SOW No. ME17-076-003

STATEMENT OF WORK No. 3

This Statement of Work ("SOW) is entered into in accordance with, and is hereby integrated into, Master Services Agreement No. ME17-076 dated July 19, 2018 (the "MSA"), for the performance of professional services, and is entered into as of the 18th day of July, 2019 (the "Effective Date") by and between the Pennsylvania Higher Education Assistance Agency, a public corporation and governmental instrumentality organized under the law of the Commonwealth of Pennsylvania, having an address of 1200 North Seventh Street, Harrisburg, Pennsylvania 17102 ("PHEAA" or "Client") and DATAMARK, Inc. ("Contractor"), a Texas Corporation with its principal offices located at 123 W. Mills Ave, Ste. 400, El Paso, Texas 79901, referred to individually hereinafter from time to time as the "Party," and collectively as the "Parties."

I. DEFINITIONS AND ATTACHMENTS

(a) Capitalized terms not otherwise herein defined shall have the meanings ascribed to them in the MSA (including its Exhibits 1-5) or in SOWs.

(b) The following documents are attached to, and are hereby integrated into, this SOW. In the case of a conflict between the documents, the following order of precedence shall apply:

1. Attachment 1 – Security Requirements
2. Attachment 2 – Site Floor Plan
3. Attachment 3 – Architecture Diagram
4. Attachment 4 – Process Flow Diagram
5. Attachment 5 – Reporting Requirements
6. Attachment 6 - Indexing Requirements
7. Attachment 7 – Electronic Documents Requirements
8. Attachment 8 – Service Level Agreements
9. Attachment 9 – Fees and Payments

(c) NEW FORM DETAILED REQUIREMENTS. CLIENT will be responsible for providing detailed business requirements to CONTRACTOR as forms are added to the CONTRACTOR's workload or as requirements change for existing forms. These additional requirements shall be added to the SOW in accordance with Provision 12, Changes, of the MSA. Turnaround time for each change request including estimate of cost will be determined as part of change impact analysis.

II. NOTICE AND APPROVAL OF SUBCONTRACTORS

Not Applicable to this SOW.

III. HIGH-LEVEL REQUIREMENTS (DELIVERABLES AND SERVICES)

This SOW supersedes and takes precedence over conflicting requirements in SOW 1 and SOW 2. SOW 1 and SOW 2 shall remain effective for the duration of the term of SOW 3. Expectations under this SOW 3 are as follows:

a. CONTRACTOR will define and implement an upgrade strategy path that will result in improved operations for PHEAA, and cost-savings to PHEAA over PHEAA's historical costs for the same or substantially similar services. The

MZ

upgrade, herein referred as Phase 2, will address the design, development & implementation of the DATAMARK integrated solution and transactional billing implementation.

b. CONTRACTOR shall provide a Master Project Plan, which will include SOW 3 activities designed to comport with this SOW 3, within two weeks of SOW 3 execution.
c. The Master Project Plan shall not contain legal terms and conditions; to the extent that legal terms and conditions are contained therein, the legal terms and conditions will not be enforceable because they have not been integrated into the MSA in accordance with the requirements of the MSA.
d. Upon acceptance of the Master Project Plan in writing by PHEAA Project Manager, the Master Project Plan shall, and upon acceptance hereby does, become a part of this SOW 3.
e. The Master Project Plan may be changed and updated by mutual agreement in writing, signed by the Parties' Project Managers, except as otherwise explicitly indicated herein.

IV. IMPLEMENTATION APPROACH

The implementation approach for SOW 3 will address the following goals:

- ***Design, develop & implement transactional billing (Phase 2 – Transactional Billing Implementation)***
  - Implementation of the Transactional pricing model as identified in Attachment 9 – Pricing and Fees shall start after the completion of the rollout of the CONTRACTOR system, using criterion listed within Attachment 6 – Indexing Requirements and other supplemental documents provided by CLIENT to the CONTRACTOR.
  - CONTRACTOR commits to completion of the system development within six (6) months of execution of this SOW. If CONTRACTOR misses this commitment date, a liquidated damage will be assessed in the amount of $80,000 for any partial or full month(s) beyond the commitment date through completion of the system development and the full rollout of the CONTRACTOR system, including migration of all documents off CLIENT system onto CONTRACTOR system.
  - CLIENT and CONTRACTOR agree to work diligently, individually and in cooperation as appropriate, to ensure the transition from the CLIENT system to the CONTRACTOR system and conversion to Transactional pricing by the deadlines as herein indicated. Project Managers will immediately communicate to both CLIENT and CONTRACTOR teams any potential delays so they can be addressed by both PARTIES.
  - Any changes to mailroom operations, including Attachment 6 – Indexing Requirements, or other supplemental documents provided by CLIENT to CONTRACTOR after SOW execution, will go through Change Control and PARTIES will determine if the change can be developed and deployed after the rollout, and if costs and/or a delay in the rollout date are necessary.
  - Any delay by CLIENT to provide resources or deliverables that are considered dependencies per Section VI (d) herein may delay the accomplishment of work

