: Systems:[178]

- Provide audit record generation capability;
- Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
- Generate audit records.

Standard: Asset custodians and data/process owners are required to:

(a) Ensure that systems produce a system-wide audit trail composed of audit records in a standardized format; and
(b) Implement mechanisms to corroborate that sensitive data has not been altered or destroyed in an unauthorized manner.

Supplemental Guidance: Audits records can be generated from many different system components. Audited events are events for which audits are to be generated. These events are typically a subset of all events for which the system is capable of generating audit records.

Enhancements: None

AU-13: Monitoring For Information Disclosure

Control Objective: The organization monitors for evidence of unauthorized exfiltration or disclosure of organizational information.[179]

Standard: Management and corporate communications personnel are required to periodically perform Internet searches of key terminology applicable to business operations for an indication of information leakage.

Supplemental Guidance: Open source information includes, for example, social networking sites and Internet-based web pages.

Enhancements: None

AU-14: Session Audit

Control Objective: Systems provide the capability to:[180]

- Capture and log all content related to a user session; and
- Remotely view all content related to an established user session in real time.

Standard: Asset custodians and data/process owners are required to provide session auditing on systems that store, process or transmit sensitive data, including, but not limited to:

(a) Capturing and logging all content related to a user session;
(b) Remotely viewing all content related to an established user session in real time.

Supplemental Guidance: Session auditing activities need to be developed, integrated, and used in consultation with legal counsel in accordance with applicable laws, policies, or regulations.

Enhancements: None

[178] NIST CSF PR.PT-1, DE.CM-1, DE.CM-3 & DE.CM-7
[179] MA201CMR17 17.04(3) | NIST CSF PR.PT-1 & DE.CM-3
[180] NIST CSF PR.PT-1

AU-15: Alternate Audit Capability

Control Objective: The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides alternate audit functionality.[181]

Standard: For critical systems, the responsible party for EAP Expert's technology infrastructure is required to provide an alternate audit capability in the event of a failure in primary audit capability that provides alternate audit functionality.

Supplemental Guidance: Since an alternate audit capability may be a short-term protection employed until the failure in the primary auditing capability is corrected, organizations may determine that the alternate audit capability need only provide a subset of the primary audit functionality that is impacted by the failure.

Enhancements: None

AU-16: Cross-Organizational Auditing

Control Objective: The organization employs methods for coordinating audit information among external organizations when audit information is transmitted across organizational boundaries.[182]

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for coordinating cross-organizational audits.

Supplemental Guidance: Because of the distributed nature of the audit information, cross-organization sharing of audit information may be essential for the effective analysis of the auditing being performed. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial system, and subsequent systems record that the requests emanated from authorized individuals.

Enhancements: None

[181] NIST CSF PR.PT-1
[182] NIST CSF PR.PT-1

CONFIGURATION MANAGEMENT (CM)

Configuration Management Policy: EAP Expert shall maintain accurate inventories of its systems and enforce security configuration settings for information technology products employed in support of EAP Expert's business operations.

Management Intent: The purpose of Configuration Management (CM) policy is to establish and maintain the integrity of systems.

Supporting Documentation: Configuration Management (CM) control objectives & standards directly support this policy.

CM-01: CONFIGURATION MANAGEMENT POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:

- A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Standard: EAP Expert is required to document organization-wide configuration management controls that, at a minimum, include:

(a) A formal, documented configuration management policy; and
(b) Processes to facilitate the implementation of the configuration management policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

CM-02: BASELINE CONFIGURATIONS

Control Objective: The organization develops, documents, and maintains under configuration control, a current baseline configuration for systems.[183]

Standard: Asset custodians are required to review, update, test, and approve baseline configurations as an integral part of system installations and upgrades.

Supplemental Guidance: Baseline configurations should be based on industry-recognized leading practices. Sources of approved baseline configurations are:

- Microsoft Security Configuration Wizard
- Center for Internet Security (CIS)
- Defense Cybersecurity Agency (DISA) Security Technical Implementation Guides (STIGs) [184]

Enhancements:

- CM-02(a) – Reviews & Updates
- CM-02(b) – Automation Support For Accuracy / Currency
- CM-02(c) – Retention of Previous Configurations
- CM-02(d) – Development & Test Environments
- CM-02(e) – Configure Systems, Components or Devices for High-Risk Areas
- CM-02(f) – Configuration File Synchronization

CM-02(A): BASELINE CONFIGURATION | REVIEWS & UPDATES

Control Objective: The organization reviews and updates the baseline configurations of systems:

- At least annually;

[183] PCI DSS 1.1.1 | NIST CSF PR.DS-7, PR.IP-1 & DE.AE-1 | DFARS 252.204-7008
[184] DISA STIGs official site: http://iase.disa.mil/stigs/index.html

- When required due to so; or
- As part of system component installations and upgrades.

Standard: Asset custodians are required to review and update baseline configurations for systems under their control:

(a) At least annually;
(b) When required due to so; or
(c) As part of system component installations and upgrades.

Supplemental Guidance: None

CM-02(B): BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY

Control Objective: The organization employs automated mechanisms to maintain an up-to-date, complete, accurate and readily available baseline configuration of the information system.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of information systems.

Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels.

CM-02(C): BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

Control Objective: The organization retains previous versions of baseline configurations of systems to support rollback.

Standard: Asset custodians are required to store and maintain at least three (3) previous versions of configurations to support rollback and troubleshooting operations.

Supplemental Guidance: Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.

CM-02(D): BASELINE CONFIGURATION | DEVELOPMENT & TEST ENVIRONMENTS

Control Objective: The organization maintains a baseline configuration for development and test environments that are managed separately from the operational baseline configuration. [185]

Standard: Asset custodians are required to maintain and manage baseline configurations for development and test environments separately from its production baseline configurations.

Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments help protect systems from unplanned/unexpected events related to development and testing activities). Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. This control enhancement requires separate configurations but not necessarily separate physical environments.

CM-02(E): BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS

Control Objective: The organization:

- Issues information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that the organization deems to be of significant risk; and
- Applies organization-defined security safeguards to the devices when the individuals return.

Standard: Where technically and/or economically feasible, EAP Expert must:

(a) Issue information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that EAP Expert deems to be of significant risk; and

[185] PCI DSS 6.4.1

(b) Apply additional, EAP Expert-defined security safeguards to the devices when the individual(s) return.

Supplemental Guidance: When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

CM-02(F): BASELINE CONFIGURATION | CONFIGURATION FILE SYNCHRONIZATION

Control Objective: The organization synchronizes configuration files.[186]

Standard: Where technically feasible, asset custodians responsible for network devices are required to verify running configuration files and start-up configuration files are:

(a) Synchronized with the correct build; and
(b) The same secure configurations.

Supplemental Guidance: None

CM-03: CONFIGURATION CHANGE CONTROL

Control Objective: The organization:[187]

- Determines the types of changes to systems that are configuration controlled;
- Approves configuration-controlled changes to systems with explicit consideration for security impact analyses;
- Documents approved configuration-controlled changes to systems;
- Retains and reviews records of configuration-controlled changes to systems;
- Audits activities associated with configuration-controlled changes to systems; and
- Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes on a routine basis.

Standard: Asset custodians and data/process owners are required to test, validate, and document changes to systems before implementing the changes on the production network.

Supplemental Guidance: Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities.

Enhancements:

- CM-03(a) – Prohibition of Changes
- CM-03(b) – Test, Validate & Document Changes
- CM-03(c) – Security Representative

CM-03(A): CONFIGURATION CHANGE CONTROL | PROHIBITION OF CHANGES

Control Objective: The organization employs mechanisms to:

- Document proposed changes to systems;
- Notify organized-defined approval authorities;
- Prohibit changes to systems until designated approvals are received; and
- Document completed changes to systems.

[186] PCI DSS 1.2.2
[187] NIST CSF PR.IP-1, PR.IP-3, DE.CM-1 & DE.CM-7

Standard: Asset custodians and data/process owners are prohibited from implementing a change without first obtaining pre-approval from the Change Control Board (CCB) and notifying all affected parties prior to the implementation of the change.

Supplemental Guidance: The scope of affected parties must include any clients, partners or vendors that would be affected by the change.

CM-03(B): CONFIGURATION CHANGE CONTROL | TEST, VALIDATE & DOCUMENT CHANGES

Control Objective: The organization tests, validates, and documents changes to systems before implementing the change(s) on the operational system.

Standard: Asset custodians and data/process owners are required to test configuration changes, wherever it is possible, to test a configuration, prior to deploying in the production environment.

Supplemental Guidance: If it is not technically or logistically feasible to test a configuration change, compensating control should be identified and implemented in order to mitigate any negative impact to the production environment from an adverse change event. Compensating controls can include, but is not limited to:

- Images of systems;
- Backups of configurations;
- Viable back out plan;
- After-hours implementation; and
- Pilot/test group rollouts.

CM-03(C): CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE

Control Objective: The organization requires a cybersecurity representative to be a member of the organization-defined configuration change control element (e.g., committee, board).

Standard: EAP Expert's Cybersecurity personnel are required to represent Cybersecurity topics as a representative of EAP Expert's Change Control Board (CCB).

Supplemental Guidance: Cybersecurity representatives can include, for example, system security officers or system security managers. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-03.

CM-04: SECURITY IMPACT ANALYSIS

Control Objective: The organization analyzes changes to systems to determine potential security impacts prior to change implementation.[188]

Standard: From a test environment, asset custodians are required to test proposed changes to assess the security functions of a system to verify that those functions are:

(a) Implemented correctly;
(b) Operating as intended; and
(c) Producing the desired outcome with regard to meeting the security requirements for the system.

Supplemental Guidance: Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. The analysis process should include a review of the following:

- Separate development/test and production environments;
- Separation of duties between development/test and production environments;
- Production data (live data) are not used for testing or development; and
- Removal of test data and accounts before production systems become active.

Enhancements: None

[188] PCI DSS 6.4, 6.4.5, 6.4.5.1-6.4.5.4 | NIST CSF PR.IP-1 & PR.IP-3

CM-05: Access Restriction For Change

Control Objective: The organization defines documents, approves, and enforces access restrictions associated with changes to systems.[189]

Standard: Asset custodians are required to configure systems to prevent the installation of software and hardware components by non-administrators through limiting the actions that users are capable of performing.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, EAP Expert permits only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications.

Enhancements:

- CM-05(a) – Automated Access Enforcement / Auditing
- CM-05(b) – Signed Components
- CM-05(c) – Two-Person Rule
- CM-05(d) – Limit Production / Operational Privileges (Incompatible Roles)
- CM-05(e) – Library Privileges

CM-05(a): Access Restrictions For Change | Automated Access Enforcement / Auditing

Control Objective: The information system enforces access restrictions and supports auditing of the enforcement actions.

Standard: Where technically feasible, information systems must enforce access restrictions and support auditing of the enforcement actions.

Supplemental Guidance: None

CM-05(b): Access Restrictions For Change | Signed Components

Control Objective: The information system prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Standard: Where technically feasible, information systems must prevent the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by EAP Expert.

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication.

CM-05(c): Access Restrictions For Change | Two-Person Rule

Control Objective: The organization enforces a two-person rule for implementing changes to sensitive system components and system-level information.

Standard: When dictated by a compensating control, asset custodians are required to develop and implement a two-person rule for implementing changes to sensitive system components and system-level information.

Supplemental Guidance: Organizations employ a two-person rule to ensure that any changes to selected system components and information cannot occur unless two qualified individuals implement such changes. The two individuals possess sufficient skills/expertise to determine if the proposed changes are correct implementations of approved changes.

CM-05(d): Access Restrictions For Change | Limit Production / Operational Privileges (Incompatible Roles)

Control Objective: The organization:

- Limits privileges to change information system components and system-related information within a production or operational environment; and
- Reviews and reevaluates privileges at an organization-defined frequency.

[189] NIST CSF PR.IP-1

Standard: EAP Expert's management is required to:

(a) Identify incompatible business roles;
(b) Limits privileges to change information system components and system-related information within a production or operational environment;
(c) Implement steps to remediate incompatible business roles; and
(d) Perform reviews, based on EAP Expert's access permission review requirements.

Supplemental Guidance: In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers.

CM-05(E): Access Restrictions For Change | Library Privileges

Control Objective: The organization limits privileges to change software resident within software libraries.

Standard: Data/process owners are required to limit privileges to change software archived within software libraries.

Supplemental Guidance: Software libraries include privileged programs.

CM-06: Configuration Settings

Control Objective: The organization:[190]

- Establishes and documents mandatory configuration settings for information technology products using industry-recognized leading practices consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within systems based on explicit operational requirements; and
- Monitors and controls change to the configuration settings in accordance with organizational policies and procedures.

Standard: EAP Expert is required to establish configuration standards for all technology platforms, including but not limited to:

(a) Firewalls;
(b) Routers;
(c) Switches, capable of being managed;
(d) Wireless Access Points (WAPs);
(e) Servers;
(f) Workstations; and
(g) Mobile Devices, capable of being managed.

Supplemental Guidance: Wherever possible, centralized management should be used to manage, apply, and verify configuration settings.

Enhancements:

- CM-06(a) – Automated Central Management / Application / Verification
- CM-06(b) – Responding to Unauthorized Changes

CM-06(A): Configuration Settings | Automated Central Management / Application / Verification

Control Objective: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for organization-defined information system components.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall employ automated mechanisms to centrally manage, apply, and verify configuration settings for information system components.

Supplemental Guidance: None

[190] PCI DSS 1.1 & 1.1.1 | NIST CSF PR.IP-1

CM-06(b): Configuration Settings | Respond To Unauthorized Changes

Control Objective: The organization employs security safeguards to respond to unauthorized changes to organization-defined configuration settings.

Standard: Upon identifying an unauthorized change to an approved configuration setting, users are required to report the unauthorized change to EAP Expert's Cybersecurity personnel.

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected system processing.

CM-07: Least Functionality

Control Objective: The organization configures systems to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services.[191]

Standard: EAP Expert utilizes the "principle of least privilege,"[192] which states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary. Asset custodians are required to the following:

(a) Identifying and removing insecure services, protocols, and ports;
(b) Enabling only necessary and secure services, protocols, and daemons, as required for the function of the system;
(c) Implementing security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.);
(d) Verifying services, protocols, and ports are documented and properly implemented by examining firewall and router configuration settings; and
(e) Removing all unnecessary functionality, such as:
    i. Scripts;
    ii. Drivers;
    iii. Features;
    iv. Subsystems;
    v. File systems; and
    vi. Unnecessary web servers.

Supplemental Guidance: Asset custodians should review functions and services of systems, to determine which functions and services are candidates for elimination (e.g., Instant Messaging, SMS, auto-execute, and file sharing). EAP Expert may utilize network scanning tools, intrusion detection and prevention systems, and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

Enhancements:

- CM-07(a) – Periodic Review
- CM-07(b) – Prevent Program Execution
- CM-07(c) – Unauthorized or Authorized Software / Blacklisting or Whitelisting

CM-07(a): Least Functionality | Periodic Review

Control Objective: The organization:

- Reviews systems prior to production use to identify unnecessary and non-secure functions, ports, protocols, and services; and
- Disables organization-defined functions, ports, protocols, and services within systems deemed to be unnecessary or non-secure.

Standard: Asset custodians are required to:

(a) Periodically review their systems to identify non-secure functions, ports, protocols, and services; and
(b) Disable unnecessary and non-secure functions, ports, protocols, and services.

[191] PCI DSS 1.1.5, 1.2.1, 2.2.2, 2.2.4 & 2.2.5 | MA201CMR17 17.03(2)(a) | NIST CSF PR.IP-1
[192] Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems." Proceedings of the IEEE 63, 9 (September 1975): 1278-1308.

Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols.

CM-07(B): Least Functionality | Prevent Program Execution

Control Objective: Systems employ automated mechanisms to prevent program execution of unauthorized software programs.

Standard: Asset custodians are required to configuring systems to employ automated mechanisms to prevent program execution of unauthorized software programs.

Supplemental Guidance: None

CM-07(C): Least Functionality | Unauthorized or Authorized Software / Blacklisting or Whitelisting

Control Objective: The organization:

- Identifies software programs not/are note authorized to execute on the information system;
- Employs whitelisting or blacklisting mechanisms; and
- Reviews and updates the list of authorized/unauthorized software programs at an organization-defined frequency.

Standard: Where technically and a business justification exists, EAP Expert may implement application blacklisting or whitelisting.

Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution

CM-08: Information System Component Inventory

Control Objective: The organization develops, documents, and maintains an inventory of system components that:[193]

- Accurately reflects the current system;
- Is at the level of granularity deemed necessary for tracking and reporting;
- Includes organization-defined information deemed necessary to achieve effective property accountability; and
- Is available for review and audit by designated organizational officials.

Standard: EAP Expert is required to create, maintain, and update an inventory of its assets.

Supplemental Guidance: The inventory should be updated as an integral part of component installations, removals, and system updates. Information deemed necessary for effective property accountability includes, for example, hardware inventory specifications, software license information, software version numbers, system/component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

Enhancements:

- CM-08(a) – Updates During Installations / Removals
- CM-08(b) – Automated Unauthorized Component Detection
- CM-08(c) – No Duplicate Accounting of Components
- CM-08(d) – Approved Deviations
- CM-08(e) – Network Diagrams
- CM-08(f) – Network Access Control (NAC)

CM-08(A): Information System Component Inventory | Updates During Installations / Removals

Control Objective: The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Standard: Where technically feasible, asset custodians must update the inventory of information system components as an integral part of component installations, removals, and information system updates.

[193] HIPAA 164.310(d)(b)(iii) | PCI DSS 1.1.2 | NIST CSF ID.AM-1, ID.AM-2, PR.DS-3, PR.PT-3 & DE.CM-7

Supplemental Guidance: None.

CM-08(B): Information System Component Inventory | Automated Unauthorized Component Detection

Control Objective: The organization:

- Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
- Takes action when unauthorized components are detected.

Standard: If applicable, EAP Expert's management of Network Access Control (NAC) technologies:

(a) Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
(b) Takes action when unauthorized components are detected.

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.

CM-08(C): Information System Component Inventory | No Duplicate Accounting of Components

Control Objective: The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Standard: Where technically feasible, asset custodians must verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

CM-08(D): Information System Component Inventory | Approved Deviations

Control Objective: The organization includes assessed component configurations and any approved deviations to currently deployed configurations in the system component inventory.

Standard: Asset custodians are required to request and document approved deviations to deployed configurations in a system under their control.

Supplemental Guidance: This control enhancement focuses on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.

CM-08(E): Information System Component Inventory | Network Diagrams

Control Objective: The organization verifies that all components within the authorization boundary of the system are either inventoried as a part of the system or recognized by another system as a component of that system.[194]

Standard: Asset custodians and data/process owners are required to:

(a) Verify that a current network diagram exists for their environment(s);
(b) Maintain a current diagram that shows all cardholder data flows across systems and networks; and
(c) Documents all connections, including any wireless networks and hosted services.

Supplemental Guidance: The network diagrams should provide sufficient documentation to describe the high-level design of the network in terms of systems and implementation details of the security controls employed, with sufficient detail to permit analysis and testing.

CM-08(F): Information System Component Inventory | Network Access Control (NAC)

Control Objective: The organization:

[194] PCI DSS 1.1.2 & 1.1.3

- Employs automated mechanisms to detect the addition of unauthorized components/devices into the system; and
- Disables network access by such components/devices or notifies designated organizational officials.

Standard: If applicable, EAP Expert's management of Network Access Control (NAC) technologies:

(a) Requires the identification, organization, and categorization of key resources, devices and users,
(b) Must be mapped to EAP Expert's least functionality controls; and
(c) Requires updating as resources, devices, and users change and evolve.

Supplemental Guidance: None.

CM-09: Configuration Management Plan

Control Objective: The organization develops, documents, and implements a configuration management plan for systems that:[195]

- Addresses roles, responsibilities, and configuration management processes and procedures;
- Defines the configuration items for systems and when in the system development life cycle the configuration items are placed under configuration management; and
- Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Standard: Where technically feasible, asset custodians and data/process owners are required to configure systems to include a description of groups, roles, and responsibilities for the logical management of those devices.

Supplemental Guidance: As systems continue through the System Development Life Cycle (SDLC), new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Configuration management plans satisfy the requirements in organizational configuration management policies while being tailored to individual systems.

Enhancements: None

CM-10: Software Usage Restrictions

Control Objective: The organization:[196]

- Uses software and associated documentation in accordance with contract agreements and copyright laws;
- Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
- Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Standard: Users are required to implement and utilize software in accordance with license agreements and copyright laws.

Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on organizational needs. EAP Expert should:

- Employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
- Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Enhancements:

- CM-10(a) – Open Source Software

CM-10(a): Software Usage Restrictions | Open Source Software

Control Objective: The organization establishes restrictions on the use of open source software.

Standard: Only when a strong business case exists and a risk assessment supports it is open source software approved for use.

[195] PCI DSS 1.1.5 | NIST CSF PR.IP-1
[196] NIST CSF DE.CM-3

Supplemental Guidance: Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software.

CM-11: User-Installed Software

Control Objective: The organization enforces explicit rules governing the installation of software by users.[197]

Standard: Software installation is permitted only by authorized system administrators.

Supplemental Guidance: If provided the necessary privileges, users may have the ability to install software in organizational systems. However, to maintain control over the types of software installed, EAP Expert has identified permitted and prohibited software installations. Permitted software installations may include, for example, updates and security patches to existing software. Prohibited software installations may include, for example, software with unknown or suspect software that EAP Expert considers potentially malicious.

Enhancements:

- CM-11(a) – Unauthorized Installation Alerts
- CM-11(b) – Prohibit Installation Without Privileged Status

CM-11(a): User-Installed Software | Unauthorized Installation Alerts

Control Objective: The system alerts personnel or roles when the unauthorized installation of software is detected.

Standard: Where technically feasible, alerting is required to be configured to notify appropriate asset custodians or Cybersecurity personnel when the unauthorized installation of software is detected.

Supplemental Guidance: None

CM-11(b): User-Installed Software | Prohibit Installation Without Privileged Status

Control Objective: The system prohibits user installation of software without explicit privileged status.

Standard: Software installation is permitted only by authorized system administrators.

Supplemental Guidance: Privileged status can be obtained, for example, by serving in the role of system administrator.

[197] NIST CSF DE.CM-3

IDENTIFICATION & AUTHENTICATION (IA)

Identification & Authentication Policy: EAP Expert shall implement mechanisms are employed to properly identify system users, processes acting on behalf of users, or devices, and authenticate the identities of those users, processes, or devices.

Management Intent: The purpose of the Identification & Authentication (IA) policy is to ensure sufficient methods are enacted to properly identify and authenticate EAP Expert's authorized users and processes.

Supporting Documentation: Identification & Authentication (IA) control objectives & standards directly support this policy.

IA-01: IDENTIFICATION & AUTHENTICATION POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates: [198]

- A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Standard: EAP Expert is required to document organization-wide identification and authentication controls that, at a minimum, include:

(a) A formal, documented identification and authentication policy; and
(b) Processes to facilitate the implementation of the identification and authentication policy, procedures, and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

IA-02: USER IDENTIFICATION & AUTHENTICATION (ORGANIZATIONAL USERS)

Control Objective: Systems uniquely identify and authenticate organizational users or processes to:[199]

- Allow the use of group authenticators only when used in conjunction with an individual/unique authenticator; and
- Require individuals to be authenticated with an individual authenticator prior to using a group authenticator.

Standard: EAP Expert is required to assign all users a unique identification (ID) before allowing them to access systems. In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

(a) Something you know, such as a password or passphrase;
(b) Something you have, such as a token device or smart card; or
(c) Something you are, such as a biometric.