MJ

by CONTRACTOR under this SOW, and may require submission through the change control process. Any agreement to change a due date hereunder shall be made in writing signed by both Parties' Project Managers.

- ***Design, develop & implement DATAMARK integrated solution (Phase 2 – To-Be System Implementation)***
    - Implementation will proceed by multiple rollouts from SOW 3 Effective Date through the date upon which the DATAMARK integrated solution is being used for 100% of the service volumes. Rollout 1 through system Go-Live (defined as the time at which DATAMARK system is in production, and DATAMARK and PHEAA systems are both operational and in use) shall not exceed seven and one-half months after the SOW 3 Effective Date. Go-Live to the date upon which the DATAMARK integrated solution is being used for 100% of the service volumes shall not exceed 1 ½ months.
    - The Master Project Plan will include substantially the same activities CONTRACTOR has utilized to implement their document intake and processing solution with other customers.
    - Detailed requirements gathering will commence first around topics such as, but not limited to, the scope of indexing requirements for all line of business forms, records management and vendor management reporting.
    - Associated design, development and testing activities will be planned and executed with the intent of aligning the CONTRACTOR's IT systems with the targeted CLIENT IT systems (to the extent that CLIENT systems are needed to communicate with the fully implemented DATAMARK integrated solution) as a holistic integrated solution.
    - Critical activities around integration testing will be listed in the project schedule (which shall be a part of the Master Project Plan) as CLIENT components are being delivered.
    - As part of detailed requirements gathering CLIENT and CONTRACTOR will work collaboratively to build a recommended approach by source based on volume of source, then by Line of Business (LOB) volume.
    - CONTRACTOR shall use detailed requirements to create a document transition plan beginning at Go-Live which shall be, and upon its written approval by PHEAA Project Manager hereby is, an addendum to the Master Project plan.
    - Results of each initial rollout will be utilized to verify/revise and execute follow-on rollouts. Activities required will be captured in the Master Project Plan two weeks after SOW 3 execution.
    - Maintenance of the legacy system and new system will be required for multiple channels and LOBs after Go-Live until full implementation of the DATAMARK integrated solution is approved by PHEAA.

V. DETAILED REQUIREMENTS (DELIVERABLES AND SERVICES)

1. **The following Facility Modification Services shall be provided by the Contractor to the Client:**

(a) Facility Modifications:

ML

a. Contractor shall build out Facility to meet Client's Enterprise Security Office requirements as specified within SOW 3 Attachment 1 – Security Requirements.
b. Contractor shall build out Facility to support the Records Management Process as specified within SOW 3 Attachment 4 – Process Flow Diagram to be performed by Contractor's personnel.
c. Contractor shall build out Facility as specified within SOW 3 Attachment 2 – Site Floor Plan to support Contractor's personnel. Any changes to the Floor Plan require written approval by both Client and Contractor.
d. Contractor will prepare the information technology infrastructure as specified within SOW 3 Attachment 3 – Architecture Diagram. Client supporting activities are listed within the Master Project Plan. Infrastructure includes but is not limited to the following items:
    i. Network Connectivity
    ii. Telecom
    iii. Desktops
    iv. Scanning Workstations
    v. Commercial Workspace
    vi. Federal Workspace
e. Contractor shall update the equipment list (which will, and upon its approval by PHEAA Project Manager in writing hereby does, become an addendum to the Master Project Plan) as part of project execution specifying equipment that will be procured by Contractor, and ownership dispositions. No equipment changes shall incur additional cost to PHEAA.
f. Contractor and Client shall develop a mutual test plan (which will, and upon its approval by PHEAA Project Manager in writing hereby does, become an addendum to the Master Project Plan) as part of project execution to guarantee operations as specified within Records Management Operations section.
g. Client will perform an audit and will provide Enterprise Security Approval in writing before transitioning to the new DATAMARK integrated solution.
h. The parties agree and acknowledge that any references to SOW 2 in SOW 1 shall now be considered SOW 3 unless the context clearly indicates otherwise.