Supplemental Guidance: Organizational users include employees or individuals that EAP Expert deems to have the equivalent status of employees (e.g., contractors, consultants). This control applies to all accesses other than accesses that:

- Are explicitly identified and documented in AC-14; and
- Occur through authorized use of group authenticators without individual authentication.

Enhancements:

- IA-02(a) – Network Access to Privileged Accounts
- IA-02(b) – Network Access to Non-Privileged Accounts
- IA-02(c) – Local Access to Privileged Accounts
- IA-02(d) – Group Authentication

[198] PCI DSS 8.1 | NY DFS 500.07
[199] PCI DSS 8.1.1 & 8.2 | MA201CMR17 17.04(1)(c) & 17.04(2)(b) | NY DFS 500.07

- IA-02(e) – Network Access to Privileged Accounts - Replay Resistant
- IA-02(f) – Network Access to Non-Privileged Accounts - Replay Resistant
- IA-02(g) – Remote Access – Separate Device
- IA-02(h) – Acceptance of PIV Credentials

IA-02(A): User Identification & Authentication | Network Access to Privileged Accounts

Control Objective: The information system implements multifactor authentication for network access to privileged accounts.

Standard: Where technically feasible, information systems must implement multifactor authentication for network access by privileged accounts.

Supplemental Guidance: None

IA-02(B): User Identification & Authentication | Network Access to Non-Privileged Accounts

Control Objective: The information system implements multifactor authentication for network access to non-privileged accounts.

Standard: Where technically feasible and a business justification exists, information systems must implement multifactor authentication for network access by non-privileged accounts.

Supplemental Guidance: None

IA-02(C): User Identification & Authentication | Local Access to Privileged Accounts

Control Objective: The information system implements multifactor authentication for local access to privileged accounts.

Standard: Where technically feasible and a business justification exists, asset custodians are required to incorporate two-factor authentication for local access to systems by employees, administrators, and third parties.

Supplemental Guidance: Two-factor authentication requires that two of the three authentications identified in IA-02 be used for authentication. Using one factor twice (e.g., using two separate passwords) is not considered two-factor authentication.

IA-02(D): User Identification & Authentication | Group Authentication

Control Objective: The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

Standard: Where technically feasible, individuals must be authenticated with an individual authenticator when a group authenticator is employed.

Supplemental Guidance: Requiring individuals to use individual authenticators as the second level of authentication helps organizations to mitigate the risk of using group authenticators.

IA-02(E): User Identification & Authentication | Network Access to Privileged Accounts - Replay Resistant

Control Objective: The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Standard: Where technically feasible and a business justification exists, information systems must implement replay-resistant authentication mechanisms for network access by privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

IA-02(F): User Identification & Authentication | Network Access to Non-Privileged Accounts - Replay Resistant

Control Objective: The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Standard: Where technically feasible and a business justification exists, information systems must implement replay-resistant authentication mechanisms for network access by non-privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

IA-02(G): User Identification & Authentication | Remote Access – Separate Device (Multifactor Authentication)

Control Objective: The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets organization-defined strength of mechanism requirements. [200]

Standard: Asset custodians are required to secure all individual non-console administrative access and all remote access to sensitive networks using multi-factor authentication: [201]

(a) Incorporate multi-factor authentication for all non-console access for personnel with administrative access. [202]
(b) Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside EAP Expert's network. [203]

Supplemental Guidance: For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Using one factor twice (e.g., using two separate passwords) is not considered two-factor authentication.

IA-02(H): User Identification & Authentication | Acceptance of PIV Credentials

Control Objective: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall configure information systems to accept and electronically verify Personal Identity Verification (PIV) credentials.

Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable the agency-wide use of PIV credentials.

IA-03: Device-To-Device Identification & Authentication

Control Objective: Systems uniquely identify and authenticate devices before establishing a connection.

Standard: EAP Expert is required to use Active Directory (AD) to authenticate devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Supplemental Guidance: Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by the device, or by a combination of type/device. Systems typically use either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) for device identification or organizational authentication solutions (e.g., Kerberos, IEEE 802.1x and Extensible Authentication Protocol (EAP), Radius server with EAP-Transport Layer Security (TLS) authentication) to identify/authenticate devices on local and/or wide-area networks. Organizations determine the required strength of authentication mechanisms by the security categories of systems.

Enhancements: None

IA-04: Identifier Management (User Names)

Control Objective: The organization manages system identifiers for users and devices by:[204]

- Receiving authorization from a designated organizational official to assign a user or device identifier;

[200] PCI DSS 8.3 | NY DFS 500.12
[201] PCI DSS version 3.2 Requirement 8.3
[202] PCI DSS version 3.2 Requirement 8.3.1
[203] PCI DSS version 3.2 Requirement 8.3.2
[204] HIPAA 164.312(a)(b)(i) | MA201CMR17 17.04(1)(d)

- Selecting an identifier that uniquely identifies an individual or device;
- Assigning the user identifier to the intended party or the device identifier to the intended device; and
- Preventing reuse of user or device identifiers.

Standard: EAP Expert is required to ensure proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(a) Ensure that only authorized users are provided with user IDs;
(b) Ensure that user names and service accounts are uniquely named and in a manner consistent with organizationally defined guidelines; and
(c) Require written authorization by a supervisor or manager to receive a user ID.

Supplemental Guidance: Management of individual identifiers is not applicable to shared system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the names of the system accounts associated with those individuals. Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

Enhancements:

- IA-04(a) – Identity User Status
- IA-04(b) – Dynamic Management
- IA-04(c) – Cross-Organization Management
- IA-04(d) – Privileged Account Identifiers

IA-04(A): IDENTIFIER MANAGEMENT | IDENTITY USER STATUS

Control Objective: The organization manages individual identifiers by uniquely identifying each individual with a characteristic identifying individual status.

Standard: Where technically feasible, EAP Expert shall identify individuals with unique username characteristics that correspond to employment status.

Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

IA-04(B): IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT

Control Objective: The information system dynamically manages identifiers.

Standard: Where technically feasible, information systems shall dynamically manage identifiers.

Supplemental Guidance: In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed information systems including, for example, service-oriented architectures, rely on establishing identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

IA-04(C): IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT

Control Objective: The organization coordinates with external organizations for cross-organization management of identifiers.

Standard: Where technically feasible, EAP Expert shall coordinate with external organizations for cross-organization management of identifiers.

Supplemental Guidance: Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

IA-04(D): IDENTIFIER MANAGEMENT | PRIVILEGED ACCOUNT IDENTIFIERS

Control Objective: The organization manages system identifiers for privileged users by:

- Receiving authorization from a designated organizational official to assign a privileged user identifier; and

- Selecting an identifier that uniquely identifies the privileged user.

Standard: EAP Expert requires privileged user accounts be:

(a) A unique account, separate from a standard user account; and
(b) Used only when necessary for running privileged functions.

Supplemental Guidance: An example of uniqueness, the difference can be adding a designator to the end of the username, such as an "A" for administrator. Examples include:

- Standard user named John Smith: JSMITH1
- Privileged user named John Smith: A.JSMITH1

IA-05: Authenticator Management (Passwords)

Control Objective: The organization manages system authenticators for users and devices by: [205]

- Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators upon system installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
- Changing/refreshing authenticators according to an organization-defined time period by authenticator type;
- Protecting authenticator content from unauthorized disclosure and modification; and
- Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Standard: EAP Expert manages system accounts (authenticators) for users and devices by the following: [206]

a. Verify, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
b. Ensure that authenticators have sufficient strength of mechanism for their intended use;
c. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
d. Change default content of authenticators upon system installation;
e. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
f. Change/refresh authenticators according to an EAP Expert-defined time period by authenticator type;
g. Protect authenticator content from unauthorized disclosure and modification; and
h. Require users to take, and having devices implement, specific measures to safeguard authenticators.

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. Systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and a number of allowed rejections during verification stage of biometric authentication. Specific actions to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

Enhancements:

- IA-05(a) – Password-Based Authentication
- IA-05(b) – PKI-Based Authentication
- IA-05(c) – In-Person or Trusted Third-Party Registration
- IA-05(d) – Automated Support For Password Strength
- IA-05(e) – Protection of Authenticators

[205] HIPAA 164.308(a)(5)(ii)(D) | PCI DSS 8.1.2, 8.2.3, 8.2.4 & 8.2.5 | MA201CMR17 17.04(1)(b)-(e) & 17.04(2)(b)
[206] HIPAA 164.308(a)(5)(ii)(D) | PCI DSS 8.1.2, 8.2.3, 8.2.4 & 8.2.5 | MA201CMR17 17.04(1)(b)-(e) & 17.04(2)(b)

- IA-05(f) – No Embedded Unencrypted Static Authenticators
- IA-05(g) – Hardware Token-Based Authentication
- IA-05(h) – Vendor-Supplied Defaults

IA-05(a): Authenticator Management | Password-Based Authentication

Control Objective: The information system, for password-based authentication:

- Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
- Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];
- Stores and transmits only encrypted representations of passwords;
- Enforces password minimum and maximum lifetime restrictions of [Assignment: organization- defined numbers for lifetime minimum, lifetime maximum];
- Prohibits password reuse for [Assignment: organization-defined number] generations; and
- Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Standard: EAP Expert manages system accounts (authenticators) for users and devices by the following: [207]

(a) User Accounts:

i. Password Length: Minimum of eight (8) characters
ii. Password Reuse: N/A
iii. Password Life: N/A
iv. Password Complexity:
    1. Passwords are not a derivative of the user ID
    2. Passwords have at least one (1) lower alpha, one (1) upper alpha, one (1) number, and one (1) special character.
    3. Passwords cannot contain two identical, consecutive characters

(b) Service Accounts:

i. Password Length: Minimum of ten (10) characters
ii. Password Reuse: N/A
iii. Password Life: N/A
iv. Password Complexity:
    1. Passwords are not a derivative of the user ID
    2. Passwords have at least one (1) lower alpha, one (1) upper alpha, one (1) number, and one (1) special character.
    3. Passwords cannot contain two identical, consecutive characters

(c) Password Protection:

i. Do not use the same password for EAP Expert accounts as for other non-EAP Expert access (e.g., personal ISP account, online banking, benefits, etc.). Users must not use the same password for various EAP Expert access needs and are required to have unique passwords for each account they access.
ii. Do not share EAP Expert passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as Restricted, Confidential EAP Expert information.
iii. Prohibited password practices:
    1. Do not use default vendor passwords
    2. Do not reveal a personal passwords over the phone to anyone for any reason
    3. Do not reveal a personal passwords in an e-mail message
    4. Do not reveal a password to a co-worker or supervisor
    5. Do not talk about a password in front of others
    6. Do not hint at the format of a password (e.g., "my family name")
    7. Do not reveal a password on questionnaires or security forms
    8. Do not share a password with family members
    9. Do not write passwords down and store them anywhere in the user's office
    10. Do not store passwords in a file on any information asset without encryption

(d) Compromise:

[207] HIPAA 164.308(a)(5)(ii)(D) | PCI DSS 8.1.2, 8.2.3, 8.2.4 & 8.2.5 | MA201CMR17 17.04(1)(b)-(e) & 17.04(2)(b)

i. If an account or password is suspected to have been compromised, report the incident to management and change all passwords immediately.

Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords

Passwords should never be written down or stored on-line in an unencrypted format. Users must create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or another phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

Strong (good) passwords have the following characteristics:

- Contain both upper and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*)
- Eight (8) or more alphanumeric characters.
- Not a word in any language, slang, dialect, or jargon.
- Not based on personal information, names of family, or important calendar dates.

Weak (bad) passwords have the following characteristics:

- Default vendor password
- Contain less than eight (8) characters
- A word found in a dictionary (English or foreign)
- A common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
- The words "EAP Expert" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns (e.g., aaabbb, qwerty, zyxwvuts or 123321)
- Any of the above spelled backward.
- Any of the above preceded or followed by a digit (e.g., secret1 or 1secret)

IA-05(B): AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION

Control Objective: The information system, for PKI-based authentication:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
- Enforces authorized access to the corresponding private key;
- Maps the authenticated identity to the account of the individual or group; and
- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Standard: Where technically feasible, asset custodians must configure assets for PKI-based authentication by:

a. Validating certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
b. Enforcing authorized access to the corresponding private key;
c. Mapping the authenticated identity to the account of the individual or group; and
d. Implementing a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing

IA-05(C): Authenticator Management | In-Person or Trusted Third-Party Registration

Control Objective: The organization requires that the registration process to receive an organization-defined types of and/or specific authenticators be conducted in person or by a trusted third party before with authorization by organization-defined personnel or roles.

Standard: EAP Expert's Human Resources (HR) department, in conjunction with the Identity and Access Management (IAM) team, must develop and implement mechanisms to enforce authenticators are only issued by:

a. An in-person process that is managed by HR-designated personnel/roles; or
b. An outsourced process that is managed by a trusted third party.

Supplemental Guidance: None

IA-05(D): Authenticator Management | Automated Support For Password Strength

Control Objective: The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy organization-defined requirements.

Standard: EAP Expert Identity and Access Management (IAM) team may perform password cracking on a periodic or random basis determine if password authenticators are sufficiently strong to satisfy EAP Expert-defined requirements.

Supplemental Guidance: This focuses on the creation of strong passwords and the characteristics of such passwords (e.g., complexity) prior to use, the enforcement of which is carried out by organizational information systems.

IA-05(E): Authenticator Management | Protection of Authenticators

Control Objective: The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access. [208]

Standard: Users are required to follow EAP Expert's practices in

a. The use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.); and
b. Protecting authenticators commensurate with the risk posed to EAP Expert that use of the authenticator permits access.

Supplemental Guidance: For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

IA-05(F): Authenticator Management | No Embedded Unencrypted Static Authenticators

Control Objective: The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Standard: EAP Expert prohibits unencrypted static authenticators from being:

a. Embedded in applications or access scripts; or
b. Stored on function keys.

Supplemental Guidance: Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

IA-05(G): Authenticator Management | Hardware Token-Based Authentication

Control Objective: The information system, for hardware token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.

Standard: Where applicable, asset custodians must employ mechanisms for hardware token-based authentication that satisfy EAP Expert's token quality requirements.

[208] NIST 800-53 IA-5(6) | ISO 27002 9.3.1 | FedRAMP | PCI DSS 8.6

Supplemental Guidance: Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.

IA-05(H): AUTHENTICATOR MANAGEMENT | VENDOR-SUPPLIED DEFAULTS

Control Objective: The organization changes vendor-supplied defaults before installing a system on the network, including but not limited to passwords, Simple Network Management Protocol (SNMP) strings, and eliminate unnecessary accounts.[209]

Standard: Asset custodians and data/process owners are required to changes vendor-supplied defaults before installing a system on the network, including but not limited to

(a) Passwords;
(b) Encryption keys;
(c) Simple Network Management Protocol (SNMP) strings; and
(d) Removing unnecessary, default accounts.

Supplemental Guidance: None

IA-06: AUTHENTICATOR FEEDBACK

Control Objective: Systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Standard: Asset custodians and data/process owners are required to ensure all systems and applications obscure the visible feedback of authentication information (e.g., passwords) during the authentication process to protect the information from possible exploitation by unauthorized individuals.

Supplemental Guidance: The feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices.

Enhancements: None

IA-07: CRYPTOGRAPHIC MODULE AUTHENTICATION

Control Objective: Systems use mechanisms for authentication to a cryptographic module that meet the requirements of applicable local, state, and federal laws, as well as non-regulatory requirements that the organization is contractually bound to address.[210]

Standard: Asset custodians and data/process owners are required to ensure all systems and applications use strong cryptography to render all passwords unreadable during transmission and storage on all system components.

Supplemental Guidance: This control reinforces the requirements for organizational systems implementing cryptographic protections using cryptographic modules. If cryptography is required, systems are required to authenticate to the associated cryptographic modules implementing the cryptography.

National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the data and/or system.

Enhancements: None

IA-08: IDENTIFICATION & AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control Objective: Systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

[209] PCI DSS 2.1, 2.1.1 & 8.3
[210] PCI DSS 8.2.1

Standard: Where technically feasible, asset custodians are required to assign non-EAP Expert users with unique identifiers in both usernames and email addresses to clarify the user is not directly employed by EAP Expert.

Supplemental Guidance: Non-organizational users include system users other than organizational users explicitly covered by IA-02. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. EAP Expert should use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

Enhancements:

- IA-08(a) – Acceptance of PIV Credentials from Other Organizations
- IA-08(b) – Acceptance of Third-Party Credentials
- IA-08(c) – Use of FICAM-Approved Products
- IA-08(d) – Use of FICAM-Issued Profiles

IA-08(A): Identification & Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Organizations

Control Objective: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from US federal agencies.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall configure information systems to accept and electronically verify Personal Identity Verification (PIV) credentials from US federal agencies.

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable the agency-wide use of PIV credentials.

IA-08(B): Identification & Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials

Control Objective: The information system accepts only FICAM-approved third-party credentials.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall configure information systems to accept only FICAM-approved third-party credentials.

Supplemental Guidance: This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.

IA-08(C): Identification & Authentication (Non-Organizational Users) | Use of FICAM-Approved Products

Control Objective: The organization employs only FICAM-approved information system components to accept third-party credentials.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall employ only FICAM-approved information system components to accept third-party credentials.

Supplemental Guidance: This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program.

IA-08(D): Identification & Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles

Control Objective: The information system conforms to FICAM-issued profiles.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall configure information systems to conform to FICAM-issued profiles.

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).

IA-09: Service Provider Identification & Authentication (Vendors)

Control Objective: The organization identifies and authenticates service provider system services using security safeguards.

Standard: Where technically feasible, asset custodians are required to implement mechanisms to authenticate traffic from external information service providers that connect to EAP Expert's networks.

Supplemental Guidance: This control supports service-oriented architectures and other distributed, architectural approaches requiring the identification and authentication of system services. In such architectures, external services often appear dynamically. Therefore, systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

Enhancements: None

IA-10: Adaptive Identification & Authentication

Control Objective: The organization requires that individuals accessing the system employ authentication techniques or mechanisms under specific circumstances or situations.

Standard: Adaptive identification or authentication mechanisms must be pre-approved by the Cybersecurity Officer (ISO) or his/her designated representatives.

Supplemental Guidance: Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations when certain pre-established conditions or triggers occur, organizations can require selected individuals to provide additional authentication information.

Enhancements: None

IA-11: Re-Authentication

Control Objective: The organization requires users and devices to re-authenticate when circumstances or situations requiring re-authentication. [211]

Standard: Asset custodians and data/process owners are required to configure systems to terminate sessions and require users to re-authenticate to re-activate a terminal or session if a session has been idle for more than sixty (60) minutes.

Supplemental Guidance: In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of individuals and/or devices in other situations including, for example:

- When authenticators change;
- When roles change;
- When security categories of systems change;
- When the execution of privileged functions occurs;
- After a fixed period of time; or periodically.

[211] PCI DSS 8.1.8

Enhancements: None

MAINTENANCE (MA)

Maintenance Policy: EAP Expert shall perform periodic and timely maintenance on systems, so that EAP Expert assets are protected from the latest threats.

Management Intent: The purpose of the Maintenance (MA) policy is to ensure that due diligence is performed by properly maintaining EAP Expert systems.

Supporting Documentation: Maintenance (MA) control objectives & standards directly support this policy.

MA-01: MAINTENANCE POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates:[212]

- A formal, documented system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.

Standard: EAP Expert is required to document organization-wide maintenance controls that, at a minimum, include:

(a) A formal, documented maintenance policy; and
(b) Processes to facilitate the implementation of the maintenance policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

MA-02: CONTROLLED MAINTENANCE

Control Objective: The organization:[213]

- Schedules, performs, documents, and reviews records of maintenance and repairs on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- Requires explicit management approval for the removal of the system or system components from organizational facilities for off-site maintenance or repairs;
- Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and
- Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Standard: Asset custodians are required to:

(a) Schedule, perform, document, and review records of maintenance and repairs on systems in accordance with manufacturer or vendor specifications and company requirements;
(b) Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
(c) Require explicit management approval for the removal of the systems or system components from company facilities for off-site maintenance or repairs;
(d) Sanitize equipment to remove all information from associated media prior to removal from company facilities for off-site maintenance or repairs; and

[212] HIPAA 164.310(a)(b)(iv)
[213] NIST CSF PR.MA-1

(e) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Supplemental Guidance: This control addresses the cybersecurity aspects of the system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or non-local entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers.

Enhancements:

- MA-02(a) – Maintenance Activities

MA-02(A): CONTROLLED MAINTENANCE | MAINTENANCE ACTIVITIES

Control Objective: The organization produces up-to-date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

Standard: For critical systems, asset custodians are required to keep maintenance records for systems that include:

(a) Date and time of maintenance;
(b) Name of the individual performing the maintenance;
(c) Name of escort, if necessary;
(d) A description of the maintenance performed; and
(e) A list of equipment removed or replaced (including identification numbers, if applicable).

Supplemental Guidance: None

MA-03: MAINTENANCE TOOLS

Control Objective: The organization approves controls, monitors the use of, and maintains on an ongoing basis, system maintenance tools.[214]

Standard: Asset custodians are required to inspect all maintenance tools carried into EAP Expert facilities by maintenance personnel for obvious improper modifications or indications that proper maintenance is not being performed.

Supplemental Guidance: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers.

Enhancements:

- MA-03(a) – Inspect Tools
- MA-03(b) – Inspect Media
- MA-03(c) – Prevent Unauthorized Removal

MA-03(A): MAINTENANCE TOOLS | INSPECT TOOLS

Control Objective: The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Standard: Where technically feasible, asset custodians must inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

MA-03(B): MAINTENANCE TOOLS | INSPECT MEDIA

Control Objective: The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

[214] NIST CSF PR.MA-1

Standard: Where technically feasible, asset custodians must check media containing diagnostic and test programs for malicious code before the media are used in an information system.

Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

MA-03(c): Maintenance Tools | Prevent Unauthorized Removal

Control Objective: The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

- Verifying that there is no organizational information contained on the equipment;
- Sanitizing or destroying the equipment;
- Retaining the equipment within the facility; or
- Obtaining an exemption from organization-defined personnel or roles explicitly authorizing the removal of the equipment from the facility.

Standard: Asset custodians and data/process owners are required to:

(a) Verify that there is no EAP Expert information contained in the equipment;
(b) Sanitize or destroy the equipment; or
(c) Retain the equipment within the facility.

Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

MA-04: Non-Local Maintenance

Control Objective: The organization:[215]

- Authorizes, monitors, and controls non-local maintenance and diagnostic activities;
- Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
- Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
- Maintains records of non-local maintenance and diagnostic activities; and
- Terminates all sessions and network connections when non-local maintenance is completed.

Standard: Asset custodians and data/process owners are required to:

(a) Authorize, monitor, and control non-local maintenance and diagnostic activities;
(b) Allow the use of non-local maintenance and diagnostic tools only in accordance with policy and standards;
(c) Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
(d) Maintain records of non-local maintenance and diagnostic activities; and
(e) Terminate all sessions and network connections when non-local maintenance is completed.

Supplemental Guidance: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the system or system component and not communicating across a network connection. Authentication techniques used in the establishment of non-local maintenance and diagnostic sessions reflect the network access requirements in IA-02. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-04 is accomplished in part, by other controls.

Enhancements:

- MA-04(a) – Auditing
- MA-04(b) – Document Non-Local Maintenance
- MA-04(c) – Cryptographic Protection
- MA-04(d) – Remote Disconnect Verification

[215] NIST CSF PR.MA-2

MA-04(A): NON-LOCAL MAINTENANCE | AUDITING

Control Objective: The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.

Standard: Asset custodians and data/process owners are required to routinely perform audits of non-local maintenance and diagnostic sessions to observe for indications of unauthorized activity.

Supplemental Guidance: None

MA-04(B): NON-LOCAL MAINTENANCE | DOCUMENT NON-LOCAL MAINTENANCE

Control Objective: The organization requires:

- Maintenance personnel notify organization-defined personnel when non-local maintenance is planned (e.g., date/time); and
- Pre-approval of non-local maintenance sessions.

Standard: EAP Expert requires:

(a) Maintenance personnel to provide prior notification when non-local maintenance is planned (e.g., date & time); and
(b) A designated employee with specific system knowledge to approve the non-local maintenance.

Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of non-local maintenance sessions is accomplished by organizational personnel with sufficient cybersecurity and system knowledge to determine the appropriateness of the proposed maintenance.

MA-04(C): NON-LOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION

Control Objective: The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.[216]

Standard: Asset custodians are required to use technologies that incorporate strong encryption for non-console administrative access.

Supplemental Guidance: EAP Expert should use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.

MA-04(D): NON-LOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION

Control Objective: The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.

Standard: Asset custodians and data/process owners are responsible for determining a method to verify remote disconnect upon at the termination of non-local maintenance.

Supplemental Guidance: None

MA-05: MAINTENANCE PERSONNEL

Control Objective: The organization:[217]

- Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and
- Ensures that personnel performing maintenance on the system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise system maintenance when maintenance personnel do not possess the required access authorizations.

Standard: Asset custodians and data/process owners are required to:

(a) Establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel; and

[216] PCI DSS 2.3
[217] NIST CSF PR.MA-1

(b) Ensure that personnel performing maintenance have required access authorizations or designate specific personnel with required access authorizations and technical competence necessary to supervise the maintenance when maintenance personnel do not possess the required access authorizations.

Supplemental Guidance: This control applies to individuals performing hardware or software maintenance on organizational systems and to individuals whose maintenance duties place them within the physical protection perimeter of the systems. Individuals who might be located within the physical protection perimeter include, for example, physical plant maintenance personnel and janitorial staff. Technical competence of supervising individuals relates to the maintenance performed on the systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, and consultants, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Enhancements:

- MA-05(a) – Individuals Without Appropriate Access

MA-05(A): MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

Control Objective: The organization:

- Implements procedures for the use of maintenance personnel who lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
  - Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
  - Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized, and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
- Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall implement procedures to manage maintenance personnel that lack appropriate security clearances or are not U.S. citizens.

Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained in organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems.

MA-06: TIMELY MAINTENANCE

Control Objective: The organization obtains maintenance support and/or spare parts for systems and/or key information technology components within an organization-defined time period.

Standard: Asset custodians and data/process owners are required to obtain maintenance support and spare parts for critical systems and key information technology components within defined Service Level Agreements (SLAs).

Supplemental Guidance: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, or other organizations when the security functionality provided by those components is not operational. Security-critical components include, for example, firewalls, guards, gateways, routers, intrusion detection and prevention systems, audit repositories, authentication servers, and intrusion prevention systems.

Enhancements: None

System & Communication Protection (SC)

System & Communication Protection Policy: EAP Expert shall employ industry-recognized leading practice principles that promote effective Cybersecurity within systems and the network.

Management Intent: The purpose of the System & Communication Protection (SC) policy is to ensure sufficient protections are in place to protect the confidentiality and integrity of EAP Expert's communications.

Supporting Documentation: System & Communication Protection (SC) control objectives & standards directly support this policy.

SC-01: System & Communication Policy & Procedures

Control Objective: The organization develops, disseminates, reviews & updates:

- A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Standard: EAP Expert is required to document organization-wide system and communication controls that, at a minimum, include:

(a) A formal, documented system and communication policy; and
(b) Processes to facilitate the implementation of the system and communication policy, procedures, and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

SC-02: Application Partitioning

Control Objective: System configurations separate user functionality (including user interface services) from system management functionality.[218]

Standard: Where technically feasible, physically or logically separate user interfaces (e.g., public Web pages) are required to be implemented from storage and management services (e.g., administrative or database management). Separation may be accomplished through the use of one or more of the following:

(a) Network segmentation;
(b) Different computers;
(c) Different central processing units;
(d) Different instances of the operating system;
(e) Different network addresses; or
(f) Other methods as appropriate.

Supplemental Guidance: System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

Enhancements: None

[218] PCI DSS 11.3.4

SC-03: Security Function Isolation

Control Objective: System configurations isolate security functions from non-security functions.[219]

Standard: Asset custodians and data/process owners are required to implement isolation techniques to prevent functions that require different security levels from co-existing on the same server. Isolation techniques include, but are not limited to:

(a) Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server;
(b) Firewall and router configurations need be configured to restrict connections between untrusted networks and any system components in EAP Expert's trusted, internal network;
(c) Firewall need be installed at all connections from an internal to any other internal or external network;
(d) Demilitarized Zones (DMZs) need to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;
(e) Servers which access external networks or are accessed from external networks need to be logically isolated from the private Intranet;
(f) Networks need to be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices;
(g) Switched network technology need to be utilized, when possible, to prevent eavesdropping, session stealing or other exploits based on the accessibility of network traffic;
(h) Trust relationships should be strictly avoided between information resources with different risk profiles; and
(i) Information resources with higher protection requirements for confidentiality should not have a trusted relationship with a system that has lower protection requirements.
(j) If segmentation is used to isolate the sensitive networks from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. [220]

Supplemental Guidance: The system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

Enhancements:

- SC-03(a) – Layered Defenses

SC-03(a): Security Function Isolation | Layered Defenses

Control Objective: The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. [221]

Standard: EAP Expert is required to use a Defense-in-Depth (DiD) architecture to protect the Confidentiality, Integrity, and Availability of systems and data, placing systems that contain sensitive data in an internal network zone, segregated from the DMZ and other untrusted networks.

Supplemental Guidance: The implementation of layered structures with minimized interactions among security functions and non-looping layers (e.g., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.

SC-04: Information In Shared Resources

Control Objective: Systems prevent unauthorized and unintended information transfer via shared system resources.

Standard: Asset custodians and data/process owners are required to ensure that systems are configured to require privilege levels for access. The levels must ensure data is not exposed to individuals or processes with a lower privilege level.

[219] PCI DSS 1.2, 1.3.1, 2.2.1 & 11.3.4
[220] PCI DSS 11.3.4 & 11.3.4.1
[221] PCI DSS 1.3.7

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resource have been released back to systems. The control of information in shared system resources is also referred to as object reuse.

Enhancements: None

SC-05: Denial of Service (DoS) Protection

Control Objective: Systems protect against or limit the effects of denial of service attacks.[222]

Standard: Technology architects, asset custodians, and data/process owners are required to configure the architecture of the network and systems to ensure the capability exists to limit the effects of denial of service attacks.

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.

Enhancements: None

SC-06: Resource Priority

Control Objective: Systems limit the use of resources by priority.

Standard: Asset custodians and data/process owners are required to prioritize resources to prevent or limit Denial of Service (DoS) attack effectiveness.

Supplemental Guidance: Priority protection helps prevent lower-priority processes from delaying or interfering with the system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to system components for which there are only single users/roles.

Enhancements: None

SC-07: Boundary Protection

Control Objective: The organization employs boundary protection mechanisms to separate system components directly supporting organization-defined missions and/or business functions. [223]

Standard: Network administrators are required to:

(a) Implement a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and the internal network zone;
(b) Verify that the current network diagrams are consistent with the firewall configuration standards;
(c) Prohibit direct public access between the Internet and any sensitive system in the internal network zone;
(d) Restrict inbound and outbound traffic to that which is necessary for authorized business purposes;
(e) Limit the number of access points to the system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic;
(f) Ensure traffic flow policies are established and reviewed for each managed interface;
(g) Ensure the exceptions to Access Control Lists (ACLs) are documented and reviewed;
(h) Ensure systems prevent remote devices that have established a non-remote connection (e.g., VPN) with the system from communicating outside that path and with resources external to the network;
(i) Ensure systems prevent the unauthorized release of information outside the system boundary or any unauthorized communication through the system boundary when there is an operational failure of the boundary protection mechanisms;
(j) Ensure private IP addresses and routing information are not disclosed to unauthorized parties; and

[222] NIST CSF PR.DS-4 & DE.CM-1
[223] PCI DSS 1.1.3, 1.1.4, 1.2.1, 1.2.3 & 1.3 | MA201CMR17 17.04(6) | NIST CSF PR.AC-5, PR.DS-5, PR.PT-4 & DE.CM-1

(k) Implement a firewall between any wireless networks and the internal network zone:
    i. Verify that there are perimeter firewalls installed between any wireless networks and systems that store sensitive data;
    ii. Configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the internal network zone; and
    iii. Verify that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Supplemental Guidance: Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or sub-networks, cross-domain devices separating sub-networks, and encrypting information flows among system components using distinct encryption keys. EAP Expert can isolate system components performing different business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provide the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber-attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen.

Enhancements:
- SC-07(a) – Access Points
- SC-07(b) – External Telecommunications Services
- SC-07(c) – Deny Traffic by Default & Allow Traffic by Exception
- SC-07(d) – Prevent Split Tunneling for Remote Devices
- SC-07(e) – Route Traffic To Proxy Servers
- SC-07(f) – Host-Based Protection
- SC-07(g) – Isolation of Security Tools / Mechanisms / Support Components
- SC-07(h) – Internal Network Address Space
- SC-07(i) – Fail Secure

SC-07(A): Boundary Protection | Access Points

Control Objective: The organization limits the number of external network connections to the information system.

Standard: Where technically feasible, asset custodians and asset owners must limit the number of external network connections to the information system.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

SC-07(B): Boundary Protection | External Telecommunications Services

Control Objective: The organization:
- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
- Reviews exceptions to the traffic flow policy and removes exceptions that are no longer supported by an explicit mission/business need.

Standard: EAP Expert must:
(a) Implement a managed interface for each external telecommunication service;
(b) Establish a traffic flow policy for each managed interface;
(c) Protect the confidentiality and integrity of the information being transmitted across each interface;
(d) Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
(e) Review exceptions to the traffic flow policy and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: None

SC-07(c): Boundary Protection | Deny Traffic by Default & Allow Traffic by Exception

Control Objective: The organization, at managed interfaces, denies network traffic by default and allows network traffic by exception (e.g., deny all, permit by exception). [224]

Standard: An explicit "deny all" or an implicit deny after allow statement is required to ensure that all unnecessary inbound and outbound traffic is denied by default.

Supplemental Guidance: None

SC-07(d): Boundary Protection | Prevent Split Tunneling for Remote Devices

Control Objective: The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Standard: Asset custodians are required to configure information systems to prevent "split tunneling" for remote devices.

Supplemental Guidance: This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

SC-07(e): Boundary Protection | Route Traffic To Proxy Servers

Control Objective: Systems route internal communications traffic to external networks through approved proxy servers at managed interfaces. [225]

Standard: EAP Expert prohibits direct public access between the Internet and any system on EAP Expert's internal networks.

Supplemental Guidance: External networks are networks outside the control of organizations. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Proxy servers can be configured with organization-defined lists of authorized and unauthorized websites.

SC-07(f): Boundary Protection | Host-Based Protection

Control Objective: Systems implement underlying software separation mechanisms to facilitate security function isolation. [226]

Standard: EAP Expert requires:

(a) The installation of firewall software or equivalent functionality on any Internet-accessible mobile device or computer;
(b) Verification that the firewall software is configured to specific standards and is not alterable by users of the mobile and/or employee-owned computers; and
(c) The installation of a Web Application Firewall (WAF) in front of sensitive, public-facing web applications to detect and prevent web-based attacks.

Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. System components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.

[224] PCI DSS 1.2.1
[225] PCI DSS 1.3
[226] PCI DSS 1.4

SC-07(G): BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS

Control Objective: The organization isolates cybersecurity tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Standard: Where technically feasible, EAP Expert shall isolate cybersecurity tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks.

Supplemental Guidance: Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations.

SC-07(H): BOUNDARY PROTECTION | INTERNAL NETWORK ADDRESS SPACE

Control Objective: The organization prevents the disclosure of internal address information.[227]

Standard: Asset custodians and data/process owners are required to configure systems to prevent the disclosure of private IP addresses and routing information to unauthorized parties. Methods to obscure IP addressing may include, but are not limited to:

(a) Network Address Translation (NAT);
(b) Placing systems behind proxy servers/firewalls or content caches;
(c) Removing or filtering route advertisements for private networks that employ registered addressing; or
(d) Using internal use of RFC1918 address space instead of registered addresses.

Supplemental Guidance: None

SC-07(I): BOUNDARY PROTECTION | FAIL SECURE

Control Objective: The information system fails securely in the event of an operational failure of a boundary protection device.[228]

Standard: Where technically feasible, asset custodians and data/process owners are required to configure assets to fail in a known state for types of failures in order to preserve system state information at the time of the failure.

Supplemental Guidance: This is used to manage risk to specialized systems, including operational technology (e.g., ICS, SCADA, DCS, and PLC) consistent with risk analysis.

Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases

SC-08: TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control Objective: The organization protects the integrity of transmitted information. [229]

Standard: Asset custodians and data/process owners are required to prevent unauthorized disclosure of information during transmission, ensuring systems transmitting sensitive information:

(a) Only trusted keys and certificates are accepted;
(b) Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive data during transmission over public or private networks;
    i. Examples of public networks include, but are not limited to:
        1. The Internet;
        2. Wireless technologies;
        3. Global System for Mobile communications (GSM); and
        4. General Packet Radio Service (GPRS).
    ii. Examples of private networks include, but are not limited to:

[227] PCI DSS 1.3.8
[228] NIST 800-53 SC-7(18) | NIST CSF PR.PT-5
[229] NIST 800-53 SC-8 | NIST 800-171 3.13.8 | HIPAA 164.312(e)(2)(i) | PCI DSS 4.1 | NIST CSF PR.DS-2 & PR.DS-5 | NY DFS 500.15

1. Local Area Networks (LAN); and
2. Virtual Private Network (VPN).

(c) Verify that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized leading practices; and

(d) Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations. For TLS implementations:
   i. Verify that HTTPS appears as a part of the browser Universal Record Locator (URL); and
   ii. Verify that no sensitive data is required when HTTPS does not appear in the URL.

Supplemental Guidance: This control applies to both internal and external networks. For distributed systems including, for example, service-oriented architectures, this control applies to end-to-end integrity between the system components/services originating the transmitted information and the system components/services receiving the transmitted information. Organizations relying on commercial service providers offering transmission services as commodity items rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, EAP Expert may implement appropriate compensating security controls or explicitly accept the additional risk.

National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the data and/or system.

Enhancements:
- SC-08(a) – Cryptographic or Alternate Physical Protection

SC-08(A): TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION

Control Objective: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information; detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards. [230]

Standard: Unless otherwise protected by EAP Expert-defined alternative physical safeguards, information systems must:

(a) Implement cryptographic mechanisms to prevent unauthorized disclosure of information; and

(b) Detect changes to information during transmission.

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.

National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or system.

Enhancements: None

SC-09: TRANSMISSION CONFIDENTIALITY

[Control Withdrawn – Incorporated Into SC-08]

SC-10: NETWORK DISCONNECT

Control Objective: Systems terminate remote sessions at the end of the session or after an organization-defined time period of inactivity.[231]

Standard: Asset custodians and data/process owners are required to configure systems to terminate sessions and require users to re-authenticate to re-activate a terminal or session if a session has been idle for more than sixty (60) minutes.

[230] HIPAA 164.312(e)(1) & 164.312(e)(2)(i) | MA201CMR17 17.04(3) | OR646A.622(2)(d)(C)(iii) | NY DFS 500.15
[231] PCI DSS 8.1.8

Supplemental Guidance: This control applies to both internal and external networks and local and remote connections.

Enhancements: None

SC-11: Trusted Path

Control Objective: Systems establish a trusted communications path between the user and the security functions of the system.

Standard: Where technically feasible, systems must authenticate with Active Directory (AD).

Supplemental Guidance: A trusted path is simply some mechanism that provides confidence that the user is communicating with what the user intended to communicate with, ensuring that attackers can't intercept or modify whatever information is being communicated. The traditional example is a "fake login" program (e.g., a program is written to look like the login screen of a system) where users try to log in, the fake login program can then capture user passwords for later use.

Microsoft's Active Directory provides a trusted path to its login window by requiring the user to press Ctrl+Alt+Del. This key sequence causes a non-maskable interrupt that can only be intercepted by the operating system, thus guaranteeing that the login window cannot be spoofed by any application.

Enhancements: None

SC-12: Cryptographic Key Establishment & Management

Control Objective: The organization establishes and manages cryptographic keys for required cryptography employed within systems.[232]

Standard: Asset custodians responsible for Public Key Infrastructure (PKI) are required to:

(a) Protect any keys used to secure sensitive data against disclosure and misuse;
(b) Restrict access to cryptographic keys to the fewest number of custodians necessary;
(c) Store cryptographic keys securely in the fewest possible locations and forms; and
(d) Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption, including the following:
    i. Generation of strong cryptographic keys;
    ii. Secure cryptographic key distribution; and
    iii. Secure cryptographic key storage; and
(e) Maintain a documented description of the cryptographic architecture that includes:
    i. Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date;
    ii. Description of the key usage for each key; and
    iii. Inventory of any Hardware Security Modules (HSMs) and other Secure Cryptographic Devices (SCDs) used for key management.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters.

National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the data and/or system.

Enhancements:

- SC-12(a) – Symmetric Keys
- SC-12(b) – Asymmetric Keys
- SC-12(c) – Cryptographic Key Loss or Change
- SC-12(d) – Control & Distribution of Cryptographic Keys

[232] PCI DSS 3.5, 3.5.1-3.5.4, 3.6 & 3.6.1-3.6.3

SC-12(A): CRYPTOGRAPHIC KEY ESTABLISHMENT & MANAGEMENT | SYMMETRIC KEYS

Control Objective: The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes.

Standard: Where technically feasible, EAP Expert shall produce, control, and distribute symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes.

Supplemental Guidance: None

SC-12(B): CRYPTOGRAPHIC KEY ESTABLISHMENT & MANAGEMENT | ASYMMETRIC KEYS

Control Objective: The organization produces, controls, and distributes asymmetric cryptographic keys using approved key management technology and processes that protect the user's private key.

Standard: Where technically feasible, EAP Expert shall produce, control, and distribute asymmetric cryptographic keys using approved key management technology and processes that protect the user's private key.

Supplemental Guidance: None

SC-12(C): CRYPTOGRAPHIC KEY ESTABLISHMENT & MANAGEMENT | CRYPTOGRAPHIC KEY LOSS OR CHANGE

Control Objective: The organization maintains the availability of information in the event of the loss of cryptographic keys by users.[233]

Standard: Asset custodians responsible for Public Key Infrastructure (PKI) are required to:

(a) Change cryptographic keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry-recognized leading practices and guidelines;
(b) Retire or replace (e.g., archive, destroy, and/or revoke) keys as deemed necessary when the integrity of the key has been weakened (e.g., departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised; and
(c) Use archived cryptographic keys only for decryption/verification purposes.

Supplemental Guidance: National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the data and/or system.

SC-12(D): CRYPTOGRAPHIC KEY ESTABLISHMENT & MANAGEMENT | CONTROL & DISTRIBUTION OF CRYPTOGRAPHIC KEYS

Control Objective: The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using organization-approved key management technology and processes.[234]

Standard: Asset custodians responsible for Public Key Infrastructure (PKI) are required to:

(a) Use split knowledge and dual control (e.g., require two or three people, each knowing only their own key component, to reconstruct the whole key) if manual, clear-text cryptographic key management operations are used. Examples of manual key management operations include, but are not limited to:
    1. Key generation;
    2. Transmission;
    3. Loading;
    4. Storage; and
    5. Destruction.
(b) Prevent the unauthorized substitution of cryptographic keys; and
(c) Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

Supplemental Guidance: National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the data and/or system.

[233] PCI DSS 3.6.4 & 3.6.5
[234] PCI DSS 3.6.6-3.6.8

SC-13: Use of Cryptography

Control Objective: Systems implement required cryptographic protections using cryptographic modules that comply with applicable local, state, and federal laws, as well as non-regulatory requirements that the organization is contractually bound to address.[235]

Standard: Asset custodians and data/process owners are required to ensure systems storing, processing or transmitting sensitive information:

(a) Employ cryptographic mechanisms;
(b) Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive data during transmission over public or private networks;
(c) Verify that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized leading practices; and
(d) Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.

Supplemental Guidance: This control does not impose any requirements on organizations to use cryptography. Rather, if cryptography is required based on the selection of other controls and subsequently implemented by organizational systems, the cryptographic modules comply with applicable laws, policies, regulations, standards, and guidance.

National Institute of Science & Technology (NIST) guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the data and/or system.

SC-14: Public Access Protections

Control Objective: The organization protects the integrity and availability of publicly available information and applications.

Standard: Users are required to take reasonable measures to protect the integrity and availability of publicly available information and applications, commensurate with the sensitivity of the data being distributed.

Supplemental Guidance: This control addresses the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

Enhancements: None

SC-15: Collaborative Computing Devices

Control Objective: Systems prohibit remote activation of collaborative computing devices with the following exceptions:

- Networked whiteboards;
- Cameras; and
- Microphones.

Standard: Asset custodians and data/process owners are required to configure systems to provide an explicit indication of use that includes signaling to users when collaborative computing devices are activated.

Supplemental Guidance: Collaborative computing devices include, for example, networked whiteboards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Enhancements: None

SC-16: Transmission of Security Attributes

Control Objective: Systems associate security attributes with information exchanged between systems.

Standard: EAP Expert is required to configure systems to use Public Key Infrastructure (PKI) to validate the integrity of transmitted security attributes.

[235] HIPAA 164.312(e)(2)(ii) | PCI DSS 2.2.3 & 4.1 | NIST CSF PR.DS-5

Supplemental Guidance: Security attributes can be explicitly or implicitly associated with the information contained in systems or system components.

Enhancements: None

SC-17: Public Key Infrastructure (PKI) Certificates

Control Objective: The organization issues public key certificates under an organization-defined certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Standard: Asset custodians responsible for publicly-facing Public Key Infrastructure (PKI) are required to provide the following PKI management services:

(a) Certificate creation;
(b) Certificate signing;
(c) Certificate revocation;
(d) Key management;
(e) Publication of certificate revocation lists (CRLs); and
(f) Authority revocation lists (ARLs).

Supplemental Guidance: This control addresses certificates with visibility external to EAP Expert systems and does not address certificates related to the internal operations of systems, for example, application-specific time services.

Enhancements: None

SC-18: Mobile Code

Control Objective: The organization:[236]

- Defines acceptable and unacceptable mobile code and mobile code technologies;
- Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- Authorizes, monitors, and controls the use of mobile code within systems.

Standard: Asset custodians and data/process owners are required to manage the use of mobile code technologies through:

(a) Defining acceptable and unacceptable mobile code and mobile code technologies;
(b) Establishing usage restrictions for mobile code and mobile code technologies; and
(c) Developing secure system configurations to address mobile code usage within systems that include, but is not limited to:
    i. Preventing the download and execution of prohibited mobile code; and
    ii. Preventing the automatic execution of mobile code.

Supplemental Guidance: Decisions regarding the employment of mobile code within EAP Expert's systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smartphones).

The following mobile code and mobile code technologies are defined below as High Risk, Moderate Risk, and Low Risk:

- High Risk: Mobile code technologies that exhibit functionality allowing unmediated access to host and remote system services and resources.
- Medium Risk: Mobile code technologies that have functionality allowing mediated or controlled access to local system services and resources.
- Low Risk: Mobile code technologies that have functionality with no capability for unmediated access to local system services and resources.