2. **The following Mailroom Services shall be provided by the Contractor to the Client:**
Mailroom Services shall be provided in accordance with this SOW 3 including all Attachments, other applicable SOWs, and the MSA. CONTRACTOR will create a new Mailroom Standard Operating Procedure (SOP) as a deliverable, subject to PHEAA's acceptance, and to be owned by PHEAA as a work related to the business of PHEAA in accordance with MSA Provision #30. The new Mailroom SOP, shall replace CLIENT's current Mailroom SOP.

(a) **Mail Receipt and Logging**

CONTRACTOR will pick up mail from the USPS facilities at least twice per day Monday through Friday (3:00 am and 5:00 am Eastern Time) or as otherwise stated in each Schedule. CONTRACTOR acknowledges and agrees that CONTRACTOR is responsible for processing mail received at CONTRACTOR facilities from various US Postal Service (USPS) stations, private providers, third party mail services, and/or from

MZ

any CLIENT service centers. USPS, includes national direct mail and express carrier shipments, and mail received at CLIENT HQ.

The CLIENT holidays listed below are excluded from turn-around time (TAT) calculations. Changes in the operating hours required to meet TAT either before, during, or after a CLIENT holiday period, are incorporated into the CONTRACTOR's processing schedule.

New Year's Day
Martin Luther King Day
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Day after Thanksgiving
Christmas Day

All mail received shall reflect a date of receipt.

Mail in USPS units, e.g., mail trays, mailbags or mail tubs, will be received and counted at the CONTRACTOR location. The number of units received will be verified and reconciled to the number of units picked up at the USPS facility.

(b) **Mail Opening and Processing**

CONTRACTOR shall open and count all USPS mail envelopes. Actual count of envelopes processed shall be recorded in the CONTRACTOR's Tracking System. CONTRACTOR staff shall process the mail by extracting all contents from each envelope. Documents will be sorted as detailed in Attachment 4 – Process Flow Diagram.

Mail opening and sorting functions required for Data Entry shall be completed every day to ensure every sort station results in a "Clean Desk", i.e., no carry over work, at the end of the day.

CONTRACTOR conducts the primary mailroom sorts according to the requirements detailed in Attachment 4 – Process Flow Diagram. After completing the primary mailroom sorts, CONTRACTOR processes the work in accordance with separate workflow streams as required for ensuring compliance with mailroom requirements. The workflow streams for scannable and non-scannable documents are detailed in Attachment 4 – Process Flow Diagram.

(c) **Electronic Channel Documents**

CONTRACTOR will establish intake channel for the receipt of electronic documents from CLIENT. Electronic images will flow into the same workflow as

AL

scanned images for basic indexing and enhanced data capture. This intake of electronic documents is outlined in Attachment 4 – Process Flow.

(d) **Electronic Data Capture**

CONTRACTOR shall have infrastructure to support the following workflows as defined in Attachment 3 – Architecture Diagram:

a. Scanning

CONTRACTOR shall scan all documents and document attachments in their mailroom(s) located at the Facility. The transaction date assigned to each claim received from the USPS or other entity will be the actual date the CONTRACTOR receives the mail. Images will be created using standards as provided within Attachment 7 – Electronic Documents Requirements.
The CONTRACTOR shall employ industry standard, systematic and image quality controls to ensure quality requirements and document image clarity is consistently met.

The CONTRACTOR shall rescan documents as needed or requested (within 30 calendar days from scan date). Image quality will be managed and measured by the CONTRACTOR and by CLIENT, as detailed in The Quality Control and Audit Process within the Acceptance and Performance Criteria section herein.

All electronic and physical documents shall be assigned a single, unique Internal Control Number (ICN). Refer to Attachment 6 – Indexing Requirements for full details.

b. Data Entry Verification/Validation

CONTRACTOR shall perform verification/validation controls to ensure quality service levels are met as documented within Attachment 8 – Service Level Agreements.

c. Data Entry With Enhanced Data Capture

CONTRACTOR will utilize enhanced data capture technology (specific enhanced data capture technology may vary by form and process) to supplement and/or enhance manual data entry within CLIENT-defined specifications. The established Quality target is expected to be met and maintained as defined in Attachment 8 – Service Level Agreement – Quality Control and Audit Process.