Ensure usage restrictions and implementation guidelines for mobile code and mobile code technologies are limited to:

- Intranet Usage – Low, Medium, and High risk mobile code is permitted in controlled and trusted environments; and
- Internet Usage – All High risk mobile code will be blocked or disabled for Internet browsing sessions.

[236] NIST CSF DE.CM-5

Enhancements: None

SC-19: Communications Technologies

Control Objective: The organization establishes usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.

Standard: Human Resources (HR) is responsible for establishing usage restrictions and implementation guidance for the following communications technologies based on the potential to cause damage to systems, if used maliciously:

(a) Electronic Mail (email);
(b) Instant Messaging (IM);
(c) Short Message Service (SMS);
(d) Voice Over Internet Protocol (VOIP);
(e) Analog Lines (Plain Old Telephone Service (POTS)); and
(f) Facsimile (Fax) Machines (analog & digital).

Supplemental Guidance: None

Enhancements: None

SC-20: Secure Name / Address Resolution Service (Authoritative Source)

Control Objective: Systems provide additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Standard: EAP Expert is required to use trusted sources for authoritative DNS queries to prevent DNS spoofing attacks.

Supplemental Guidance: Recommended settings for primary and alternate DNS sources include those provided EAP Expert's the Internet Service Provider (ISP) or a trusted service provider. This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include, for example, domain name system (DNS) servers.

Both IPv4 and IPv6 DNS should be addressed:

- IPv4: The Google Public DNS IP addresses (IPv4) are as follows:[237]
  - 8.8.8.8
  - 8.8.4.4
- IPV6: The Google Public DNS IPv6 addresses are as follows:
  - 2001:4860:4860::8888
  - 2001:4860:4860::8844

Enhancements: None

SC-21: Secure Name / Address Resolution Service (Recursive or Caching Resolver)

Control Objective: Systems perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

Standard: Asset custodians are required to configure internal DNS queries to use recursive or cached name resolution.

Supplemental Guidance: Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

Enhancements: None

[237] Google DNS - http://code.google.com/speed/public-dns/docs/using.html

SC-22: Architecture & Provisioning For Name / Address Resolution Service

Control Objective: Systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Standard: Asset custodians responsible for Domain Name System (DNS) are required to:

(a) Ensure DNS Servers providing name/address resolution service are fault tolerant and implement internal/external role separation;
(b) Ensure primary and secondary authoritative DNS servers are on separate subnets at separate locations;
(c) Ensure DNS servers with an internal role only process name/address resolution requests from internal clients; and
(d) Ensure DNS servers with an external role only process name/address resolution requests from external clients.

Supplemental Guidance: Systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server, and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically-separated network subnetworks (e.g., not located in the same physical facility). For role separation, DNS servers with internal roles, only process name, and address resolution requests from within organizations (e.g., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (e.g., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).

Enhancements: None

SC-23: Session Authenticity

Control Objective: Systems provide mechanisms to protect the authenticity of communications sessions.

Standard: Where technically feasible and a business reason exists, EAP Expert is required to implement authenticity protection mechanisms to protect the integrity of session communications.

Supplemental Guidance: This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

Enhancements: None

SC-24: Fail In Known State

Control Objective: Systems fail to an organization-defined known-state for types of failures, preserving system state information in failure.

Standard: Where technically feasible and a business reason exists, asset custodians and data/process owners are required to maintain a mirrored, clustered or failover system as part of the Disaster Recovery Plan (DRP) / Continuity of Operations Plan (COOP) for critical systems so that, upon failure of the primary system, the mirror/failover system can assume the primary role while the failed system is repaired or replaced.

Supplemental Guidance: Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps prevents the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.

Any controls that are implemented should be documented and retained across the life cycle of the system to document the process for failing to a known state.

Enhancements: None

SC-25: Thin Nodes

Control Objective: Systems employ processing components that have minimal functionality and information storage.

Standard: Where technically feasible and a business reason exists, EAP Expert authorizes the use of thin clients in scenarios where the physical security of a workstation cannot be guaranteed, such as kiosks, or where system customization is not permitted.

Supplemental Guidance: The deployment of system components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, systems, and services to cyber-attacks.

Enhancements: None

SC-26: Honeypots

Control Objective: Systems include components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Standard: Where technically feasible and a business reason exists, EAP Expert approves the use of honeypots on an "as needed" basis with the requirement that prior to the use of a honeypot in a production environment in a production environment, a comprehensive methodology governing its use is developed and implemented that covers:

(a) Clear objectives;
(b) The responsible design of the honey pot system:
    i. Minimize negative exposures; and
    ii. Maximize data collection capabilities; and
(c) Sufficient resources and proper training.

Supplemental Guidance: A honey pot is a computer system set up expressly to attract and "trap" individuals who are attempting to penetrate a network. Honey pots serve their purpose by diverting intruders away from legitimate production systems, which increases the amount of time IT personnel have to identify the activity and develop countermeasures. Honey pots are not recommended for the purpose of intrusion prevention since they do not prevent exploits from happening.

Should an individual wish to proceed with implementing a honeypot, both EAP Expert & legal counsel should review the proposed solution, since it could have legal implications.

Enhancements: None

SC-27: Operating System-Independent Applications

Control Objective: The organization addresses operating system-independent applications.

Standard: Asset custodians are required to:

(a) Manage operating system-independent applications, based on the threat posed since operating system-independent applications are applications that can run on multiple operating systems; and
(b) Uninstall operating system-independent applications from systems where the applications are not required for a business purpose.

Supplemental Guidance: Operating system indepenent applications (e.g., Java, Flash, QuickTime, etc.) promote functionality across platforms, but are considered security risks. Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability of critical functions within organizations while systems with specific operating systems are under attack.

Enhancements: None

SC-28: Encrypting Data At Rest

Control Objective: Systems protect the confidentiality and integrity of information at rest.[238]

Standard: Asset custodians and data/process owners are required to protect sensitive information by:

(a) Employing cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.
    i. If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases);
(b) Rendering sensitive data unreadable anywhere it is stored; and
(c) Not tying user accounts to decryption keys.

Supplemental Guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved.

Enhancements:

- SC-28(a) – Cryptographic Protection

SC-28(a): Encrypting Data at Rest | Cryptographic Protection

Control Objective: The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of information on information system components.[239]

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information on information system components.

Supplemental Guidance: Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

SC-29: Heterogeneity

Control Objective: The organization employs a diverse set of information technologies for system components in the implementation of the system.

Standard: EAP Expert's network and Cybersecurity architects are required to develop solutions that implement a defense-in-depth architecture that follow industry-recognized leading practices.

Supplemental Guidance: Increasing the diversity of information technologies within organizational systems reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber-attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations.

Enhancements:

- SC-29(a) – Virtualization Techniques

[238] HIPAA 164.312(a)(b)(iv) | PCI DSS 3.4 & 3.4.1 | MA201CMR17 17.04(5) | OR646A.622(2)(d)(C)(iii) | NIST CSF PR.DS-1 | NY DFS 500.15
[239] NY DFS 500.15

SC-29(A): HETEROGENEITY | VIRTUALIZATION TECHNIQUES

Control Objective: The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed at an organization-defined frequency.

Standard: EAP Expert's network and Cybersecurity architects must approve virtualization techniques.

Supplemental Guidance: Changing virtual operating systems or applications, as opposed to changing actual operating systems/applications, provide virtual changes that impede attacker success while reducing configuration management efforts. In addition, virtualization techniques can assist organizations in isolating untrustworthy software and/or software of dubious provenance into confined execution environments.

SC-30: CONCEALMENT & MISDIRECTION

Control Objective: The organization employs concealment and misdirection techniques for systems at organization-defined time periods to confuse and mislead adversaries.

Standard: Where technically feasible and a strong business need exists, EAP Expert's Cybersecurity personnel may employ concealment and misdirection techniques for systems at organization-defined time periods to confuse and mislead adversaries.

Supplemental Guidance: Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (e.g., the window of opportunity and available attack surface) to initiate and complete cyber-attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or expose tradecraft.

Enhancements: None

SC-31: COVERT CHANNEL ANALYSIS

Control Objective: The organization:[240]

- Performs a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert channels; and
- Estimates the maximum bandwidth of those channels.

Standard: The responsible party for EAP Expert's technology infrastructure is authorized to employ the following methods to perform covert channel analysis:

(a) Test a subset of possible covert channels to determine which channels are exploitable;
(b) Reduce the maximum bandwidth for identified covert channels; and
(c) Measure the bandwidth of possible covert channels to identify covert channel usage.

Supplemental Guidance: Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of systems containing export-controlled information and having connections to external networks (e.g., networks not controlled by organizations). Covert channel analysis is also meaningful for multilevel secure (MLS) systems, multiple security level (MSL) systems, and cross-domain systems.

Enhancements: None

SC-32: INFORMATION SYSTEM PARTITIONING

Control Objective: The organization partitions the system so that partitions reside in separate physical domains or environments.

Standard: Where technically feasible and a strong business need exists, asset custodians are required to partition critical systems to reside in separate physical domains or environments.

[240] NIST CSF PR.DS-5

Supplemental Guidance: System partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.

Enhancements: None

SC-33: Transmission Preparation Integrity

[Control Withdrawn: Incorporated Into SC-08]

SC-34: Non-Modifiable Executable Programs

Control Objective: Systems:

- Load and execute the operating environment from hardware-enforced, read-only media; and
- Load and execute applications from hardware-enforced, read-only media.

Standard: Where technically feasible and a business need exists, EAP Expert may employ systems with no writeable storage that is persistent across component restart or power on/off.

Supplemental Guidance: The term operating environment is defined as the specific code that hosts applications, for example, operating systems, executives, or monitors including virtual machine monitors (e.g., hypervisors). It can also include certain applications running directly on hardware platforms. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image.

Enhancements: None

SC-35: Honeyclients

Control Objective: Systems include components that proactively seek to identify malicious websites and/or web-based malicious code.

Standard: Where technically feasible and a business reason exists, EAP Expert approves the use of honeyclients on an "as needed" basis with the requirement that prior to the use of a honeyclient in a production environment, a comprehensive methodology governing its use is developed and implemented that covers:

(a) Clear objectives;
(b) The responsible design of the honeyclient system:
    i. minimize negative exposures; and
    ii. maximize data collection capabilities; and
(c) Sufficient resources and proper training.

Supplemental Guidance: Honeyclients differ from honeypots in that the components actively probe the Internet in search of malicious code (e.g., worms) contained on external websites. As with honeypots, honeyclients require some supporting isolation measures (e.g., virtualization) to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational systems.

Enhancements: None

SC-36: Distributed Processing & Storage

Control Objective: The organization distributes processing and storage across multiple physical locations.

Standard: Where technically feasible and a strong business need exists, EAP Expert shall employ polling techniques to identify potential faults, errors, or compromises to distributed processing and storage components.

Supplemental Guidance: Distributing processing and storage across multiple physical locations provide some degree of redundancy or overlap for organizations and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage.

Enhancements: None

SC-37: Out-of-Band Channels

Control Objective: The organization employs organization-defined out-of-band channels for the physical delivery or electronic transmission of information, system components, or devices to authorized individuals.

Standard: Asset custodians and data/process owners are required to employ security safeguards to ensure that only authorized individuals receive information, system components, or devices through out-of-band channel delivery.

Supplemental Guidance: Out-of-band channels include, for example, local (non-network) accesses to systems, network paths physically separate from network paths used for operational traffic, or non-electronic paths such as the US Postal Service.

Enhancements: None

SC-38: Operations Security

Control Objective: The organization employs organization-defined operations security safeguards to protect the organization.

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are responsible for developing, publishing and governing Operational Security (OPSEC) controls.

Supplemental Guidance: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps:

- Identification of critical information (e.g., the security categorization process);
- Analysis of threats;
- Analysis of vulnerabilities;
- Assessment of risks; and
- The application of appropriate countermeasures.

Enhancements: None

SC-39: Process Isolation

Control Objective: The system maintains a separate execution domain for each executing process.

Standard: Where technically feasible and a strong business need exists, asset custodians are required to implement a separate execution domain for each executing process.

Supplemental Guidance: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled by the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.

Enhancements:

- SC-39(a) – Hardware Separation
- SC-39(b) – Thread Separation

SC-39(a): Process Isolation | Hardware Separation

Control Objective: Systems implement underlying hardware separation mechanisms to facilitate process separation.

Standard: Where technically feasible and a strong business need exists, asset custodians are required to configure systems to implement underlying hardware separation mechanisms to facilitate process separation.

Supplemental Guidance: Hardware-based separation of system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Underlying hardware separation mechanisms include, for example, hardware memory management.

SC-39(B): PROCESS ISOLATION | THREAD SEPARATION

Control Objective: Systems maintain a separate execution domain for each thread in multi-threaded processing.

Standard: Where technically feasible and a strong business need exists, asset custodians are required to configure systems to maintain a separate execution domain for each thread in multi-threaded processing.

Supplemental Guidance: None

SC-40: WIRELESS LINK PROTECTION

Control Objective: The organization: [241]

- Protects external and internal wireless links from signal parameter attacks;
- Monitors for unauthorized wireless connections, including scanning for unauthorized wireless access points; and
- Takes appropriate action if an unauthorized connection is discovered.

Standard: The responsible parties for EAP Expert's technology infrastructure are required to:

(a) Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis:
  i. Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS; and
  ii. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices;

(b) Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:
  i. WLAN cards inserted into system components;
  ii. Portable wireless devices connected to system components (e.g., PCMCIA card, USB, etc.); and
  iii. Wireless devices attached to a network port or network device;

(c) Maintains an inventory of authorized wireless access points including a documented business justification;

(d) Implement incident response procedures in the event unauthorized wireless access points are detected;

(e) Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities. If automated monitoring is utilized (e.g., wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel; and

(f) Verify EAP Expert's Incident Response Plan (IRP) includes a response in the event unauthorized wireless devices are detected.

Supplemental Guidance: This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized system users. This control reduces the impact of attacks that are unique to wireless systems.

Enhancements: None

SC-41: PORT & I/O DEVICE ACCESS

Control Objective: The organization physically disables or removes connection ports or input/output devices on sensitive systems or system components.

Standard: Where technically feasible and a strong business need exists, asset custodians shall physically disable or remove connection ports or input/output devices on sensitive systems or system components.

Supplemental Guidance: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such

[241] PCI DSS 11.1 & 11.1-11.1.2

connection ports and I/O devices helps prevent exfiltration of information from systems and the introduction of malicious code into systems from those ports/devices.

Enhancements: None

SC-42: Sensor Capability & Data

Control Objective: Systems:

- Prohibit the remote activation of environmental sensing capabilities; and
- Provides an explicit indication of sensor use to users.

Standard: Where applicable, asset custodians and data/process owners are required to configure systems to:

(a) Prohibit the remote activation of environmental sensing capabilities (e.g., GPS mechanisms); and
(b) Provides an explicit indication of sensor use to users.

Supplemental Guidance: This control often applies to types of systems or system components characterized as mobile devices, for example, smartphones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.

Enhancements: None

SC-43: Usage Restrictions

Control Objective: The organization:

- Establishes usage restrictions and implementation guidance for system components based on the potential to cause damage to the system, if used maliciously; and
- Authorizes, monitors, and controls the use of such components within the system.

Standard: Where applicable, asset custodians and data/process owners are required to take appropriate precautions to secure system components based on the potential to cause damage to the system, if used maliciously.

Supplemental Guidance: This control addresses threats that include the Aurora cyber-attack where technical configurations caused catastrophic failure of a mechanical system. System components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).

Enhancements: None

SC-44: Detonation Chambers

Control Objective: The organization employs a detonation chamber capability for systems.[242]

Standard: The Cybersecurity Officer (ISO) and his/her designated representatives are authorized to establish a segmented lab environment that provides a safe environment to execute potentially hostile commands or executables.

Supplemental Guidance: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code.

Enhancements: None

[242] NIST CSF DE.CM-5

System & Information Integrity (SI)

System & Information Integrity Policy: EAP Expert shall correct flaws in its systems in a timely manner and ensure mechanisms are in place to protect systems from malicious code.

Management Intent: The purpose of the System & Information Integrity (SI) policy is to ensure the confidentiality, integrity, and availability of EAP Expert's data.

Supporting Documentation: System & Information Integrity (SI) control objectives & standards directly support this policy.

SI-01: System & Information Integrity Policy & Procedures

Control Objective: The organization develops, disseminates, reviews & updates:

- A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Standard: EAP Expert is required to document EAP Expert-wide system and information integrity controls that, at a minimum, include:

(a) A formal, documented system and information integrity policy; and
(b) Processes to facilitate the implementation of the system and information integrity policy, procedures and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable laws, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Enhancements: None

SI-02: Flaw Remediation (Software Patching)

Control Objective: The organization:[243]

- Identifies, reports, and corrects system flaws;
- Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational systems before installation; and
- Incorporates flaw remediation into the organization's configuration management process.

Standard: Asset custodians and data/process owners are required to ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed:

(a) Install applicable, critical security patches within one (1) month of release from the vendor; and
(b) Install applicable, non-critical patches within three (3) months of release from the vendor.

Supplemental Guidance: Organizations identify systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with cybersecurity responsibilities. Security-relevant software updates include, for example, patches, service packs, hotfixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts.

[243] PCI DSS 6.1 & 6.2 | MA201CMR17 17.04(6) | OR646A.622(2)(d)(B)(iii) | NIST CSF ID.RA-1 & PR.IP-12

EAP Expert is required to ensure it maintains its cybersecurity solutions by ensuring Systems are maintained and kept updated to manufacturer's specifications. This will help ensure that existing solutions are up to date and operating properly.

Enhancements:

- SI-02(a) – Centralized Management
- SI-02(b) – Automated Flaw Remediation Status
- SI-02(c) – Time To Remediate Flaws / Benchmarks For Corrective Action

SI-02(A): FLAW REMEDIATION | CENTRALIZED MANAGEMENT

Control Objective: The organization centrally manages the flaw remediation process.[244]

Standard: Asset custodians and data/process owners are required to centrally manage the flaw remediation process that includes, but is not limited to the following:

(a) Documentation of impact;
(b) Documented change approval by authorized parties;
(c) Functionality testing to verify that the change does not adversely impact the security of the system;
(d) Back-out procedures; and
(e) Upon completion of significant change, all relevant compliance requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

Supplemental Guidance: Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls. Asset custodians should use the following process to help ensure patches do not compromise the security of the information resources being patched:

- Obtain the patch from a known, trusted source;
- Verify the integrity of the patch through such means as comparisons of cryptographic hashes to ensure the patch obtained is the correct, unaltered patch;
- Apply the patch to an isolated test system and verify that the patch:
    - Is compatible with other software used on systems to which the patch will be applied;
    - Does not alter the system's security posture in unexpected ways, such as altering log settings; and
    - Corrects the pertinent vulnerability.
- Backup production systems prior to applying the patch;
- Apply the patch to production systems using secure methods, and update the cryptographic checksums of key files as well as that system's software archive; and
- Create and document an audit trail of all changes.

SI-02(B): FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Control Objective: The organization employs automated mechanisms to determine the state of information system components with regard to flaw remediation.

Standard: Where technically feasible, EAP Expert shall employ automated mechanisms to determine the state of information system components with regard to flaw remediation.

Supplemental Guidance: None

SI-02(C): FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTION

Control Objective: The organization:

- Measures the time between flaw identification and flaw remediation; and
- Establishes metrics / benchmarks for taking corrective actions.

Standard: Where technically feasible, EAP Expert shall collect metrics associated with flaw remediation and provide metrics reports to key stakeholders.

Supplemental Guidance: This requires EAP Expert to determine the current time it takes on the average to correct information system flaws after such flaws have been identified, and subsequently establish benchmarks (e.g., time frames) for taking corrective actions. Benchmarks can be established by type of flaw and/or severity of the potential vulnerability if the flaw can be exploited.

[244] PCI DSS 6.2, 6.4.5, 6.4.5.1-6.4.5.4 & 6.4.6 | MA201CMR17 17.04(7)

SI-03: Malicious Code Protection (Malware)

Control Objective: The organization:[245]

- Employs malicious code protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
  - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
  - Inserted through the exploitation of system vulnerabilities;
- Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;
- Configures malicious code protection mechanisms to:
  - Perform periodic scans of the system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;
  - Quarantines malicious code; send alert to an administrator; in response to malicious code detection; and
- Addresses the receipt of false positives during malicious code detection.

Standard: EAP Expert is required to deploy anti-malware software on all systems commonly affected by malicious software, including but not limited to:

(a) Servers;
(b) Workstations;
(c) Laptops;
(d) Tablets; and
(e) Smartphones.

Supplemental Guidance: System entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware.

Enhancements:

- SI-03(a) – Central Management
- SI-03(b) – Automatic Updates
- SI-03(c) – Nonsignature-Based Detection
- SI-03(d) – Malware Protection Mechanism Testing
- SI-03(e) – Evolving Malware Threats
- SI-03(f) – Always On Protection

SI-03(a): Malicious Code Protection | Central Management

Control Objective: The organization centrally manages malicious code protection mechanisms.

Standard: EAP Expert's Cybersecurity personnel are responsible for selecting and implementing the approved application for centrally managing host-based, malicious code protection mechanisms.

Supplemental Guidance: None

SI-03(b): Malicious Code Protection | Automatic Updates

Control Objective: The system automatically updates malicious code protection mechanisms (including signature definitions). [246]

Standard: Asset custodians are required to ensure anti-malware software is configured to automatically update malicious code protection mechanisms.

Supplemental Guidance: None

SI-03(c): Malicious Code Protection | Nonsignature-Based Detection

Control Objective: The information system implements nonsignature-based malicious code detection mechanisms.

[245] HIPAA 164.308(a)(5)(ii)(B) | PCI DSS 5.1, 5.1.1 & 5.2 | MA201CMR17 17.04(7) | NIST CSF DE.CM-4 & DE.DP-3
[246] PCI DSS 5.2

Standard: Where technically feasible, EAP Expert shall implement nonsignature-based malicious code detection mechanisms.

Supplemental Guidance: Nonsignature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (e.g., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.

SI-03(D): MALICIOUS CODE PROTECTION | MALWARE PROTECTION MECHANISM TESTING

Control Objective: The organization tests malicious code protection mechanisms by introducing a known benign, non-spreading test case into the system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.

Standard: Asset custodians are required to use the European Institute of Computer Anti-virus Research (EICAR) Standard Anti-Virus Test File to ensure anti-malware software is properly detecting and removing threats.

Supplemental Guidance: None

SI-03(E): MALICIOUS CODE PROTECTION | EVOLVING MALWARE THREATS

Control Objective: The organization performs periodic evaluations to identify and evaluate evolving malware threats for systems considered to be not commonly affected by malicious software. [247]

Standard: EAP Expert's Cybersecurity personnel are responsible for developing and implementing the process for periodic evaluations to identify and evaluate evolving malware threats for systems considered to be not commonly affected by malicious software.

Supplemental Guidance: None

SI-03(F): MALICIOUS CODE PROTECTION | ALWAYS ON PROTECTION

Control Objective: The organization ensures that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited time period. [248]

Standard: EAP Expert's Cybersecurity personnel are responsible for ensuring that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited time period.

Supplemental Guidance: Anti-virus solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.

SI-04: INFORMATION SYSTEM MONITORING

Control Objective: The organization:[249]

- Monitors events on systems in accordance with organization-defined monitoring objectives and detects system attacks;
- Identifies unauthorized use of systems; and
- Heightens the level of system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, or other organizations, based credible sources of information.

Standard: EAP Expert management is responsible for developing and implementing daily, operational cybersecurity procedures that are consistent with legal and contractual requirements.

Supplemental Guidance: System monitoring includes external and internal monitoring and the collection of monitoring data will be limited to justifiable business and legal purposes.

---

[247] PCI DSS 5.1.2

[248] PCI DSS 5.3

[249] HIPAA 164.308(a)(1)(ii)(D) & 164.308(a)(5)(ii)(C) | PCI DSS 11.4 | MA201CMR17 17.03(2)(b)(c) & 17.04(4) | NIST CSF ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-5, DE.CM-6, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 & RS.CO-3

- External monitoring includes the observation of events occurring at the system boundary (e.g., part of perimeter defense and boundary protection).
- Internal monitoring includes the observation of events occurring within the system.

Monitoring is necessary to ensure that only authorized processes are being performed. The level of monitoring required will depend upon the business function in question. All monitoring activities will be formally authorized by management.

Enhancements:
- SI-04(a) – Near Real-Time Analysis & Alerting
- SI-04(b) – Automated Tools for Real-Time Analysis
- SI-04(c) – Inbound & Outbound Communications Traffic
- SI-04(d) – System-Generated Alerts
- SI-04(e) – Wireless Intrusion Detection
- SI-04(f) – Correlate Monitoring Information
- SI-04(g) – Host-Based Devices

SI-04(A): INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEMS

Control Objective: The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

Standard: Where technically feasible, EAP Expert shall connect and configure individual intrusion detection tools into an information system-wide intrusion detection system.

Supplemental Guidance: None

SI-04(B): INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

Control Objective: The organization employs automated tools to support real-time analysis of events. [250]

Standard: For critical systems, EAP Expert Cybersecurity personnel are responsible for correlating information and generating near real-time alerts from monitoring tools employed throughout the network to achieve organization-wide situational awareness.

Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

SI-04(C): INFORMATION SYSTEM MONITORING | INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC

Control Objective: The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

Standard: EAP Expert is required to monitor inbound and outbound communications for unusual or unauthorized activities or conditions.

Supplemental Guidance: Unusual/unauthorized activities or conditions include, but is not limited to:
- Internal traffic that indicates the presence of malicious code within a system or propagating among system components,
- Internal traffic that indicates the presence of unauthorized software (e.g., Peer-to-Peer software); and
- The unauthorized export of information, or signaling to an external system.

SI-04(D): INFORMATION SYSTEM MONITORING | SYSTEM GENERATED ALERTS

Control Objective: The organization correlates results from monitoring physical, cyber, and supply chain activities to achieve integrated situational awareness.

Standard: EAP Expert is responsible for developing and implementing an integrated situational awareness capability to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out the attacks.

Supplemental Guidance: Situational awareness involves being aware of the following:
- Physical security incidents;

[250] PCI DSS 10.6, 10.6.1, 10.6.2 & 10.6.3

- Supply chain incidents;
- Industry-specific incidents; and
- Technology-specific incidents (related to technology current in use on the production network).

SI-04(E): INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

Control Objective: The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. [251]

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Supplemental Guidance: Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing information systems, but also include areas outside of facilities as needed, to verify that unauthorized wireless access points are not connected to the systems.

SI-04(F): INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

Control Objective: The organization correlates information from monitoring tools employed throughout the information system.

Standard: EAP Expert shall correlate information from monitoring tools employed throughout the organization.

Supplemental Guidance: Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs.

SI-04(G): INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES

Control Objective: The organization implements host-based monitoring mechanisms on information system components.

Standard: Where technically feasible and justified by a valid business case, EAP Expert shall implement host-based monitoring mechanisms on information system components.

Supplemental Guidance: Information system components where host-based monitoring can be implemented include, for example, servers, workstations, and mobile devices. Organizations consider employing host-based monitoring mechanisms from multiple information technology product developers.

SI-05: SECURITY ALERTS, ADVISORIES & DIRECTIVES

Control Objective: The organization:[252]

- Receives system security alerts, advisories, and directives from designated external organizations on an ongoing basis; and
- Generates internal security alerts, advisories, and directives as deemed necessary.

Standard: EAP Expert Cybersecurity personnel responsible for incident response operations are required to utilize automated mechanisms to receive security alert and advisory information.

Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government.

Enhancements: None

SI-06: SECURITY FUNCTIONALITY VERIFICATION

Control Objective: Systems are verified to correctly process security functions when anomalies are discovered.

---

[251] PCI DSS 11.1

[252] OR646A.622(2)(d)(B)(iii) | NIST CSF ID.RA-1, ID.RA-2, ID.RA-3 & RS.CO-5

Standard: Asset custodians are required to test security-related tools (e.g., antivirus software) to ensure systems provide notification of failed events.

Supplemental Guidance: After major changes or software upgrades, it is recommended to test security-related tools to ensure the change did not disable the functionality of the security tool.

An example of security functionality verification is the European Institute of Computer Antivirus Research (EICAR) Standard Anti-Virus Test File, which is used to ensure anti-malware software is properly detecting and removing threats.

Enhancements: None

SI-07: Software, Firmware & Information Integrity

Control Objective: Systems detect unauthorized changes to software and information.[253]

Standard: On critical systems, asset custodians are required to:

(a) Deploy File Integrity Monitoring (FIM) tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly;
(b) Verify the use of FIM tools by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:
    i. System executables;
    ii. Application executables;
    iii. Configuration and parameter files; and
    iv. Centrally stored, historical or archived, log and audit files.
(c) Verify the tools are configured to alert personnel to unauthorized modification of critical files and to perform critical file comparisons at least weekly.

Supplemental Guidance: Cybersecurity integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of systems and hosted applications. Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. The firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with the information.

Enhancements:

- SI-07(a) – Integrity Checks
- SI-07(b) – Integration of Detection & Response

SI-07(a): Software, Firmware & Information Integrity | Integrity Checks

Control Objective: The information system performs an integrity check of organization-defined software, firmware, and information at:

- Startup;
- At organization-defined transitional states or security-relevant events; or
- At an organization-defined frequency.

Standard: Where technically feasible, system will perform an integrity check of organization-defined software, firmware, and information at:

(a) Startup; or
(b) Upon security-relevant events.

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

[253] PCI DSS 11.5 & 11.5.1 | NIST CSF PR.DS-6

SI-07(B): Software, Firmware & Information Integrity | Integration of Detection & Response

Control Objective: The organization incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.

Standard: Where technically feasible, EAP Expert shall incorporate the detection of unauthorized security-relevant changes to the information system into EAP Expert's incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.

SI-08: Spam Protection

Control Objective: The organization:

- Employs spam protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
- Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

Standard: EAP Expert is required to centrally manage spam protection mechanisms, including signature definitions, in an effort to reduce the introduction of malicious software to client systems.

Supplemental Guidance: System entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.

Enhancements:

- SI-08(a) – Central Management
- SI-08(b) – Automatic Updates

SI-08(A): Spam Protection | Central Management

Control Objective: The organization centrally manages spam protection mechanisms.

Standard: Where technically feasible, EAP Expert shall centrally manage the spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.

SI-08(B): Spam Protection | Automatic Updates

Control Objective: The information system automatically updates spam protection mechanisms.

Standard: Where technically feasible, information systems must automatically update spam protection mechanisms.

Supplemental Guidance: None

SI-09: Information Input Restrictions

Control Objective: The organization restricts the capability to input information to systems to authorized personnel.

Standard: On custom-developed applications and web pages, asset custodians and data/process owners are required to enforce rules to require inputs to be prescreened to prevent the content from being unintentionally interpreted as commands.

Supplemental Guidance: Input restrictions are important to prevent against common hacking techniques that take advantage of poor software development principles (e.g., SQL injection and buffer overflow attacks).

Enhancements: None

SI-10: Input Data Validation

Control Objective: Systems check the validity of information inputs.

Standard: On custom-developed applications and web pages, asset custodians and data/process owners are required to enforce rules for checking the valid syntax and semantics of system inputs are in place to verify that inputs match specified definitions for format and content. System inputs include, but are not limited to:

(a) Character set;
(b) Length;
(c) Numerical range; and
(d) Acceptable values.

Supplemental Guidance: Checking the valid syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Prescreening inputs prior to passing to interpreters prevent the content from being unintentionally interpreted as commands. Input validation helps ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Enhancements: None

SI-11: Error Handling

Control Objective: Systems:

- Identify potentially security-relevant error conditions;
- Generate error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and
- Reveal error messages only to authorized personnel.

Standard: Asset custodians and data/process owners are required to examine the structure and content of error messages to identify how error conditions are handled for systems.

Supplemental Guidance: Asset custodians and data/process owners are required to carefully consider the structure/content of error messages. Sensitive information may include, for example, erroneous login attempts with passwords entered by mistake as the username, mission or business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.

Enhancements: None

SI-12: Information Output Handling & Retention

Control Objective: The organization handles and retains both information within and output from systems in accordance with applicable local, state, and Federal laws, as well as regulatory requirements.[254]

Standard: EAP Expert is required to design, implement and maintain a data retention program for the systematic retention and destruction of physical and digital documents based on statutory and regulatory record-keeping requirements and practical business needs that include:

(a) Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements;
(b) Processes for secure deletion of data when no longer needed;
(c) Specific retention requirements for cardholder data; and
(d) A quarterly process (automatic or manual) for identifying and securely deleting stored sensitive data that exceeds defined retention requirements.

Supplemental Guidance: The retention of data (e.g., paper documents, backup tapes, email messages and other media) not otherwise necessary to conduct business is both expensive and inefficient. Unnecessary retention could leave EAP Expert open to potential legal

[254] PCI DSS 3.1 & 10.7 | OR646A.622(b)(C)(i) & (iv) | NY DFS 500.13

challenges on grounds based on the outdated and irrelevant material. Retention periods are based primarily on current Federal record-keeping requirements, state statutes of limitation, and industry-recognized leading practices for document retention.

Security controls shall be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system. Security controls must be designed and maintained to ensure compliance with all legal requirements. Appendix B: Data Classification Examples contains a list of common media types and recommended retention periods.

The output handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of systems.

Currently Relevant Documents
Currently relevant documents should be filed systematically for accessibility.

Permanent Retention Documents
Documents that must be maintained permanently can be cataloged and, if possible, reduced to some secure form of digital record for storage that ensures easy access when needed.

Non-Relevant Documents
Non-relevant documents should be securely destroyed. Destruction methods will be dictated by both type of media (e.g., paper, floppy disks, hard drives, emails, etc.) and the sensitivity of the data contained on the media (e.g., Personally Identifiable Information (PII), billing history, client communications, etc.).

The method of destruction for media shall follow one of the following methods, based on the type of media:

Physical Paper-Based Media
The process of shredding may be performed internally or outsourced to a trusted third-party that specializes in document destruction.

- Physical paper-based media containing non-sensitive data should be shredded but can be recycled.
- Physical paper-based media containing sensitive data (e.g., SSNs, financial information, client communications, etc.) must be shredded.

Physical Digital Media
Physical digital media (e.g., Hard Disk Drives (HDDs), flash drives, floppy drives, tape drives, etc.) must be destroyed to make recovery of data technically impossible.

- The process of destruction shall be outsourced to a trusted third-party that specializes in the physical destruction of digital media.
- HDDs must be removed from all systems, prior to the disposal of the system.
- Outsourced destruction vendors should track HDDs by serial number to ensure the secure destruction of the devices.

Digital Media
Digital media may be destroyed by the process of "deleting" files from systems and storage devices. The actual process of deleting data varies based on the type of operating system, so vendor documentation should be followed.

Enhancements: None

SI-13: Predictable Failure Analysis

Control Objective: The organization:[255]

- Determines Mean Time To Failure (MTTF) for system components in specific environments of operation; and
- Provides substitute system components and a means to exchange active and standby components at organization-defined MTTF substitution criteria.

Standard: The responsible parties for EAP Expert's technology infrastructure are required to take proactive steps to prevent downtime associated with predictable failure of system components. System components where protection takes into consideration Mean Time Between Failure (MTBF) includes, but is not limited to:

(a) Hard Disk Drives (HDD);

[255] OR646A.622(2)(d)(C)(iii)

(b) Network Interface Cards (NICs);
(c) Monitors (including video cards);
(d) Motherboard (including fans, CPUs and RAM);
(e) Power Supply Units (PSUs);
(f) Networking equipment (including firewalls, routers, switches and Wireless Access Points (WAPs)); and
(g) Direct output devices (including printers, fax machines, and copiers).

Supplemental Guidance: While MTBF is primarily a reliability issue, this control addresses potential failures of specific system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define criteria for substitution of system components based on MTBF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capability (e.g., preservation of state variables).

On critical systems, EAP Expert should ensure that the standby components successfully and transparently assume the primary role in the event of component failure (e.g., RAID array) or through a manual transfer between active and standby components, in an effort to reduce downtime.

Enhancements:
- SI-13(a) – Computer Lifecycle Plan (CLP)

SI-13(A): PREDICTABLE FAILURE ANALYSIS | COMPUTER LIFECYCLE PLAN (CLP)

Control Objective: The organization manages the lifecycles of assets.

Standard: Computer Lifecycle Plans (CLPs) are required to be developed for critical systems prior to asset's expected end of useful life, since that will reduce unexpected downtime from systems reaching the likely point of component failure, based on component Mean Time Between Failure (MTBF).

Supplemental Guidance: EAP Expert recognizes that not all users have the same processing requirements, so asset lifespans will vary based on the type of work performed on the system. Routine clerical workers requiring little more than word processing and e-mail capabilities should be categorized on the later part of the spectrum, as compared to "power users" who require cutting-edge technologies based on their performance requirements.

EAP Expert should follow these recommended system lifecycle criteria:
- Desktops: 3-5 years
- Laptops: 2-3 years
- Servers: 3-5 years
- Peripherals (e.g., printers): 4-5 years
- Software: 3-5 years

SI-14: NON-PERSISTENCE

Control Objective: The organization implements non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.

Standard: Asset custodians and data/process owners are required to ensure that software and data employed during system component and service refreshes are obtained from trusted sources.

Supplemental Guidance: Trusted sources include, for example, software/data from write-once, read-only media or from selected off-line secure storage facilities. This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (e.g., the window of opportunity and available attack surface) to initiate and complete cyber-attacks. Non-persistence increases the work factor of adversaries in attempting to compromise or breach organizational systems. Non-persistent system components can be implemented, for example, by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent).

Enhancements: None

SI-15: Information Output Filtering

Control Objective: Systems validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.

Standard: Asset custodians and data/process owners are required to configure critical systems to validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.

Supplemental Guidance: Certain types of cyber-attacks (e.g., SQL injections) produce output results that are unexpected or inconsistent with the output results that would normally be expected from software programs or applications. This control enhancement focuses on detecting extraneous content, preventing such extraneous content from being displayed, and alerting monitoring tools that anomalous behavior has been discovered.

Enhancements: None

SI-16: Memory Protection

Control Objective: Systems implement security safeguards to protect system memory from unauthorized code execution.

Standard: Asset custodians and data/process owners are required to configure critical systems to protect system memory from unauthorized code execution.

Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization.

Enhancements: None

SI-17: Fail-Safe Procedures

Control Objective: Systems implement fail-safe procedures when failure conditions occur.

Standard: Asset custodians and data/process owners are required to configure critical systems to implement fail-safe procedures when failure conditions occur.

Supplemental Guidance: Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take.

Enhancements: None

PRIVACY CONTROLS

Privacy controls provides a structured set of controls for protecting privacy. These controls are based on the Fair Information Practice Principles (FIPPs).[256]

AUTHORITY & PURPOSE (AP)

Data Authority & Purpose Policy: EAP Expert shall identify the authority to collect Personally Identifiable Information (PII) and specify the purposes and/or activities for which PII is collected.

Management Intent: The purpose of the Data Authority & Purpose (AP) policy is that EAP Expert identifies the authority to collect Personally Identifiable Information (PII) and specifies the purpose(s) for which PII is collected.

Supporting Documentation: Data Authority & Purpose (AP) control objectives & standards directly support this policy.

AP-01: AUTHORITY TO COLLECT

Control Objective: The organization determines the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or system need.

Standard: Before collecting PII, business units are required to determine whether the contemplated collection of PII is legally authorized.

Supplemental Guidance: Legal counsel should be engaged for determining the legal authority that permits the collection, use, maintenance, and sharing of PII, in support of business operations.

Enhancements: None

AP-02: PURPOSE SPECIFICATION

Control Objective: The organization describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.

Standard: Data/process owners are responsible for describing the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.

Supplemental Guidance: In order to avoid unauthorized collections or uses of PII, personnel who handle PII should receive training on the organizational authorities for collecting PII.

Enhancements: None

[256] Federal Trade Commission (FTC) Fair Information Practice Principles (http://www.ftc.gov/reports/privacy3/fairinfo.shtm)

ACCOUNTABILITY, AUDIT & RISK MANAGEMENT (AR)

Accountability, Audit & Risk Management Policy: EAP Expert shall implement effective controls to ensure that adequate privacy protection requirements are in place to minimize overall privacy risk.

Management Intent: The purpose of the Accountability, Audit & Risk Management (AR) policy is to enhance public confidence through effective governance, monitoring, risk management, and assessments to demonstrate that EAP Expert is complying with applicable privacy protection requirements and minimizing overall privacy risk.

Supporting Documentation: Accountability, Audit & Risk Management (AR) control objectives & standards directly support this policy.

AR-01: GOVERNANCE & PRIVACY PROGRAM

Control Objective: The organization:

- Appoints an individual who is accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and systems;
- Monitors privacy laws for changes that affect the privacy program;
- Allocates budget and staffing resources to implement and operate the organization-wide privacy program;
- Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
- Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, systems, or technologies involving PII; and
- Updates privacy plan, policies, and procedures at least biennially.

Standard: EAP Expert management is required to assign a business unit or individual the responsibility for privacy governance.

Supplemental Guidance: The development and implementation of a comprehensive governance and privacy program demonstrate organizational accountability for and commitment to the protection of individual privacy.

Enhancements: None

AR-02: PRIVACY IMPACT & RISK ASSESSMENT

Control Objective: The organization:

- Establishes a privacy risk assessment process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, and use of PII;
- Conducts a Privacy Impact Assessment (PIA) for systems and programs in accordance with applicable law, OMB policy, and any existing organizational policies and procedures; and
- Follows a documented, repeatable process for conducting, reviewing, and approving PIAs.

Standard: EAP Expert's responsible business unit for privacy governance is required to establish a privacy risk assessment program that includes a process for conducting Privacy Impact Assessments (PIA).

Supplemental Guidance: Organizational privacy risk assessment processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII.

Enhancements: None

AR-03: PRIVACY REQUIREMENTS FOR CONTRACTORS & SERVICE PROVIDERS

Control Objective: The organization includes privacy requirements in contracts and other acquisition-related documents that establish privacy roles and responsibilities for contractors and service providers.

Standard: The inclusion of privacy requirements in contracts is required to establish privacy roles and responsibilities for contractors and service providers.

Supplemental Guidance: Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing system development, information technology services, and other outsourced applications.

Enhancements: None

AR-04: Privacy Monitoring & Auditing

Control Objective: The organization monitors and audits privacy controls and internal privacy policy to ensure effective implementation.

Standard: EAP Expert's responsible business unit for privacy governance is required to monitor and audit privacy controls and internal privacy policy to ensure effective implementation.

Supplemental Guidance: To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and systems.

Enhancements: None

AR-05: Privacy Awareness & Training

Control Objective: The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

Standard: EAP Expert's responsible business unit for privacy governance is required to develop, implement, and update training and awareness aimed at ensuring users understand privacy responsibilities and procedures.

Supplemental Guidance: Through the implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy.

Enhancements: None

AR-06: Privacy Reporting

Control Objective: The organization develops, disseminates, and updates reports to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Standard: EAP Expert's responsible business unit for privacy governance is required to develop, implement, and update reports for senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Supplemental Guidance: Through external and internal privacy reporting, organizations promote accountability and transparency in organizational privacy operations.

Enhancements: None

AR-07: Privacy-Enhanced System Design & Development

Control Objective: The organization designs systems to enhance privacy by automating privacy controls.

Standard: EAP Expert's Cybersecurity personnel are responsible for designing systems to enhance privacy by automating security controls.

Supplemental Guidance: To the extent feasible when designing organizational systems, organizations employ technologies that automate privacy controls on the collection, use, and disclosure of PII. By building privacy controls into system design, organizations mitigate privacy risks to PII, thereby reducing the likelihood of system breaches and other privacy-related incidents.

Enhancements: None

AR-08: Accounting of Disclosures

Control Objective: The organization:

- Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
  - Date, nature, and purpose of each disclosure of a record; and
  - Name and address of the person or agency to which the disclosure was made;
- Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
- Makes the accounting of disclosures available to the person named in the record upon request.

Standard: EAP Expert's legal department is responsible for maintaining an accounting of disclosures.

Supplemental Guidance: None

Enhancements: None

DATA QUALITY & INTEGRITY (DI)

Data Quality & Integrity Policy: EAP Expert shall implement controls to ensure Personally Identifiable Information (PII) collected and maintained by is accurate, relevant, timely, and complete for the purpose for which it is to be used.

Management Intent: The purpose of the Data Quality & Integrity (DI) policy is to enhance public confidence that any PII collected and maintained by EAP Expert is accurate, relevant, timely, and complete for the purpose for which it is to be used.

Supporting Documentation: Data Quality & Integrity (DI) control objectives & standards directly support this policy.

DI-01: DATA QUALITY

Control Objective: The organization: [257]

- Confirms to the greatest extent practicable upon collection or creation of Personally Identifiable Information (PII), the accuracy, relevance, timeliness, and completeness of that information;
- Collects PII directly from the individual to the greatest extent practicable; and
- Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems.

Standard: Data/process owners are responsible for confirming the accuracy, relevance, timeliness, and completeness of that information.

Supplemental Guidance: Organizations take reasonable steps to confirm the accuracy of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces (APIs). The types of measures taken to protect data quality may be based on the nature and context of the PII, how it is to be used, and how it was obtained.

Enhancements: None

DI-02: DATA INTEGRITY

Control Objective: The organization documents processes to ensure the integrity of PII through existing security controls.

Standard: EAP Expert's Cybersecurity personnel are responsible for documenting existing security controls.

Supplemental Guidance: None

Enhancements: None

[257] UK Data Protection Act of 1998 (Chapter29-Schedule1-Part1-Principle 1)

DATA MINIMIZATION & RETENTION (DM)

Data Minimization & Retention Policy: EAP Expert shall implement data minimization and retention controls applicable to the collection, use, and retention of Personally Identifiable Information (PII) in order to ensure PII is relevant and necessary for the specified purpose for which it was originally collected.

Management Intent: The purpose of the Data Minimization & Retention (DM) policy is to implement data minimization and retention standards that EAP Expert uses to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

Supporting Documentation: Data Minimization & Retention (DM) control objectives & standards directly support this policy.

DM-01: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Control Objective: The organization: [258]

- Identifies the minimum PII elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the purpose of collection; and
- Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.

Standard: Where feasible and within the limits of technology, data/process owners are responsible for locating and removing/redacting unnecessary PII through the use of anonymization and de-identification techniques.

Supplemental Guidance: The collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect.

Enhancements: None

DM-02: DATA RETENTION & DISPOSAL

Control Objective: The organization: [259]

- Retains PII for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;
- Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage; and
- Uses organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Standard: Data/process owners are required to:

(a) Define retention periods for PII; and
(b) Dispose of, destroy, erase, and/or anonymizes the PII once the PII is no longer necessary for business purposes.

Supplemental Guidance: None

Enhancements:

- DM-02(a) – Data Collection
- DM-03(b) – Sensitive Data Storage
- DM-02(c) – Data Masking

DM-02(A): DATA RETENTION & DISPOSAL | DATA COLLECTION

Control Objective: The organization limits how it collects, uses and discloses personal information.

Standard: Data/process owners are required to implement limitations on the collection, use, and disclosure of personal information.