(e) **Data/Image Output**

CONTRACTOR shall provide data output in the format specified by CLIENT utilizing agreed telecommunication methodologies. Images will be created for all Documents that can be scanned to produce a usable image and those usable images will be clearly readable in every field and output as referenced in Attachment 7 – Electronic Document Requirements. The TIFF images and metadata will be sent from CONTRACTOR to CLIENT through the established telecommunication line. Upon receipt, CLIENT will ensure the document is routed through the imaging system accordingly and all Metadata has been captured. For any documents that are not routed to the imaging system automatically, such as when CONTRACTOR is not presented with the SSN/Account number, CLIENT will perform the necessary research to identify the borrower and assign the applicable attributes.

This is to allow for automated routing of the document to the imaging system and to ensure the document is imaged appropriately. For remediation purposes, CONTRACTOR will track all quality related concerns identified outside of the Audit process.

(f) **Transmissions**

Transmission requirements are listed within Attachment 7 – Electronic Document Requirements.

(g) **Web Reports**

CONTRACTOR shall create the standard reports as listed in Attachment 5 – Reporting Requirements and make available to CLIENT via Secured Internet Site no later than 12:01 am. Eastern Time each business day. These reports will cover the previous business day's activity up to 12:01 am. Eastern Time of the current day. Specific reporting frequencies and durations are provided within Attachment 5 – Reporting Requirements.

(h) **Balancing/Reconciliation**

Balancing / Reconciliation reports are listed in Attachment 5 – Reporting Requirements. Specific reporting frequencies and durations are provided within Attachment 5 – Reporting Requirements.

VI. ASSUMPTIONS AND DEPENDENCIES

(a) The design, development & implementation of the DATAMARK integrated solution will be done in accordance with this SOW with an initial expectation of work completion seven and one-half months after SOW 3 Effective Date. The actual date will be derived from the updated Master Project Plan, which shall be delivered within two weeks of SOW 3 Effective Date.

(b) The updated Master Project Plan will contain the due dates, activities, durations and assigned resources for Phase 2 sufficient to:
   a. Timely design, develop & implement transactional billing (Phase 2 – Transactional Billing)
   b. Timely design, develop & implement DATAMARK integrated solution i.e. (Phase 2 – To-Be System Implementation)

(c) Transactional billing shall be in place from, at the latest, seven and one half (7 ½) months from execution of this SOW, (or other date as may be altered by mutual agreement) through remainder of SOW term.

(d) The Master Project Plan must contain detailed information related to dependencies upon PHEAA so that PHEAA may plan for its role in Phase 2. With respect to dependencies not described in the Master Project Plan, it shall not be considered a delay where PHEAA fails to provide key input upon which a project deadline depends where PHEAA is given less than 10 calendar days of notice to provide such input.

(e) Security Requirements are provided as SOW 3 Attachment 1 – Security Requirements. The Security requirements address Authority to Operate (ATO) extension plan, PHEAA and DATAMARK Network isolation and infrastructure to support the DATAMARK system at the Facility

MJ

(f) CLIENT will be responsible for reclaiming any CLIENT equipment deemed no longer required based on successful implementation of the Phase 2 – To-Be System Implementation.

(g) Additional key assumptions may be found within the associated SOW 3 Attachment documents.

VII. TERM AND WARRANTY DURATION

Warranty duration shall be as indicated in the MSA.
This SOW 3 shall remain effective for a period of four (4) years with the option to extend by mutually-executed update to SOW #3.

VIII. PERFORMANCE CRITERIA

Performance Criteria listed within Attachment 8 – Service Level Agreements, take effect, and supersede prior Service Level Agreements, on the date upon which the DATAMARK integrated solution is being used for 100% of the service volumes. Until that date, prior Service Level Agreements apply and appropriate reporting shall be made by the CONTRACTOR.

IX. CONTRACTOR QUALITY CONTROL AND AUDIT PROCESS

CONTRACTOR shall perform a daily quality audit on a minimum of 2.5% of daily volumes. Results of the Quality Audit shall be available to CLIENT via a secured website. Additional quality audits shall be performed during any start-up phase of processing. During the audit process, CONTRACTOR will correct any identified errors prior to submitting image and data to PHEAA.

CONTRACTOR shall establish a formal mailroom quality assurance process which will measure accuracy of mail handling as part of project execution. CLIENT may assist in the development or refinement of this process.

CONTRACTOR will report results to CLIENT on a weekly or monthly basis, as requested by CLIENT.

X. FEES AND PAYMENT

Fees and Payments information is listed within Attachment 9 – Fees and Payments.

MR

Transactional fees effective no later than seven and one half (7 ½) months after the execution of this SOW, (or other date as may be altered by mutual agreement), are included in Section A of Attachment 9.

Charges, as necessary, for agreed-upon work items which are undertaken after the completion of the rollout of the CONTRACTOR system will be invoiced in accordance with the Rate Card in Section B of Attachment 9 – Fees and Payments. This rate card will remain in effect for the duration of SOW#3 in order to implement approved projects and Change Orders as applicable.

Charges for ongoing Mailroom Services shall continue to be made in accordance with SOW#1 and SOW#2 until the implementation of the transactional fees.

The remainder of this page is left intentionally blank.

IN WITNESS WHEREOF, intending to be legally bound, and in accordance with the MSA by which this SOW is governed, the Parties have hereto by their duly authorized representatives executed this SOW.

PHEAA

By: James H Steeley
(Authorized Signature)

Name: James H. Steeley
(Print Name)

Title: President & CEO

Date: 7/23/19

DATAMARK, INC.

By: Matt Lochausen
(Authorized Signature)

Name: Matt Lochausen
(Print Name)

Title: Vice President

Date: 7/19/2019

PHEAA Legal Counsel
Approved:

Name: Linda Randby
LINDA RANDBY
(Print Name)

Title: Executive Deputy General Counsel

Date: 7/23/19

DATAMARK
INCORPORATED

Attachment 1 to SOW 3, ME17-076-003

Security Controls

A.

DATAMARK will provide and implement controls in accordance with Appendix A, FISMA Moderate – NIST 800-53 standards. .) DATAMARK will also work with a third party assessment organization (3PAO) who will provide assistance in implementing and validating the security controls required per Appendix A. Appendix A may change based on the FISMA moderate revisions by NIST. The Parties acknowledge that Appendix A is NOT static for the duration of the SOW. DATAMARK must timely and appropriately react to those enhancements to remain in compliance.

B.

The 3PAO will receive required material from DATAMARK to present an assessment package that includes an onsite visit to the Facility. The assessment will be in line with current PHEAA security controls and based on a FISMA Moderate – NIST 800-53 Standards, per Appendix A. During the term of this SOW 3, DATAMARK and PHEAA will work in good faith and in a mutually agreed manner and timeframe to make any changes to the Facilities and Contractor's operations as may be required to comply with the Security Requirements directed by FSA or PHEAA from time to time. These controls will be provided by PHEAA. Any changes to this Attachment 1 – Security Controls that could have an impact on cost or process will go through the Change Control process detailed in Section 12 of the MSA for evaluation, cost impact and approval by both parties.

C.

DATAMARK will provide PHEAA required security documentation through several iterations in order to receive feedback to address any gaps. DATAMARK will then provide documentation along with any artifacts required by the 3PAO to create a summary report of their assessment to present to PHEAA. Any security gaps identified will be mitigated by DATAMARK.

D.

PHEAA is responsible for compliance with FSA's requirements. Accordingly, DATAMARK will be part of PHEAA's system boundary and therefore restricted to the performance of activities inside that boundary to those directly related to PHEAA. PHEAA will modify its system security plan (SSP) to include the controls from the

MJ

3PAO assessment to make DATAMARK part of PHEAA's control boundary and this updated SSP will be presented to FSA. As such, PHEAA will be responsible for auditing DATAMARK's practices with a TPRM. DATAMARK will be responsible for having its environment periodically reassessed by DATAMARK's 3PAO for continued compliance in alignment with FSA audits of PHEAA. DATAMARK must demonstrate the continued vulnerability and patch management compliance at the frequency that is compliant with PHEAA requirements and provide required reports to Security Operations Center (SOC) to publish on the PHEAA risk dashboard. FSA will have the right to request that PHEAA arrange to allow them to inspect DATAMARK operations for compliance. DATAMARK must maintain the required documentation and security controls, both physical and logical, in order to meet contractual agreements and protect the confidentiality, integrity and availability of PHEAA's customer data.