Supplemental Guidance: Data collection guidelines include, but are not limited to:

[258] UK Data Protection Act of 1998 (Chapter29-Schedule1-Part1-Principle 3)
[259] UK Data Protection Act of 1998 (Chapter29-Schedule1-Part1-Principle 5) | NY DFS 500.13

- Notice and Consent: EAP Expert shall collect and process information fairly and lawfully and where appropriate, with the knowledge or consent of the data subject. The type of notice or consent required will depend on the context and the circumstances, the sensitivity of the personal information, the data subject's reasonable expectations, and legal requirements.
- Specific Management Intent: EAP Expert shall collect and process personal information only for specified, limited and legitimate purposes.
- Limitations on Use: EAP Expert shall not process personal information in a manner inconsistent with the purposes for which it was originally collected without first obtaining the data subject's consent. The type of consent required will depend on the context and the circumstances, the sensitivity of the personal information, the data subject's reasonable expectations, and legal requirements.
- Data Proportionality: The personal information EAP Expert collects will be relevant, adequate and not excessive for the purposes for which it is collected or to which the data subject subsequently consents.
- Direct Marketing: EAP Expert shall not use personal information for direct marketing purposes without the data subject's consent. The data subject's consent may be express or implied, "opt-out" or "opt-in," depending on the circumstances and legal requirements.
- Data Retention: EAP Expert shall keep data storage to a minimum and will securely dispose of all PII when it is no longer a business need for EAP Expert to retain the data.
- Automated Decisions: EAP Expert shall not make decisions based solely on automated processing of personal information except as permitted by applicable law.
- Transfers to Third Parties: EAP Expert shall disclose personal information to third parties (including our affiliates) only for purposes consistent with those for which the personal information was originally collected or to which the data subject has subsequently consented. EAP Expert shall take appropriate measures, by contract or otherwise, to provide adequate protection for personal information that is disclosed to a third party.
    - Before EAP Expert transfers personal information to a third party to use for its own marketing purposes, EAP Expert shall obtain the data subject's consent. The data subject's consent may be express or implied, "opt-out" or "opt-in," depending on the circumstances and legal requirements.
    - There may be exceptions to these general rules, depending on applicable law, if, for example, the disclosure is required by court order, to comply with law, to prevent crime, to enforce a legal right.
- Transfers to Other Countries: EAP Expert shall take appropriate measures, by contract or otherwise, to provide adequate protection for personal information that is transferred from one country to another, including transfers among affiliates. If required by law, EAP Expert shall first obtain the data subject's consent to the transfer. In such cases, the type of consent required will depend on the context and the circumstances, the sensitivity of the personal information, the data subject's reasonable expectations, and legal requirements.

Management of Personal Information:

- Quality: EAP Expert shall take appropriate steps to ensure that personal information is accurate and reliable for its intended use and, where necessary for its intended use, kept up-to-date.
- Access: EAP Expert shall maintain procedures to give data subjects appropriate access to their personal information and, when appropriate, an effective means to have their personal information corrected or deleted.
- Security: EAP Expert shall implement reasonable administrative, physical and technological security measures to protect personal information from unauthorized access, unauthorized use, and unauthorized or accidental destruction, modification or disclosure. We will provide a level of security appropriate to the risks and the sensitivity of the personal information.
- Retention: EAP Expert shall not keep personal information in a form that permits identification of data subjects for longer than is necessary for the purposes for which it was collected or to which the data subject has consented, except for legitimate purposes permitted by law, such as regulatory compliance.

Accountability and Enforcement:

- Accountability: EAP Expert shall designate data subjects within EAP Expert to be accountable for compliance with privacy and data protection laws and our policies and procedures.
- Enforcement: EAP Expert shall provide internal controls for verifying compliance with privacy and data protection laws and our policies and procedures.
- Complaint Process: EAP Expert shall provide a fair process for investigating and resolving complaints and objections regarding our data practices and will take appropriate steps to communicate our process to the data subjects who entrust their personal information to us.

DM-02(b): Data Retention & Disposal | Sensitive Data Storage

Control Objective: The organization limits storing sensitive data to explicit business requirements.[260]

Standard: Personally Identifiable Information (PII) is prohibited from being stored for any longer than the legitimate business need exists to retain the data.

Supplemental Guidance: For credit or debit cardholder data, EAP Expert is required to not store:

- Sensitive authentication data after authorization, even if it is encrypted;
- The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data;
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions; or
- The personal identification number (PIN) or the encrypted PIN block.

In the normal course of business, the following data elements from the magnetic stripe may need to be retained (To minimize risk, store only these data elements as needed for business):

- The cardholder's name;
- Primary account number (PAN);
- Expiration date; or
- Service code

DM-02(c): Data Retention & Disposal | Data Masking

Control Objective: The organization applies data masking to sensitive information that is displayed or printed.[261]

Standard: Sensitive information that is displayed or printed is required to be masked. This includes, but is not limited to:

(a) Financial account numbers;
(b) Social Security Numbers (SSN); and
(c) Credit or debit Primary Account Numbers (PANs) (no more than the first six and last four digits allowed).

Supplemental Guidance: Only personnel with a legitimate business need should be able to see more than the first six/last four of the PAN.

DM-03: Minimization Of PII Used In Testing, Training & Research

Control Objective: The organization:

- Develops policies and procedures for the use of PII for testing, training, and research; and
- Implements controls to protect PII used for testing, training, and research.

Standard: The use of PII is prohibited for research, testing or training.

Supplemental Guidance: Organizations often use PII for testing new applications or systems prior to deployment. Organizations also use PII for research purposes, such as statistical analysis, and for training.

Enhancements: None

[260] PCI DSS 3.2 & 3.2.1-3.2.3
[261] PCI DSS 3.3

INDIVIDUAL PARTICIPATION & REDRESS (IP)

Individual Participation & Redress Policy: EAP Expert shall enable individuals to be active participants in the decision-making process regarding the collection and use of their Personally Identifiable Information (PII).

Management Intent: The purpose of the Individual Participation & Redress (IP) policy is to addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their Personally Identifiable Information (PII).

Supporting Documentation: Individual Participation & Redress (IP) control objectives & standards directly support this policy.

IP-01: CONSENT

Control Objective: The organization:

- Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;
- Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
- Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
- Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to support itemized or tiered consent for specific uses of data.

Supplemental Guidance: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase the risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.

Enhancements: None

IP-02: INDIVIDUAL ACCESS

Control Objective: The organization provides individuals the ability to have access to their Personally Identifiable Information (PII).[262]

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to support access requests to users' PII.

Supplemental Guidance: Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. Legal counsel should be consulted for record request processing.

Enhancements: None

IP-03: REDRESS

Control Objective: The organization provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate.

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to address end user redress issues.

[262] Argentina Personal Data Protection Law #25.326 & Regulatory Decree # 1558/2001 (PDPL)

Supplemental Guidance: Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations apply discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes.

Enhancements: None

IP-04: User Feedback Management

Control Objective: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to address an end user feedback process.

Supplemental Guidance: Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards.

Enhancements: None

SECURITY (SE)

Security Policy: EAP Expert shall implement controls to ensure safeguards are in place to protect Personally Identifiable Information (PII) against loss, unauthorized access, or disclosure.

Management Intent: The purpose of the Security (SE) policy is to supplements the management, operational and technical security controls to ensure safeguards are in place to protect Personally Identifiable Information (PII) collected or maintained by EAP Expert against loss, unauthorized access, or disclosure.

Supporting Documentation: Security (SE) control objectives & standards directly support this policy.

SE-01: INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Control Objective: The organization establishes, maintains, and updates an inventory that contains a listing of all programs and systems identified as collecting, using, maintaining, or sharing Personally Identifiable Information (PII).

Standard: Data/process owners are required to take due care in updating data inventories by identifying linkable data that could create PII.

Supplemental Guidance: The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII and to mitigate risks of PII exposure. As one method of gathering information for its PII inventory, organizations may extract the following information elements from Privacy Impact Assessments (PIAs) of systems containing PII:

- The name and acronym for each system identified;
- The types of PII contained in that system;
- Classification of level of sensitivity of all types of PII, as combined in that system; and
- Classification of the level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed.

Enhancements: None

SE-02: PRIVACY INCIDENT RESPONSE

Control Objective: The organization: [263]

- Develops and implements a Privacy Incident Response Plan; and
- Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Standard: Where technically feasible and a business reason exists, data/process owners are required to develop and implement a privacy-specific incident response redress process.

Supplemental Guidance: In contrast to the Incident Response (IR) family, which concerns a broader range of incidents affecting cybersecurity, this control uses the term Privacy Incident to describe only those incidents that relate to Personally Identifiable Information (PII). An organizational Privacy Incident Response Plan includes:

- The establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan;
- A process to determine whether notice to affected individuals is required and, where appropriate, to provide that notice;
- A privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; and
- Internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to cybersecurity officials.

Enhancements: None

[263] UK Data Protection Act of 1998 (Chapter29-Schedule1-Part1-Principles 7)

TRANSPARENCY (TR)

Transparency Policy: EAP Expert shall implement methods for disclosing data privacy practices and activities for consumer-related data.

Management Intent: The purpose of the Transparency (TR) policy is to implement EAP Expert's method for disclosing information practices and activities for consumer data.

Supporting Documentation: Transparency (TR) control objectives & standards directly support this policy.

TR-01: PRIVACY NOTICE

Control Objective: The organization provides effective notice to the public and to individuals regarding:

- Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
- Authority for collecting PII;
- The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and
- The ability, if any, to access and have PII amended or corrected if necessary.

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to provide notice to the public and to individuals regarding:

(a) Activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
(b) The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and
(c) The ability, if any, to access and have PII amended or corrected if necessary.

Supplemental Guidance: Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices.

Enhancements: None

TR-02: SAFE HARBOR

Control Objective: The organization limits how it collects, uses and discloses personal information in accordance with Safe Harbor privacy protection principles. [264]

Standard: EAP Expert requires business processes to adhere to the international safe harbor privacy principles.

Supplemental Guidance: The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998.[265] It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Community. The United States uses a sectorial approach that relies on a mix of legislation, regulation, and self-regulation. Personal data is data about an identified or identifiable individual that is recorded in any form.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the U.S. Department of Commerce issued principles under its statutory authority to foster, promote, and develop international commerce. The principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and the European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates.

[264] UK Data Protection Act of 1998 (Chapter29-Schedule1-Part1-Principles 8)
[265] Reference: http://ita.doc.gov/td/ecom/shprin.html

Organizations may qualify for the safe harbor in different ways. If an organization joins a private sector developed privacy program that adheres to these principles, it qualifies for the safe harbor.

Where an organization is subject to U.S. statutory, regulatory, administrative or another body of law (or body of rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or a Municipal Securities Rule-making Board) that also effectively protects personal data privacy, it qualifies for the safe harbor to the extent that its activities are governed by such laws or rules. Organizations may also put in place the safeguards deemed necessary by the EU for transfers of personal data from the EU to the US by incorporating the relevant safe harbor principles into agreements entered into with parties transferring personal data from the EU.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, but organizations that decide to adhere to these principles must comply with these principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so.

In addition to any exceptions provided for by the Directive and EU Member State law, adherence to these principles may be limited to the extent necessary to meet U.S. national security, public interest, and law enforcement requirements as well as other U.S. statutory and regulatory provisions. Adherence to these principles is not required for participation in the safe harbor where data is manually processed.

- **NOTICE**. An organization must inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or discloses it to a third party.

- **CHOICE**. An organization must offer individuals the opportunity to choose (opt-out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice.

- **ONWARD TRANSFER**. An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the safe harbor principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant safe harbor principles.

- **SECURITY**. Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration, and destruction.

- **DATA INTEGRITY**. Consistent with these principles, an organization may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is accurate, complete, and current.

- **ACCESS**. Individuals must have reasonable access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate. Reasonableness of access depends on the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the information.

- **ENFORCEMENT**. Effective privacy protection must include mechanisms for assuring compliance with the safe harbor principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include:

- Readily available and affordable independent recourse mechanisms by which an individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide;
- Follow-up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and
- Obligations to remedy problems arising out of failure to comply with these principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

Enhancements: None

TR-03: Dissemination of Privacy Program Information

Control Objective: The organization:

- Ensures that the public has access to information about its privacy activities and is able to communicate with its Chief Privacy Officer (CPO); and
- Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Standard: EAP Expert's legal department is responsible for disseminating privacy program information.

Supplemental Guidance: EAP Expert may employ different mechanisms for informing the public about privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). EAP Expert may also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

Enhancements: None

USE LIMITATION (UL)

Use Limitation Policy: EAP Expert shall implement controls to ensure that the scope of Personally Identifiable Information (PII) use is limited to justifiable business needs.

Management Intent: The purpose of the Use Limitation (UL) policy is to help EAP Expert implement controls that will ensure that the scope of Personally Identifiable Information (PII) use is limited accordingly.

Supporting Documentation: Use Limitation (UL) control objectives & standards directly support this policy.

UL-01: INTERNAL USE

Control Objective: The organization uses Personally Identifiable Information (PII) internally only for the authorized purpose(s) identified in public notices.

Standard: PII is authorized to be used only as the data was originally authorized to be used.

Supplemental Guidance: Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII.

Enhancements: None

UL-02: INFORMATION SHARING WITH THIRD PARTIES

Control Objective: The organization:

- Shares PII externally, only for authorized purposes or in a manner compatible with those purposes;
- Where appropriate, enters into contract or agreement, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;
- Monitors, audits, and trains its staff on the authorized uses and sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
- Evaluates any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.

Standard: Data/process owners are required to:

(a) Share PII externally, only for authorized purposes or in a manner compatible with those purposes;
(b) Where appropriate, enters into a contract with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;
(c) Monitor, audit, and train its staff on the authorized uses and sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
(d) Evaluate any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.

Supplemental Guidance: Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.

Enhancements: None

APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES

A-1: DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to EAP Expert. · Impact could include negatively affecting EAP Expert's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by EAP Expert
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to EAP Expert. · Impact could include negatively affecting EAP Expert's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by EAP Expert, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to EAP Expert. · Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to EAP Expert. · Impact would not be damaging or a risk to business operations.

A-2: Labeling

Labeling is the practice of marking a system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed**. Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material since marketing material is primarily developed for public release.
- **Displayed**. Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

A-3: General Assumptions

- Any information created or received by EAP Expert employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

A-4: Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number (e.g., passport, permanent resident card, etc.)
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
  - Passport number
  - Permanent resident card
- Driver License (DL)
- Financial account number
  - Payment card number (credit or debit)
  - Bank account number
- Electronic Protected Health Information (ePHI)

A-5: Personal Information (PI)

PI is any information about an individual maintained by EAP Expert including any information that:

- Can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PII is always PI, but PI is not always PII. Examples of PI include, but are not limited to:

- Name
  - Full name;
  - Maiden name;
  - Mother's maiden name; and
  - Alias(es);
- Personal Identification Numbers
  - Social Security Number (SSN);
  - Passport number;
  - Driver's license number;

- Taxpayer Identification Number (TIN), and
- Financial account or credit card number;

- Address Information
  - Home address; and
  - Personal email address;
- Personal Characteristics
  - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
  - Fingerprints;
  - Handwriting, and
  - Other biometric data:
    - Retina scan;
    - Voice signature; and
    - Facial geometry; and
- Linkable Information
  - Date of birth;
  - Place of birth
  - Race;
  - Religion;
  - Weight;
  - Social / recreational activities or hobbies;
  - Geographical indicators (e.g., geolocation information);
  - Employment information;
  - Medical information;
  - System-specific information (e.g., MAC or hardware address);
  - IP address;
  - Username;
  - Education information; and
  - Financial information.

A-6: Data Handling Guidelines

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-EAP Expert employees.	▪ NDA is recommended prior to access by non-EAP Expert employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*

Web Sites	▪ Posting to intranet sites is prohibited unless it is pre-approved to contain Restricted data. ▪ Posting to Internet sites is prohibited unless it is pre-approved to contain Restricted data.	▪ Posting to publicly-accessible Internet sites is prohibited.	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*
Telephone	▪ Confirm participants on the call line ▪ Ensure private location	▪ Confirm participants on the call line ▪ Ensure private location	*No special requirements*	*No special requirements*
Video / Web Conference Call	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line	*No special requirements*
Fax	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	*No special requirements*	*No special requirements*
Paper, Film/Video, Microfiche	▪ Return to owner for destruction ▪ Owner personally verifies destruction	▪ Shred or delete all documents or place in secure receptacle for future shredding	▪ Shred or delete all documents or place in secure receptacle for future shredding	*No special requirements*
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	▪ Physically destroy the hard drives and media ▪ Requires use of company-approved vendor for destruction	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient)	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media

APPENDIX B: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

Data Class	Sensitive Data Elements	Public	Internal Use	Confidential	Restricted
Client or Employee Personal Data	Social Security Number (SSN)				X
	Employer Identification Number (EIN)				X
	Driver's License (DL) Number				X
	Financial Account Number				X
	Payment Card Number (credit or debit)				X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X
	Controlled Unclassified Information (CUI)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	

	Investment-Related Activity			X	
	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)			X	
	Debt Amount Information			X	
	SEC Disclosure Information			X	

APPENDIX C: DATA RETENTION PERIODS

The following schedule highlights suggested retention periods* for some of the major categories of data:
** Retention periods are measured in years, after the event occurrence (e.g., termination, expiration, contract, filing, etc.)*

CATEGORY	TYPE OF RECORD	RETENTION PERIOD
Business Records	Amendments	Permanent
	Annual Reports	Permanent
	Articles of Incorporation	Permanent
	Board of Directors (elections, minutes, committees, etc.)	Permanent
	Bylaws	Permanent
	Capital stock & bond records	Permanent
	Charter	Permanent
	Contracts & agreements	Permanent
	Copyrights	Permanent
	Correspondence (General)	5
	Correspondence (Legal)	Permanent
	Partnership agreement	Permanent
	Patents	Permanent
	Service marks	Permanent
	Stock transfers	Permanent
	Trademarks	Permanent
CATEGORY	**TYPE OF RECORD**	**RETENTION PERIOD**
Financial Records	Audit report (external)	Permanent
	Audit report (internal)	3
	Balance sheets	Permanent
	Bank deposit slips, reconciliations & statements	7
	Bills of lading	3
	Budgets	3
	Cash disbursement & receipt record	7
	Checks (canceled)	3
	Credit memos	3
	Depreciation schedule	7
	Dividend register & canceled dividend checks	Permanent
	Employee expense reports	3
	Employee payroll records (W-2, W-4, annual earnings records, etc.)	7
	Financial statements (annual)	Permanent
	Freight bills	3
	General ledger	Permanent
	Internal reports (work orders, sales reports, production reports)	3
	Inventory lists	3
	Investments (sales & purchases)	Permanent
	Profit / Loss statements	Permanent
	Purchase and sales contracts	3
	Purchase order	3
	Subsidiary ledgers (accounts receivable, accounts payable, etc.)	Permanent
	Tax returns	Permanent
	Vendor Invoices	7
	Worthless securities	7

Category	Type of Record	Retention Period
Personnel Records	Accident report/injury claim	7
	Attendance Records	3
	Employee benefit plans	7
	Employment applications (not hired)	3
	Garnishments	3
	I-9 Forms	3
	Medical and exposure records - related to toxic substances	Permanent
	Organization Charts	Permanent
	OSHA Logs	5
	OSHA Training Documentation	5
	Patents	Permanent
	Pension plan agreement	Permanent
	Personnel files	4
	Profit sharing agreement	Permanent
	Time cards and daily time reports	3
Category	**Type of Record**	**Retention Period**
Insurance	Fire inspection reports	7
	Group disability records	7
	HIPAA-related documentation	6
	Insurance policies	7
	Safety records	3
	Settled insurance claims	7
Category	**Type of Record**	**Retention Period**
Real Estate	Deeds	Permanent
	Mortgages	3
	Plans & blueprints	Permanent
	Plant cost ledger	Permanent
	Property appraisals	Permanent
	Property register	Permanent
Category	**Type of Record**	**Retention Period**
Miscellaneous	Server audit trail history	1
	Workstation audit trail history	1
	Router audit trail history	Permanent
	Firewall audit trail history	Permanent
	Visitor logs	1

APPENDIX D: BASELINE SECURITY CATEGORIZATION GUIDELINES

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. *This basis is called an Assurance Level (AL)*.

D-1: DATA SENSITIVITY

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

D-2: SAFETY & CRITICALITY

The Safety & Criticality (SC) rating reflects two aspects of the "importance" of the asset or process:

- On one hand, SC simply represents the importance of the asset relative to the achievement of the company's goals and objectives (e.g., business critical, mission critical, or non-critical).
- On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to EAP Expert, its clients, its partners, or the general public.

The three (3) SC ratings are:

- SC-1: Mission Critical. This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of EAP Expert:
  - Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
  - Any business interruption would have a significant impact on EAP Expert's mission.
    - Cannot go down without having a significant impact on EAP Expert's mission.
    - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - *Requires the most stringent protection measures that exceed leading practices* to ensure adequate security.
  - Safety aspects of SC-1 systems, services and data could lead to:
    - Catastrophic hardware failure;
    - Unauthorized physical access to premises; and/or
    - Physical injury to users.
- SC-2: Business Critical. This category involves systems, services and data that are determined to be important to the support of EAP Expert's business operations:
  - Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on EAP Expert's mission.
    - Loss of availability is difficult to deal with and can only be tolerated for a short time.
    - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.
    - The consequences of loss of integrity are unacceptable.
  - *Requires protection measures equal to or beyond leading practices* to ensure adequate security.
  - Safety aspects of SC-2 systems could lead to:
    - Loss of privacy; and/or
    - Unwanted harassment.
- SC-3: Non-Critical. This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:
  - Includes systems, services or data with little or potential to impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on EAP Expert's mission.
    - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.
    - The consequences could include the delay or degradation of services or routine activities.
  - *Requires protection measures that are commensurate with leading practices* to ensure adequate security.
  - Safety aspects of SC-3 systems could lead to:
    - Inconvenience;
    - Frustration; and/or
    - Embarrassment.

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

Figure D-1: Asset Categorization Risk Matrix

D-3: Basic Assurance Requirements

- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

D-4: Enhanced Assurance Requirements

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to EAP Expert.

APPENDIX E: CYBERSECURITY ROLES & RESPONSIBILITIES

EAP Expert's cybersecurity roles and responsibilities are based on the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, as described in NIST Special Publication 800-181.

The NICE Framework is a model that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization.

As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity workforce development, planning, training, and education.

E-1: CYBERSECURITY ROLE CATEGORIES

Categories provide the overarching organizational structure of the NICE Framework. There are seven Categories and all are composed of Specialty Areas and work roles. This organizational structure is based on extensive job analyses, which group together work and workers that share common major functions, regardless of job titles or other occupational terms.

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

E-2: Cybersecurity Specialty Areas (Roles)

Categories contain groupings of cybersecurity work, which are called Specialty Areas. There were 31 specialty areas called out in the NICE Framework. Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work.