DATAMARK
INCORPORATED

Attachment 3 to SOW 3, ME17-076-003

ARCHITECTURE DIAGRAM

Parties acknowledge and agree that all system and asset connectivity and data movement, including the connectivity shown herein, must be reviewed and approved by PHEAA ESO in advance of use.

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

SORT ID	CONTROL_FAMILY	CONTROL_ID	CONTROL_NAME	CONTROL_DESCRIPTION	APPLICABILITY	IMPLEMENTATION_GUIDANCE	COMMENTS
AC-01	ACCESS CONTROL	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency]. Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.	Yes		DATAMARK has access control policies and procedures specific to network access and physical access that is applicable to all sites. They are reviewed and updated at a minimum of a year to keep current with today's business environment. The policies and procedures are reflective with applicable laws, regulations, and directives.
AC-02	ACCESS CONTROL	AC-2	ACCOUNT MANAGEMENT	The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. Supplemental Guidance: Information system account types include individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when			Physical and network access is given based on role-based access and least privilege. At time of reassignment or termination, employee's access is reevaluated to reflect correct role or none, whichever is applicable. Scheduled audits by HR and Security team to ensure policies and procedures for physical and network access are compliant.
AC-02 (01)	ACCESS CONTROL	AC-2 (1)	ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT	The organization employs automated mechanisms to support the management of information system accounts. 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.			DATAMARK uses Network Access Termination Request(NATR) when removing access from a user, this form generates an automated email to the user's manager who needs to approve the removal, then IT is notified by an automatic email to remove the access.
AC-02 (02)	ACCESS CONTROL	AC-2 (2)	ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. 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.	N/A		If temporary or emergency access were given, it would have to be done manually. The one providing access would set a reminder to remove the access when it would be no longer needed.
AC-02 (03)	ACCESS CONTROL	AC-2 (3)	ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	N/A		Accounts don't get to inactive status, once a user is terminated, HR initiates their access removal via our NATR process, IT removes access immediately upon approval from user's manager.
AC-02 (04)	ACCESS CONTROL	AC-2 (4)	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Related controls: AU-2, AU-12.			Account changes are tracked through forms(NATR, NACRs) and are auditible internally by the Security Team
AC-02 (05)	ACCESS CONTROL	AC-2 (5)	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT	The organization requires that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out]. Supplemental Guidance: Related control: SC-23.	Yes		It is DATAMARK's policy for all users to log out of their PC/laptop when leaving their equipment unattended.
AC-02 (07)	ACCESS CONTROL	AC-2 (7)	ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES	The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.			DATAMARK utilizes role-based access for specific individuals to perform admin/privileged roles for network/system administration, database admin, account management, etc.
AC-02 (09)	ACCESS CONTROL	AC-2 (9)	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS	The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].	N/A		It is against DATAMARK policy to allow shared/group accounts into the network

AC-02 (10)	ACCESS CONTROL	AC-2 (10)	ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION	The information system terminates shared/group account credentials when members leave the group.	N/A		It is against DATAMARK policy to allow shared/group accounts into the network.
AC-02 (12)	ACCESS CONTROL	AC-2 (12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE	The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]; and (b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related control: CA-7.			DATAMARK monitors users accounts and can pull reports on each user's usage.
AC-03	ACCESS CONTROL	AC-3	ACCESS ENFORCEMENT	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3. References: None.			Access Control is on need to know basis. There must be an apparent business need to grant access to any employee.
AC-04	ACCESS CONTROL	AC-4	INFORMATION FLOW ENFORCEMENT	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regarding mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message- filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18. References: None.			Network/folder access is done based upon an approval process utilizing electronic forms. Network access request forms are located on our internal intranet called The Source, a product by Adenin. The electronic forms are created utilizing a product called PerfectForms. Workflow of these forms goes for managerial approval, folder owner approver and then forwarded to IT for final implementation. Many of the permissions are handled through Microsoft Active Directory or at folder level. Access is removed when employees change role or leave DATAMARK.
AC-04 (21)	ACCESS CONTROL	AC-4 (21)	INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS	The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization- defined required 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.	Yes	Same as PHEAA SSP	Network/folder access is done based upon an approval process utilizing electronic forms. Network access request forms are located on our internal intranet called The Source, a product by Adenin. The electronic forms are created utilizing a product called PerfectForms. Workflow of these forms goes for managerial approval, folder owner approver and then forwarded to IT for final implementation. Many of the permissions are handled through Microsoft Active Directory or at folder level. Access is removed when employees change role or leave DATAMARK.
AC-05	ACCESS CONTROL	AC-5	SEPARATION OF DUTIES	The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2. Control Enhancements: None. References: None.		Same as PHEAA SSP	Separation of duties is considered for both physical and network access. This is to reduce risk and provide functionality within each department.
AC-06	ACCESS CONTROL	AC-6	LEAST PRIVILEGE	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2. References: None.		Same as PHEAA SSP	Least privilege is considered for both physical and network access. This is to reduce risk and provide functionality within each department.
AC-06 (01)	ACCESS CONTROL	AC-6 (1)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]. 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. Related controls: AC-17, AC-18, AC-19.		Same as PHEAA SSP	Accesses to establishing and configuring security functions are established by least privilege and separation of duties and are auditble by the security Team