Categories	Specialty Areas	Specialty Area Descriptions
Securely Provision (SP)	Risk Management (RSK)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
	Software Development (DEV)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
	Systems Architecture (ARC)	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
	Technology R&D (TRD)	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
	Systems Requirements Planning (SRP)	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of systems to meet business needs.
	Test and Evaluation (TST)	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost- effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.
	Systems Development (SYS)	Works on the development phases of the systems development life cycle.
Operate and Maintain (OM)	Data Administration (DTA)	Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.
	Knowledge Management (KMG)	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support (STS)	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.
	Network Services (NET)	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and systems.
	Systems Administration (ADM)	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
	Systems Analysis (ANA)	Studies an organization's current computer systems and procedures, and designs systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

	Training, Education, and Awareness (TEA)	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.
	Cybersecurity Management (MGT)	Oversees the cybersecurity program of a system or network, including managing cybersecurity implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
	Strategic Planning and Policy (SPP)	Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.
	Executive Cyber Leadership (EXL)	Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.
	Program/Project Management (PMA) and Acquisition	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information
		exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.
Protect and Defend (PR)	Cybersecurity Defense Analysis (CDA)	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, systems, and networks from threats.
	Cybersecurity Defense Infrastructure Support (INF)	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
	Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and cybersecurity. Investigates and analyzes all relevant response activities.
	Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.
Analyze (AN)	Threat Analysis (TWA)	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
	Exploitation Analysis (EXP)	Analyzes collected information to identify vulnerabilities and potential for exploitation.
	All-Source Analysis (ASA)	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
	Targets (TGT)	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
	Language Analysis (LNG)	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.
Collect and Operate (CO)	Collection Operations (CLO)	Executes collection using appropriate strategies and within the priorities established through the collection management process.
	Cyber Operational Planning (OPL)	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

	Cyber Operations (OPS)	Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
Investigate (IN)	Cyber Investigation (INV)	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
	Digital Forensics (FOR)	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

E-3: Cybersecurity Work Roles & Responsibilities

Work roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of Knowledge, Skills, and Abilities (KSAs) and tasks performed in that role.

Work being performed in a job or position is described by selecting one or more work roles from the NICE Framework relevant to that job or position, in support of mission or business processes. To aid in the organization and communication about cybersecurity responsibilities, work roles are grouped into specific classes of categories and specialty areas.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Securely Provision (SP)	Risk Management (RSK)	Authorizing Official/Designating Representative	SP-RSK-001	Senior official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations.
		Security Control Assessor	SP-RSK-002	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development (DEV)	Software Developer	SP-DEV-001	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	SP-DEV-002	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	SP-ARC-002	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
	Technology R&D (TRD)	Research & Development Specialist	SP-TRD-001	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning (SRP)	Systems Requirements Planner	SP-SRP-001	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation (TST)	System Testing and Evaluation Specialist	SP-TST-001	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
		Systems Security Developer	SP-SYS-001	Designs, develops, tests, and evaluates system security throughout the systems development life cycle.

	Systems Development (SYS)	Systems Developer	SP-SYS-002	Designs, develops, tests, and evaluates systems throughout the systems development life cycle.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator	OM-DTA-001	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.
		Data Analyst	OM-DTA-002	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
	Knowledge Management (KMG)	Knowledge Manager	OM-KMG-001	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support (STS)	Technical Support Specialist	OM-STS-001	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (e.g., Master Incident Management Plan, when applicable).
	Network Services (NET)	Network Operations Specialist	OM-NET-001	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration (ADM)	System Administrator	OM-ADM-001	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
	Systems Analysis (ANA)	Systems Security Analyst	OM-ANA-001	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	OV-LGA-001	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Officer/Privacy Compliance Manager	OV-LGA-002	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
	Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer	OV-TEA-001	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
		Cyber Instructor	OV-TEA-002	Develops and conducts training or education of personnel within cyber domain.
	Cybersecurity Management (MGT)	Systems Security Manager	OV-MGT-001	Responsible for the cybersecurity of a program, organization, system, or enclave.
		Communications Security (COMSEC) Manager	OV-MGT-002	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).

	Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	OV-SPP-001	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
		Cyber Policy and Strategy Planner	OV-SPP-002	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
	Executive Cyber Leadership (EXL)	Executive Cyber Leadership	OV-EXL-001	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Program/Project Management (PMA) and Acquisition	Program Manager	OV-PMA-001	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
		IT Project Manager	OV-PMA-002	Directly manages information technology projects.
		Product Support Manager	OV-PMA-003	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
		IT Investment/Portfolio Manager	OV-PMA-004	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.
		IT Program Auditor	OV-PMA-005	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Cyber Defense Analyst	PR-CDA-001	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
	Cyber Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response (CIR)	Cyber Defense Incident Responder	PR-CIR-001	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	PR-VAM-001	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze (AN)	Threat Analysis (TWA)	Threat/Warning Analyst	AN-TWA-001	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
	Exploitation Analysis (EXP)	Exploitation Analyst	AN-EXP-001	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
	All-Source Analysis (ASA)	All-Source Analyst	AN-ASA-001	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

		Mission Assessment Specialist	AN-ASA-002	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
	Targets (TGT)	Target Developer	AN-TGT-001	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.
		Target Network Analyst	AN-TGT-002	Conducts advanced analysis of collection and open- source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
	Language Analysis (LNG)	Multi-Disciplined Language Analyst	AN-LNG-001	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collect and Operate (CO)	Collection Operations (CLO)	All Source-Collection Manager	CO-CLO-001	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.
		All Source-Collection Requirements Manager	CO-CLO-002	Evaluates collection operations and develops effects- based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
	Cyber Operational Planning (OPL)	Cyber Intel Planner	CO-OPL-001	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.
		Cyber Ops Planner	CO-OPL-002	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

		Partner Integration Planner	CO-OPL-003	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.
	Cyber Operations (OPS)	Cyber Operator	CO-OPS-001	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.
Investigate (IN)	Cyber Investigation (INV)	Cyber Crime Investigator	IN-INV-001	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
	Digital Forensics (FOR)	Law Enforcement/Counterintelligence Forensics Analyst	IN-FOR-001	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	IN-FOR-002	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

APPENDIX F: CYBERSECURITY EXCEPTION REQUEST PROCEDURES

The following procedure defines the process for the review and approval of exceptions to the Written Cybersecurity Program (WISP)'s policies, standards, guidelines, and procedures:

1) A manager (or an appointed designee) seeking an exception must assess the risks that non-compliance creates for the company. If the manager believes the risk is reasonable, then the manager prepares a written request describing the risk analysis and request for an exception (Note: The only reason to justify an exception is when compliance with a policy adversely affects business objectives or when the cost to comply offsets the risk of non-compliance). The risk analysis shall include:
   a) Identification of the threats and vulnerabilities, how likely each is to occur and the potential costs of an occurrence.
   b) The cost to comply.
2) Submit the request for an exception to the company's Cybersecurity Officer (ISO). The ISO will gather any necessary background information and make a recommendation to approve or deny the request. The ISO may recommend that other areas such as managers, asset custodians, and legal representatives review certain decisions.
3) The ISO will approve or deny the request for an exception.
4) The requestor will be notified of the decision to approve or deny.
5) All requests for exception will be retained by the ISO.
6) Exceptions are valid for a one-year period. Annually, the ISO will send a copy of approved exceptions back to the requestor, who must determine whether the conditions that justified the original exceptions are still in effect. If the conditions have substantially changed, a new request for exception must be submitted. Where little has changed, the review process may be shortened as recommended by the ISO.

Appendix G: Types of Security Controls

G-1: Preventative Controls

Preventive security controls are put in place to prevent intentional or unintentional disclosure, alteration, or destruction of sensitive information. Examples include, but are not limited to:

- Policy - Unauthorized network connections are prohibited.
- Firewall - Blocks unauthorized network connections.
- Locked wiring closet - Prevents unauthorized equipment from being physically plugged into a network switch.

G-2: Detective Controls

Detective security controls are like a burglar alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred. Examples include, but are not limited to:

- Log monitoring and review – monitoring for anomalous traffic can detect unauthorized activity.
- System audit – monitoring for unauthorized changes can detect a breakdown in the change control process.
- File integrity checkers – monitoring for file changes can detect integrity compromises.
- Motion detection systems – monitoring for physical activity can detect a break in of a facility.

G-3: Corrective Controls

Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. In many cases, the corrective security control is triggered by a detective security control. Examples include, but are not limited to:

- Procedures to clean a virus from an infected system.
- A guard checking and locking a door left unlocked by a careless employee.
- Updating firewall rules to block an attacking IP address as the attack is occurring.

G-4: Recovery Controls

Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category. Examples include, but are not limited to:

- After a disk failure, data is restored from a backup tape.
- A server automatically fails over to another server when a heartbeat (connectivity) is lost.

G-5: Directive Controls

Directive security controls are the equivalent of administrative controls. Directive controls direct that some action is taken to protect sensitive organizational information. Examples include, but are not limited to:

- Policy, standards, procedures, or guidelines.
- HR handbook

G-6: Deterrent Controls

Deterrent security controls are controls that discourage security violations. Examples include, but are not limited to:

- An "Unauthorized Access Prohibited" sign may deter a trespasser from entering an area.
- The presence of security cameras might deter an employee from stealing equipment.
- A policy that states access to servers is monitored could deter unauthorized access.

G-7: Compensating Controls

Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason. Examples include, but are not limited to:

- If a specific server cannot have antivirus software installed because it interferes with a critical application, a compensating control would be to increase monitoring of that server or isolate that server on its own network segment.
- If a system is not able to restrict who can log onto it, network segmentation would be a compensating control to protect the rest of the network from the lack of access control on the system.

APPENDIX H: RULES OF BEHAVIOR / USER ACCEPTABLE USE

These Rules of Behavior apply to the use of EAP Expert-provided IT resources, regardless of the geographic location:

- Data and system use must comply with EAP Expert policies and standards.
- Unauthorized access to data and/or systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII).

H-1: ACCEPTABLE USE

Users shall:

- In accordance with organizational procedures, immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected security policy violations or compromises, or suspicious activity. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information, including PII, maintained or in possession of the user.
- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on organization-owned systems.
- Log off or lock systems when leaving them unattended.
- Complete security awareness training before accessing any system and on an annual basis thereafter. Permit only authorized users to use organization-provided systems.
- Secure sensitive information (on paper and in electronic formats) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with organization records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information necessary to perform job functions (e.g., need to know).
- Use PII only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary.
- Wear organization-issued identification badges at all times in organization-operated facilities.

H-2: PROHIBITED USE

Users shall not:

- Direct or encourage others to violate organizational policies, procedures, standards or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of least privilege).
- Use another user's account, identity, or password.
- Exceed authorized access to sensitive information.
- Cause congestion, delay, or disruption of service to any organization-owned IT resource. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network, as does some uses of "push" technology, such as audio and video streaming from the Internet.
- Create, download, view, store, copy or transmit materials related to sexually explicit or sexually oriented materials.
- Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities or activities otherwise prohibited.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.
- Store sensitive information on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization or appropriate safeguards, as stipulated by organization policies.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
- Use organization-provided IT resources for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, the sale of goods or services, etc.).
- Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
- Establish unauthorized personal, commercial or non-profit organizational web pages on organization-provided systems.
- Use organization-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.
- Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.

- Use organization-owned IT resource for activities that are inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to hate speech, harassment, bullying, intimidation or other abusive conduct that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.
- Add personal IT resources to existing organization-owned systems without the appropriate management authorization, including the installation of modems on data lines and reconfiguration of systems.
- Intentionally acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.
- Send anonymous messages.
- Remove organization-proved IT resources from organization property without prior management authorization.
- Modify software without management approval.
- Post information on external blogs, social networking sites, newsgroups, bulletin boards or other public forums which:
    - Derogatory to EAP Expert or its management;
    - Contrary to EAP Expert's mission or stated positions; or
    - Brings discredit or embarrassment to EAP Expert.

H-3: Additional Rules For Security & Privileged Users

Security and system administration personnel with elevated privileges have significant access to processes and data in systems. As such, Security, Network, Systems, and Database Administrators have added responsibilities to ensure the secure operation of any EAP Expert system.

Personnel with elevated privileges are to:

- Advise the asset owner on matters concerning cybersecurity.
- Assist the asset owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to any system that affect contingency and disaster recovery plans are conveyed to the asset custodian responsible for maintaining continuity of operations plans for that system.
- Ensure that adequate physical and technical safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need to know basis.
- Verify that users have received appropriate security training before allowing access to any system.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the Cybersecurity Officer (ISO).

APPENDIX I: GUIDELINES FOR PERSONAL USE OF IT RESOURCES

EAP Expert allows authorized users to use company-owned IT resources for non-official purposes when such use involves no additional expense to the company, is performed on the employee's non-work time, does not interfere with the mission or operations of the company, and does not violate the ethical conduct or Rules of Behavior.

Managers may adopt more restrictive personal use policies or existing labor management agreements may preclude one or more of the personal use guidelines listed below:

- Any use of company-provided IT resources, including e-mail, is made with the understanding that such use may not be secure, is not private, is not anonymous and may be subject to monitoring. Users do not have a right to, nor shall they have an expectation of, privacy while using company-provided IT resources at any time, including accessing the Internet through company-provided connectivity. To the extent that users wish that their private activities remain private, they shall avoid making personal use of company-provided IT resources.
- Employees have no inherent right to utilize company-provided IT resources for personal use.
- Unauthorized or inappropriate use of company-provided IT resources could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, criminal penalties and/or employees or other users being held financially liable for the cost of inappropriate use.
- Users are permitted limited personal use of company-provided IT resources. This personal use shall not result in loss of employee productivity, interference with official duties or other than "minimal additional expense" to the company in areas such as:
    - Communications costs for voice, data, or video image transmission;
    - Use of consumables in limited amounts (e.g., paper, ink, and toner);
    - General wear and tear on equipment;
    - Data storage on local storage devices; and
    - Transmission impacts with moderate e-mail message sizes, such as e-mails with small attachments.
- Employees are expected to conduct themselves professionally in the workplace and to refrain from using company-provided IT resources for activities that are inappropriate.
- Departments may adopt policies that are more restrictive than these guidelines.
- Future labor management agreements shall comply with this policy.

APPENDIX J: RISK MANAGEMENT FRAMEWORK (RMF)

EAP Expert maintains a cybersecurity risk management program to evaluate threats and vulnerabilities in order to assure the creation of appropriate remediation plans.

J-1: RISK MANAGEMENT OVERVIEW

There is sometimes conflict between cybersecurity and other general system/software engineering principles. Cybersecurity can sometimes be construed as interfering with ``ease of use'' where installing security countermeasures take more effort than a ``trivial'' installation that works, but is insecure. Often, this apparent conflict can be resolved by re-thinking the problem and it is generally possible to make a secure system also easy to use. Based on the value owners place on their assets, it is a necessity to impose countermeasures to mitigate any risks posed by specific threats.

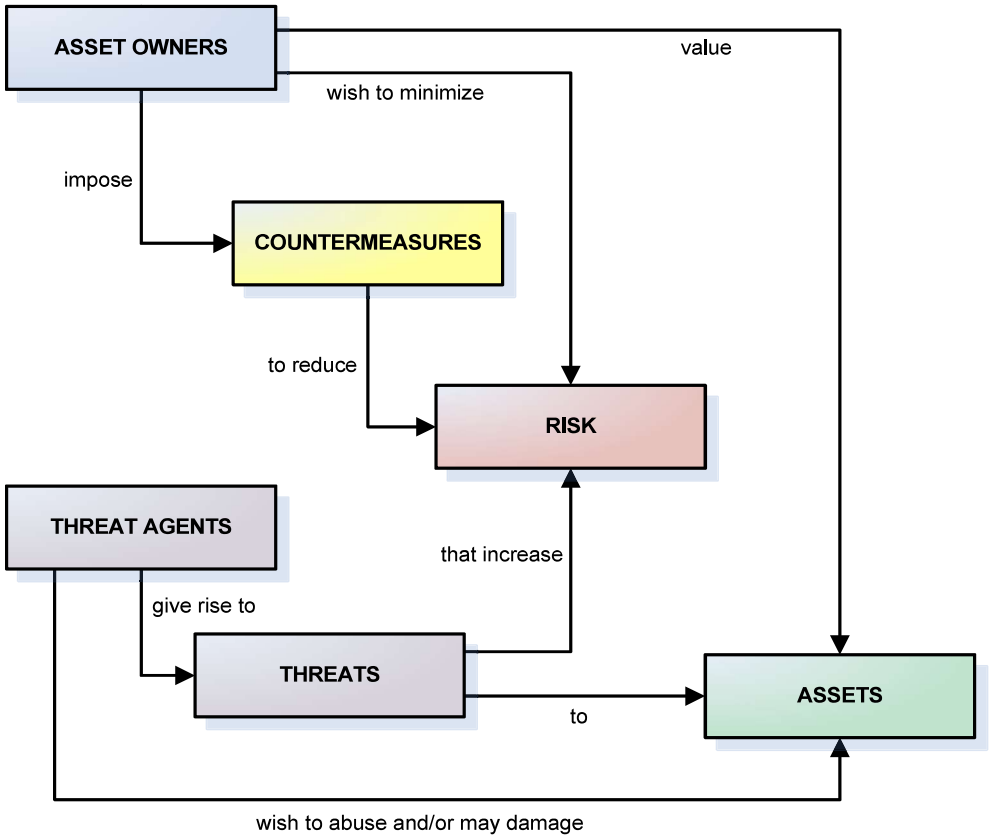

Figure J-1: Risk Overview

J-2: RISK MANAGEMENT FRAMEWORK (RMF)

Risk management requires finding security equilibrium between vulnerabilities and acceptable security controls. This equilibrium can be thought of as acceptable risk – it changes as vulnerabilities and controls change. From a systems perspective, the components used to determine acceptable risk cover the entire Defense-in-Depth (DiD) breadth. If one component is weakened, another component must be strengthened to maintain the same level of security assurance. Risk management activities can be applied to both new and legacy systems.

The Risk Management Framework (RMF) is based on NIST SP 800-37[266]:

- **Categorize**. The system and the information being processed, stored, and transmitted by the system, based on the potential impact to the organization should events occur to put the system and its information at risk. The organization assigns a security impact value (low, medium, high) for the security objectives of confidentiality, integrity, or availability of the information and systems that are needed by the organization to accomplish its mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.

- **Select**. An appropriate set of security controls is selected for the system after categorizing and determining the minimum-security requirements. Organizations meet the minimum-security requirements by selecting an appropriately tailored set of baseline security controls based on an assessment of risk and local conditions, including the organization's specific security requirements, threat information, cost-benefit analyses, or special circumstances.

- **Implement**. Security controls must be properly installed and configured in the system. Checklists of security settings are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is a series of instructions for configuring an IT product to an operational environment.

- **Assess**. Security Testing & Evaluation (ST&E) is used to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Authorize**. Based upon a determination of the risk to operations, organizational assets, or to individuals resulting from the operation of the system and the determination that this risk is acceptable.

- **Monitor**. Assessing selected security controls in the system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to appropriate organization officials on a regular basis.

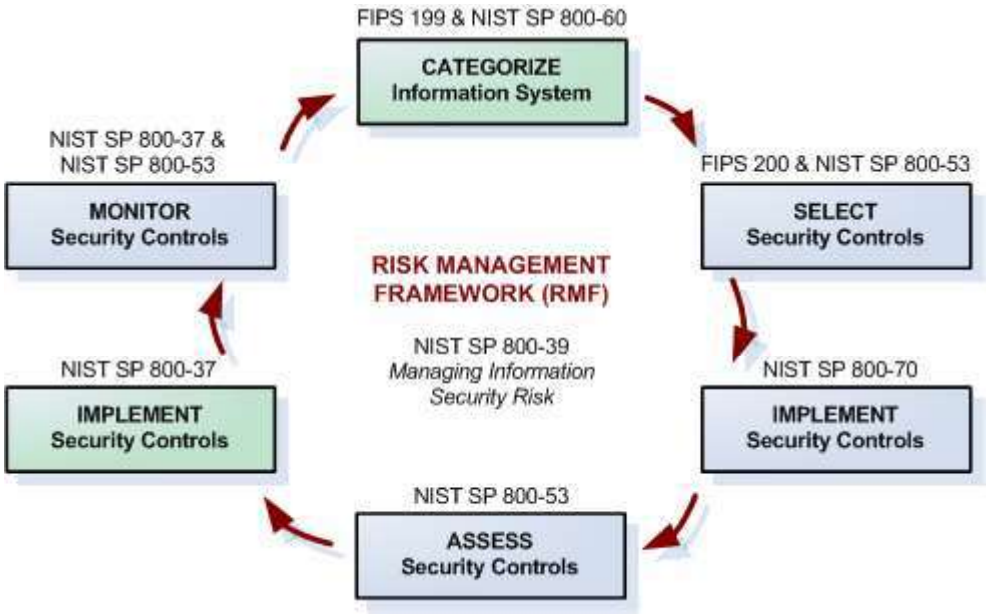

Figure J-2: Risk Management Framework (RMF)

[266] http://csrc.nist.gov/publications/PubsSPs.html

J-3: Assessing Risk

EAP Expert management must ensure that Risk Assessments (RAs) are conducted to identify the critical assets that require protection and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. RAs should take into account the potential adverse impact on EAP Expert's reputation, operations, and assets. RAs should be conducted by personnel associated with the activities subject to assessment.

RAs can be conducted on any system or project internal or external to EAP Expert, including applications, servers, networks, and any process or procedure by which these systems are administered and/or maintained. EAP Expert encourages authorized, periodic RAs for the purpose of determining areas of vulnerability and to initiate appropriate remediation.

The execution, development, and implementation of remediation programs are the responsibility of EAP Expert's management. Users are expected to cooperate fully with any RA being conducted on systems for which they are held accountable.

A method of assessing risk is to identify the likelihood of an event actually taking place and the consequences that would result from the incident occurring.

While assessing the likelihood and consequence of an event it is sometimes more subjective, rather than based on quantifiable data, the following figures should be used to assess risk:

Rating Risk	EXTREME - detailed response plan & employee training required
	HIGH – requires management attention and response plan
	MODERATE – significant impact to overall operations
	LOW – managed by routine procedures
Likelihood	CERTAINTY - expected in most circumstances (matter of time)
	LIKELY – will probably occur in most circumstances
	POSSIBLE – could occur at some time
	UNLIKELY – not expected to occur
	RARE – exceptional circumstances only
Consequences	SEVERE – would stop achievement of functional goals & objectives
	MAJOR – would threaten functional goals & objectives
	MODERATE – significant impact to overall operations
	MINOR – would threaten an element of operations
	NEGLIGIBLE – minor impact on productivity

Figure J-3: Standardizing Terminology

Occurrence Probability		Occurrence Consequence				
		Negligible	**Minor**	**Moderate**	**Major**	**Severe**
	Certainty	**L**	**M**	**H**	**E**	**E**
	Likely	**L**	**M**	**H**	**E**	**E**
	Possible	**L**	**M**	**M**	**H**	**E**
	Unlikely	**L**	**M**	**M**	**M**	**H**
	Rare	**L**	**L**	**M**	**M**	**H**

Figure J-4: Risk Matrix

APPENDIX K: SYSTEM HARDENING

K-1: SERVER-CLASS SYSTEMS

Server-class systems are defined as:

- Microsoft Server 2000
- Microsoft Server 2003
- Microsoft Server 2008
- Microsoft Server 2012
- Redhat Enterprise Linux (RHEL)
- Unix
- Solaris

Server-class systems should follow hardening procedures from the following sources:

- Center for Cybersecurity (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Cybersecurity Agency (DISA): http://iase.disa.mil/stigs/Pages/index.aspx
- Manufacturer security configuration recommendations

K-2: WORKSTATION-CLASS SYSTEMS

Workstation-class systems are defined as:

- Microsoft XP
- Microsoft Vista
- Microsoft 7
- Microsoft 8
- Apple
- Fedora (Linux)
- Ubuntu (Linux)
- SuSe (Linux)

Workstation-class systems should follow hardening procedures from the following sources:

- Center for Cybersecurity (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Cybersecurity Agency (DISA): http://iase.disa.mil/stigs/Pages/index.aspx
- Manufacturer security configuration recommendations

K-3: NETWORK DEVICES

Network devices are defined as:

- Firewalls
- Routers
- Load balancers
- Virtual Private Network (VPN) concentrators
- Wireless Access Points (WAPs)
- Wireless controllers
- Printers
- Multi-Function Devices (MFDs)

Network devices should follow hardening procedures from the following sources:

- Center for Cybersecurity (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Cybersecurity Agency (DISA): http://iase.disa.mil/stigs/Pages/index.aspx
- Manufacturer security configuration recommendations

K-4: MOBILE DEVICES

Mobile devices are defined as:

- Tablets
- Mobile phones
- Other portable electronic devices

Network devices should follow hardening procedures from the following sources:

- Center for Cybersecurity (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Cybersecurity Agency (DISA): http://iase.disa.mil/stigs/Pages/index.aspx
- Manufacturer security configuration recommendations

K-5: DATABASES

Databases are defined as:

- MySQL
- Windows SQL Server
- Windows SQL Express
- Oracle
- DB2

Network devices should follow hardening procedures from the following sources:

- Center for Cybersecurity (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Cybersecurity Agency (DISA): http://iase.disa.mil/stigs/Pages/index.aspx
- Manufacturer security configuration recommendations

APPENDIX L: CYBERSECURITY MANAGEMENT SYSTEM (ISMS)

An Cybersecurity Management System (ISMS) is a set of policies concerned with cybersecurity management or IT-related risks. The governing principle behind EAP Expert's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment. In accordance with ISO/IEC 27001, EAP Expert's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach:

- Plan: This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

L-1: CYBERSECURITY PROGRAM - PLAN

Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires that for all Federal systems must be associated with a system security level by evaluating the potential impact value (High, Moderate or Low), for each of the three security objectives of Confidentiality, Integrity and Availability (CIA). While EAP Expert is a non-governmental entity, EAP Expert determined that using Federal standards as a guide is a beneficial starting point to define appropriate Minimum Security Requirements (MSR) for the various data types processed by EAP Expert systems. This security categorization is the basis for selecting appropriate security controls for systems, as well as assessing the risks to EAP Expert operations and data.