AC-06 (02)	ACCESS CONTROL	AC-6 (2)	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non- privileged accounts or roles, when accessing nonsecurity 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. Related control: PL-4.	Same as PHEAA SSP	Non-privileged accounts are in place when accessing nonsecurity functions within the network. Accesses are separate with users and functions than Privileged accounts.
AC-06 (05)	ACCESS CONTROL	AC-6 (5)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles]. 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 system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.	Same as PHEAA SSP	Privileged accounts are restricted to only personnel that need to access certain security functions. Accounts are removed when an employee with a privileged account is also removed from organization.
AC-06 (09)	ACCESS CONTROL	AC-6 (9)	LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS	The information system audits the execution of privileged functions. 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). Related control: AU-2.	Same as PHEAA SSP	Privileged accounts are auditable by the Security Team to ensure proper and authorize use.
AC-06 (10)	ACCESS CONTROL	AC-6 (10)	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	The information system prevents 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.	Same as PHEAA SSP	Functions of privileged and non privileged accounts are separated and prevent non privileged accounts from performing functions that privileged accounts were meant to perform.
AC-07	ACCESS CONTROL	AC-7	UNSUCCESSFUL LOGON ATTEMPTS	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5. References: None.	Same as PHEAA SSP	Account/network lock outs are enabled for both non privileged and privileged accounts. Administrator is required to unlock accounts.
AC-08	ACCESS CONTROL	AC-8	SYSTEM USE NOTIFICATION	The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. Supplemental Guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content. Control Enhancements: None. References: None.	Same as PHEAA SSP	Prior to logging into workstation/PC/Laptop, a message appears describing proper usage of company systems and notice of monitoring, recording, and auditing by the company.
AC-10	ACCESS CONTROL	AC-10	CONCURRENT SESSION CONTROL	The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number]. Supplemental Guidance: Organizations may define the maximum number of concurrent sessions for information 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 information system accounts and does not address concurrent sessions by single users via multiple system accounts. Control Enhancements: None. References: None.	Same as PHEAA SSP	Information systems limits the number of concurrent sessions for each user and type of account based on business need and least privilege.