Annually, EAP Expert should perform a review of the current baseline controls. The selection and specification of security controls for a system are accomplished as part of a company-wide initiative for the management of risk. The management of risk is a key element in EAP Expert's cybersecurity program and provides an effective framework for selecting the appropriate security controls for a system. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, policies, regulations, standards, or guidelines.

L-2: CYBERSECURITY PROGRAM - DO

Knowledgeable individuals within the company (e.g., system architects, systems/security engineers, system administrators, physical security experts, personnel specialists) shall determine which personnel, processes, hardware, software, firmware, facilities, or environmental components within the defined system boundary are providing specific security functionality. There should be close coordination and collaboration among company personnel to ensure that the needed security functions are allocated to the appropriate systems and supporting infrastructure. Certain security controls employed within the company's systems require that security configuration settings be established during implementation. For many technologies, the company defines mandatory configuration settings for information technology products that are used within the systems to comply with configuration settings-related legislation, directives, and policy requirements. Mandatory security configuration settings shall be enforced across the company, including all systems that are supporting company business processes.

L-3: CYBERSECURITY PROGRAM - CHECK

Security controls must be tested and evaluated prior to system deployment to ensure that the controls are effective. A Security Test and Evaluation (ST&E) plan should be developed and executed for each system, in order to test the security controls. The ST&E provides feedback as to the effectiveness of implemented security controls to business owners and asset custodians. Satisfactory completion of the ST&E is an essential milestone for the security authorization of new systems to assure compliance with EAP Expert policies, as well as providing the desired functionality.

L-4: CYBERSECURITY PROGRAM - ACT

Periodic or continuous testing and evaluation of security controls are necessary on an on-going basis to ensure that the controls continue to be both efficient and effective. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures is a critical activity conducted by EAP Expert or by an independent third party on behalf of the company. The on-going monitoring of security control effectiveness is accomplished in a variety of ways including security reviews, self-assessments, ST&Es, and audits.

ANNEX 1 - CYBERSECURITY POLICIES SUMMARY

Policy #	FIPS 199 Focus	Family	Identifier
1	Management	Security Assessment & Authorization	CA
2	Management	Planning	PL
3	Management	Program Management	PM
4	Management	Risk Assessment	RA
5	Management	System & Services Acquisition	SA
6	Operational	Contingency Planning	CP
7	Operational	Incident Response	IR
8	Operational	Media Protection	MP
9	Operational	Awareness & Training	AT
10	Operational	Personnel Security	PS
11	Operational	Physical & Environmental Protection	PE
12	Technical	Access Control	AC
13	Technical	Audit & Accountability	AU
14	Technical	Configuration Management	CM
15	Technical	Identification & Authentication	IA
16	Technical	Maintenance	MA
17	Technical	System & Communications Protection	SC
18	Technical	System & Information Integrity	SI
19	Privacy	Authority & Purpose	AP
20	Privacy	Accountability, Audit & Risk Management	AR
21	Privacy	Data Quality & Integrity	DI
22	Privacy	Data Minimization & Retention	DM
23	Privacy	Individual Participation & Redress	IP
24	Privacy	Security	SE
25	Privacy	Transparency	TR
26	Privacy	Use Limitation	UL

POLICY STATEMENT 1: SECURITY ASSESSMENT & AUTHORIZATION (CA)

Management Intent: The purpose of the Security Assessment & Authorization (CA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to the EAP Expert.

Security Assessment & Authorization Policy: EAP Expert shall periodically assess systems to determine if Cybersecurity controls are effective and ensure Cybersecurity controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Supporting Documentation: Security Assessment & Authorization (CA) control objectives & standards directly support this policy.

POLICY STATEMENT 2: PLANNING (PL)

Management Intent: The purpose of the Planning (PL) policy is to ensure due care planning considerations are addressed to minimize risks to EAP Expert.

Planning Policy: EAP Expert shall develop, document, implement, and periodically update measures to protect its critical systems.

Supporting Documentation: Planning (PL) control objectives & standards directly support this policy.

POLICY STATEMENT 3: PROGRAM MANAGEMENT (PM)

Management Intent: The purpose of the Program Management (PM) policy is for EAP Expert to specify the development, implementation, assessment, authorization, and monitoring of the Cybersecurity program management. The successful implementation of security controls for organizational systems depends on the successful implementation of the organization's program management controls. The Cybersecurity Program Management (PM) controls are essential for managing the Cybersecurity program.

Cybersecurity Program Management Policy: EAP Expert shall implement Cybersecurity program management controls to provide a foundation for EAP Expert's Cybersecurity Management System (ISMS).

Supporting Documentation: Program Management (PM) control objectives & standards directly support this policy.

POLICY STATEMENT 4: RISK ASSESSMENT (RA)

Management Intent: The purpose of the Risk Assessment (RA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to EAP Expert.

Risk Assessment Policy: EAP Expert shall periodically assess the risk to operations, assets, and data, resulting from the operation of systems and the associated processing, storage, or transmission of data.

Supporting Documentation: Risk Assessment (RA) control objectives & standards directly support this policy.

POLICY STATEMENT 5: SYSTEM & SERVICES ACQUISITION (SA)

Management Intent: The purpose of the System & Services Acquisition (SA) policy is to ensure that systems employ a System Development Life Cycle (SDLC), where the security of systems and services are assessed throughout the operational life of the systems to reduce risks to EAP Expert.

System & Services Acquisition Policy: EAP Expert shall allocate sufficient resources to adequately protect organizational systems by employing a System Development Life Cycle (SDLC) process that incorporate Cybersecurity considerations.

Supporting Documentation: System & Service Acquisition (SA) control objectives & standards directly support this policy.

POLICY STATEMENT 6: AWARENESS & TRAINING (AT)

Management Intent: The purpose of the Awareness & Training (AT) policy is to provide guidance for broad security awareness and security training for EAP Expert users.

Awareness & Training Policy: EAP Expert shall ensure that users are made aware of the security risks associated with their roles and that users understand the applicable laws, policies, standards, and procedures related to the security of systems and data.

Supporting Documentation: Awareness & Training (AT) control objectives & standards directly support this policy.

POLICY STATEMENT 7: CONTINGENCY PLANNING (CP)

Management Intent: The purpose of Contingency Planning (CP) policy is to establish procedures that will help EAP Expert management to quickly determine the appropriate actions to be taken due to an interruption of service or disaster.

Contingency Planning Policy: EAP Expert shall establish, implement and maintain plans for the continuity of operations (COOP) in emergency situations to ensure the availability of critical information resources.

Supporting Documentation: Contingency Planning (CP) control objectives & standards directly support this policy.

POLICY STATEMENT 8: INCIDENT RESPONSE (IR)

Management Intent: The purpose of Incident Response (IR) policy is to establish a protocol to guide EAP Expert's response to a cyber-security incident.

Incident Response Policy: EAP Expert shall establish an actionable Cybersecurity incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

Supporting Documentation: Incident Response (IR) control objectives & standards directly support this policy.

POLICY STATEMENT 9: MEDIA PROTECTION (MP)

Management Intent: The purpose of the Media Protection (MP) policy is to ensure that access to both paper and digital media is limited to authorized individuals.

Media Protection Policy: EAP Expert shall protect system media, both hardcopy and digital, by limiting access to authorized users and sanitizing or destroying media so that unauthorized data recovery is technically infeasible.

Supporting Documentation: Media Protection (MP) control objectives & standards directly support this policy.

POLICY STATEMENT 10: PERSONNEL SECURITY (PS)

Management Intent: The purpose of the Personnel Security (PS) policy is to ensure that EAP Expert performs due care and due diligence in its personnel management of procedures.

Personnel Security Policy: EAP Expert shall ensure that published rules of behavior are followed by users and employ a method of formal sanctions for personnel who fail to comply with Cybersecurity policies and standards.

Supporting Documentation: Personnel Security (PS) control objectives & standards directly support this policy.

POLICY STATEMENT 11: PHYSICAL & ENVIRONMENTAL PROTECTION (PE)

Management Intent: The purpose of the Physical & Environmental Protection (PE) policy is to minimize risk to EAP Expert systems and data by addressing applicable physical security and environmental concerns.

Physical & Environmental Protection Policy: EAP Expert shall implement physical access controls to limit access to systems, equipment, and the respective operating environments to authorized individuals. EAP Expert shall provide appropriate environmental controls in facilities containing systems.

Supporting Documentation: Physical & Environmental Protection (PE) control objectives & standards directly support this policy.

POLICY STATEMENT 12: ACCESS CONTROL (AC)

Management Intent: The purpose of the Access Control (AC) policy is to ensure that EAP Expert limits access to its systems and data to authorized users.

Access Control Policy: EAP Expert shall implement logical access controls to limit access to systems and processes to authorized users.

Supporting Documentation: Access Control (AC) control objectives & standards directly support this policy.

POLICY STATEMENT 13: AUDIT & ACCOUNTABILITY (AU)

Management Intent: The purpose of the Audit & Accountability (AU) policy is to ensure that EAP Expert creates and maintains appropriate scope and totality of audit records.

Audit & Accountability Policy: EAP Expert shall create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity by ensuring that the actions of individual users and systems can be uniquely traced.

Supporting Documentation: Audit & Accountability (AU) control objectives & standards directly support this policy.

POLICY STATEMENT 14: CONFIGURATION MANAGEMENT (CM)

Management Intent: The purpose of Configuration Management (CM) policy is to establish and maintain the integrity of systems.

Configuration Management Policy: EAP Expert shall maintain accurate inventories of its systems and enforce security configuration settings for information technology products employed in support of EAP Expert's business operations.

Supporting Documentation: Configuration Management (CM) control objectives & standards directly support this policy.

POLICY STATEMENT 15: IDENTIFICATION & AUTHENTICATION (IA)

Management Intent: The purpose of the Identification & Authentication (IA) policy is to ensure sufficient methods are enacted to properly identify and authenticate EAP Expert's authorized users and processes.

Identification & Authentication Policy: EAP Expert shall implement mechanisms are employed to properly identify system users, processes acting on behalf of users, or devices, and authenticate the identities of those users, processes, or devices.

Supporting Documentation: Identification & Authentication (IA) control objectives & standards directly support this policy.

POLICY STATEMENT 16: MAINTENANCE (MA)

Management Intent: The purpose of the Maintenance (MA) policy is to ensure that due diligence is performed by properly maintaining EAP Expert systems.

Maintenance Policy: EAP Expert shall perform periodic and timely maintenance on systems, so that EAP Expert assets are protected from the latest threats.

Supporting Documentation: Maintenance (MA) control objectives & standards directly support this policy.

POLICY STATEMENT 17: SYSTEM & COMMUNICATION PROTECTION (SC)

Management Intent: The purpose of the System & Communication Protection (SC) policy is to ensure sufficient protections are in place to protect the confidentiality and integrity of EAP Expert's communications.

System & Communication Protection Policy: EAP Expert shall employ industry-recognized leading practice principles that promote effective Cybersecurity within systems and the network.

Supporting Documentation: System & Communication Protection (SC) control objectives & standards directly support this policy.

POLICY STATEMENT 18: SYSTEM & INFORMATION INTEGRITY (SI)

Management Intent: The purpose of the System & Information Integrity (SI) policy is to ensure the confidentiality, integrity, and availability of EAP Expert's data.

System & Information Integrity Policy: EAP Expert is required to correct flaws in its systems in a timely manner and ensure mechanisms are in place to protect systems from malicious code.

Supporting Documentation: System & Information Integrity (SI) control objectives & standards directly support this policy.

POLICY STATEMENT 19: AUTHORITY & PURPOSE (AP)

Management Intent: The purpose of the Data Authority & Purpose (AP) policy is that EAP Expert identifies the authority to collect Personally Identifiable Information (PII) and specifies the purpose(s) for which PII is collected.

Authority & Purpose Policy: EAP Expert shall identify the authority to collect Personally Identifiable Information (PII) and specify the purposes and/or activities for which PII is collected.

Supporting Documentation: Authority & Purpose (AP) control objectives & standards directly support this policy.

POLICY STATEMENT 20: ACCOUNTABILITY, AUDIT & RISK MANAGEMENT (AR)

Management Intent: The purpose of the Accountability, Audit & Risk Management (AR) policy is to enhance public confidence through effective governance, monitoring, risk management, and assessments to demonstrate that EAP Expert is complying with applicable privacy protection requirements and minimizing overall privacy risk.

Accountability, Audit & Risk Management Policy: EAP Expert shall implement effective controls to ensure that adequate privacy protection requirements are in place to minimize overall privacy risk.

Supporting Documentation: Accountability, Audit & Risk Management (AR) control objectives & standards directly support this policy.

POLICY STATEMENT 21: DATA QUALITY & INTEGRITY (DI)

Management Intent: The purpose of the Data Quality & Integrity (DI) policy is to enhance public confidence that any PII collected and maintained by EAP Expert is accurate, relevant, timely, and complete for the purpose for which it is to be used.

Data Quality & Integrity Policy: EAP Expert shall implement controls to ensure Personally Identifiable Information (PII) collected and maintained by is accurate, relevant, timely, and complete for the purpose for which it is to be used.

Supporting Documentation: Data Quality & Integrity (DI) control objectives & standards directly support this policy.

POLICY STATEMENT 22: DATA MINIMIZATION & RETENTION DM)

Management Intent: The purpose of the Data Minimization & Retention (DM) policy is to implement data minimization and retention standards that EAP Expert uses to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

Data Minimization & Retention Policy: EAP Expert shall implement data minimization and retention controls applicable to the collection, use, and retention of Personally Identifiable Information (PII) in order to ensure PII is relevant and necessary for the specified purpose for which it was originally collected.

Supporting Documentation: Data Minimization & Retention (DM) control objectives & standards directly support this policy.

POLICY STATEMENT 23: INDIVIDUAL PARTICIPATION & REDRESS (IP)

Management Intent: The purpose of the Individual Participation & Redress (IP) policy is to addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their Personally Identifiable Information (PII).

Individual Participation & Redress Policy: EAP Expert shall enable individuals to be active participants in the decision-making process regarding the collection and use of their Personally Identifiable Information (PII).

Supporting Documentation: Individual Participation & Redress (IP) control objectives & standards directly support this policy.

POLICY STATEMENT 24: SECURITY (SE)

Management Intent: The purpose of the Security (SE) policy is to supplements the management, operational and technical security controls to ensure safeguards are in place to protect Personally Identifiable Information (PII) collected or maintained by EAP Expert against loss, unauthorized access, or disclosure.

Security Policy: EAP Expert shall implement controls to ensure safeguards are in place to protect Personally Identifiable Information (PII) against loss, unauthorized access, or disclosure.

Supporting Documentation: Security (SE) control objectives & standards directly support this policy.

POLICY STATEMENT 25: TRANSPARENCY (TR)

Management Intent: The purpose of the Transparency (TR) policy is to implement EAP Expert's method for disclosing information practices and activities for consumer data.

Transparency Policy: EAP Expert shall implement methods for disclosing data privacy practices and activities for consumer-related data.

Supporting Documentation: Transparency (TR) control objectives & standards directly support this policy.

POLICY STATEMENT 26: USE LIMITATION (UL)

Management Intent: The purpose of the Use Limitation (UL) policy is to help EAP Expert implement controls that will ensure that the scope of Personally Identifiable Information (PII) use is limited accordingly.

Use Limitation Policy: EAP Expert shall implement controls to ensure that the scope of Personally Identifiable Information (PII) use is limited to justifiable business needs.

Supporting Documentation: Use Limitation (UL) control objectives & standards directly support this policy.

ACRONYMS

AD. Active Directory
APT. Advanced Persistent Threat
BCP. Business Continuity Plan
CDE. Cardholder Data Environment
CERT. Computer Emergency Response Team
CIRT. Computer Incident Response Team
COOP. Continuity of Operations Plan
CTI. Controlled Technical Information [267]
CUI. Controlled Unclassified Information [268]
DAC. Discretionary Access Control
DISA. Defense Cybersecurity Agency
DLP. Data Loss Prevention
DRP. Disaster Recovery Plan
EAP. Extensible Authentication Protocol
EPHI. Electronic Protected Health Information
FICAM. Federal Identity, Credential, and Access Management
FIM. File Integrity Monitor
GDPR. General Data Protection Regulation
HIPAA. Health Insurance Portability and Accountability Act
IRP. Incident Response Plan
ISMS. Cybersecurity Management System
ISO. International Organization for Standardization
LDAP. Lightweight Directory Authentication Protocol
MAC. Media Access Control
NIST. National Institute of Standards and Technology
PCI DSS. Payment Card Industry Data Security Standard
PDCA. Plan-Do-Check-Act
PIV. Personal Identity Verification
RBAC. Role-Based Access Control
TLS. Transport Layer Security

DEFINITIONS

EAP Expert recognizes two sources for authoritative definitions:

- Unified Compliance Framework (UCF) Compliance Library[269]
- The National Institute of Standards and Technology (NIST) IR 7298, Revision 2, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define common digital security terms. [270]

Security Requirements and Controls

The term control can be applied to a variety of contexts and can serve multiple purposes. When used in the security context, a security control can be a mechanism (i.e., a safeguard or countermeasure) designed to address protection needs that are specified by a set of security requirements.

- Controls are defined as the power to make decisions about how something is managed or how something is done; the ability to direct the actions of someone or something; an action, method, or law that limits; or a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system.
- Requirements are defined as statements that translate or express a need and its associated constraints and conditions.[271]

[267] CUI Registry - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html
[268] CUI Registry - https://www.archives.gov/cui/registry/category-list
[269] UCF Compliance Library - https://compliancedictionary.com
[270] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
[271] ISO/IEC/IEEE 29148

KEY WORD INDEX

RECORD OF CHANGES

Issue	Date	Pages Affected	Description
Original	2018-02-15	All	Original version for first publishing.

EAP Expert Software 3.0 Hosted Proposal

EAPexpert

Prepared For:	Poudre School District
Prepared By:	Chris Coleman
Valid Until:	Dec 31st 2022

Quantity	Software: Hosted Solution	7 Licenses		
7	• Full Version		$179.00	**$1,253.00**
			Monthly Shared Hosting:	**$1,253.00**
	Software Training/Implementation Options			
	• 1-Hour Telephonic Training Bundle		$185.00	
	• 3-Hour Telephonic Training Bundle		$470.00	
2	• 5-Hour Telephonic Training Bundle		$695.00	**$1,390.00**
	• In-Person Training (Daily Rate) [2]		$1,150.00	
	Other Monthly Services			
	PROVIDERfiles			
	• My Details - Up to 1000 Providers		$499.00	
	• My Details - Each additional 500 provider		$50.00	
	• My Details - Per Auth		$0.99	
	Online Intake			
	• Set-up Fee		$1,200.00	
	• Unlimited Intakes		$99.00	
	• Self Scheduling			
	Twillio Integration - One-Time Fee		$1,200.00	
	• Text Reminders - Monthly		$150.00	
	Sync to Outlook			
	• Set-Up Fee		$1,200.00	
	• Calendar Sync - Appt Reminders (Text and Email)		$150.00	
	Automated Surveys, forms & WOS (Workplace Outcome Suite)		$300.00	
	• Unlimited Surveys/WOS			
	Eligibility File Import		$50.00	**$50.00**
	• Send and store Utilization Reports			
	Other			
	• **Data Conversion Estimate (Hourly Rate)**		$180.00	**$4,500.00**
	Please refer to the Data Conversion Estimate Document Attached (Where Applicable)			
	• **Professional Services (Hourly Rate)**		$180.00	
	Ex: Program Customization, Consultations, GAP Fit Analysis, RFP Assistance/Security Questionnaires			
			Total One Time Investment:	**$5,890.00**
			Total Monthly Investment:	**$1,303.00**
			Total Due Upon Signing (Including first/last months payments):	**$8,496.00**

Notes/Comments:

1 Either party can terminate this Agreement at anytime on sixty (60) days written notice

2 Does not include expenses (flight, accommodation, meals etc.). See Conditions Form.

3 Customer Web Portal - Minimum 20 client organizations. One login per organization.

All Funds quoted in US dollars unless specified otherwise. Prices Subject to Change Without Notice.

Phone: 905-702-1380 x 200 Fax: 905-702-1711 E-mail: ccoleman@eapexpert.com

Proposals must be submitted and received in BidNet's electronic solicitation portal on or before 2:00 p.m. MT on March 23, 2023.

The undersigned hereby affirms that:

- He/she is a duly authorized agent of the company issuing this proposal and that all information provided in the proposal is true and accurate.
- Supplier has read the conditions, including the insurance requirements and technical specifications, which were made available to the company in conjunction with this RFP, and fully understands and accepts these terms unless specific variations have been expressly requested in the response submitted by the Supplier. Requested variations will be reviewed by the District and approved on a case-by-case basis if deemed appropriate.
- The company will adhere to all terms and conditions and provide, at a minimum, all services as expressed in the solicitation and/or the company's proposal responding to the solicitation.
- The company meets or exceeds all of the required criteria as specified by this solicitation, or if not, has submitted a Justification for Consideration addressing any failure to meet the criteria.
- The company's proposal is being offered independently of any other Supplier and in full compliance with the terms specified in Sections 1 and 2 of the solicitation.
- The company will accept any awards made to it, contingent on contract negotiation, as a result of this solicitation for a minimum of ninety (90) calendar days following the date and time of the solicitation opening.

Company Name: EAP Expert Software

Signature of Agent: Chris Coleman

Printed Name: Chris Coleman

Title: SVP, Global Solutions

E-mail address: ccoleman@eapexpert.com

Mailing address: 7111 Syntex Dr, Suite 100 Mississauga, ON L5N 8C3

Telephone: 905-703-1380 Ext 200

Contact Person: _____
(If different from Agent, include e-mail address and phone number)

NOTE: Proposals submitted without the signature of an authorized agent of the company may be considered non-responsive and ineligible for the award.