AC-11	ACCESS CONTROL	AC-11	SESSION LOCK	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information 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 information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7. References: OMB Memorandum 06-16.		Same as PHEAA SSP	Users are advised to log out of accounts at end of the day or when moving away from their workstations. AD policies are in place to enact screensaver or full log off when as applicable to specific users.
AC-11 (01)	ACCESS CONTROL	AC-11 (1)	SESSION LOCK | PATTERN-HIDING DISPLAYS	The information system conceals, 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. References: OMB Memorandum 06-16.		Same as PHEAA SSP	During moment of a screensaver or session lock, an image appears that hides any and all sensitive information that may have appeared on screen when user was active on the workstation.
AC-12	ACCESS CONTROL	AC-12	SESSION TERMINATION	The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect]. Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23. References: None.		Same as PHEAA SSP	Users sessions can be terminated at a schedule time by group policy controls when applicable.
AC-14	ACCESS CONTROL	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication. Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. 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. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2. Control Enhancements: None. (1) PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES [Withdrawn: Incorporated into AC-14]. References: None.		Same as PHEAA SSP	DATAMARK requires all accesses to have proper identification and authentication to be in place to accurately track and monitor accountability into company resources.
AC-17	ACCESS CONTROL	AC-17	REMOTE ACCESS	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections. Supplemental Guidance: Remote access is access to organizational information 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. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4. References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.		Same as PHEAA SSP	Any remote access that is allowed per business need is restricted and configured to reflect specific usage required. VPN usage is given only to those with a business need and requires two-factor authentication to connect.
AC-17 (01)	ACCESS CONTROL	AC-17 (1)	REMOTE ACCESS | AUTOMATED MONITORING / CONTROL	The information system monitors and controls remote access methods. Supplemental Guidance: Automated monitoring and control of remote access sessions allows 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, smart phones, and tablets). Related controls: AU-2, AU-12.		Same as PHEAA SSP	The IT Team monitors and controls any users with a valid remote access need. (VPN users)
AC-17 (02)	ACCESS CONTROL	AC-17 (2)	REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION	The information system implements 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. Related controls: SC-8, SC-12, SC-13.	Yes	Same as PHEAA SSP	Cryptographic mechanisms are in place in the ways of a VPN for all remote sessions into company network.
AC-17 (03)	ACCESS CONTROL	AC-17 (3)	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS	The information system routes all remote accesses through [Assignment: organization-defined number] 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. Related control: SC-7.	Yes	Same as PHEAA SSP	All remote access are managed through company VPN to specific network accesses based on user's role.
AC-17 (04)	ACCESS CONTROL	AC-17 (4)	REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS	The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system. Supplemental Guidance: Related control: AC-6.		Same as PHEAA SSP	Remote access for privileged accounts are given rationale in company security and IT security policies and procedures

MJ

AC-17 (09)	ACCESS CONTROL	AC-17 (9)	REMOTE ACCESS | DISCONNECT / DISABLE ACCESS	The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [Assignment: organization-defined time period]. 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.		Same as PHEAA SSP	DATAMARK's IT Team has the capability to disconnect or disable remote access to the network almost immediate given the proper approvals.
AC-18	ACCESS CONTROL	AC-18	WIRELESS ACCESS	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections. Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4. References: NIST Special Publications 800-48, 800-94, 800-97.		Same as PHEAA SSP	Wireless access is configured and restricted to users with a business need.
AC-18 (01)	ACCESS CONTROL	AC-18 (1)	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION	The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption. Supplemental Guidance: Related controls: SC-8, SC-13.		Same as PHEAA SSP	Wireless access is protected through proper authentication
AC-19	ACCESS CONTROL	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems. Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non- removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4. References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.		Same as PHEAA SSP	DATAMARK configues and implements connections to the network through company laptops only through wireless access that is accessed by user name and password. VPN users require 2-factor authentication for more security.
AC-19 (05)	ACCESS CONTROL	AC-19 (5)	ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION	The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined 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. Related controls: MP-5, SC-13, SC-28. References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.		Same as PHEAA SSP	Encryption is provided on all company laptops to maintain confidentiality and integrity of company information.
AC-20	ACCESS CONTROL	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems. For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as these restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments. This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.usa.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on	Yes	Same as PHEAA SSP	NDAs and third party assessments are put in place prior to any external accesses to our network.
AC-20 (01)	ACCESS CONTROL	AC-20 (1)	USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE	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: (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. 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. Related control: CA-2.	Yes	Same as PHEAA SSP	Any external information system requiring access to our network require third party assessment and a signed NDA. Controls and restrictions are set in place on approved connections.

AC-20 (02)	ACCESS CONTROL	AC-20 (2)	USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES	The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals 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.	Yes	Same as PHEAA SSP	All portable storage devices are restricted to all production PCs. Any business need to use portable storage devices must go through a approval process before authorization is allowed.
AC-21	ACCESS CONTROL	AC-21	INFORMATION SHARING	The organization: a. 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 [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. 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 related to special access programs or 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 special access program/compartment. Related control: AC-3. References: None.		Same as PHEAA SSP	Information sharing is restricted to only authorized personnel based on business need and least privilege.
AC-22	ACCESS CONTROL	AC-22	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered. Supplemental Guidance: In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy. Related controls: AC-3; AC-4, AT-2, AT-3, AU-13. Control Enhancements: None. References: None.		Same as PHEAA SSP	DATAMARK designates specific people in the Marketing team to post information on public access systems such as company website or social media accounts. All information is approved prior to posing to ensure no nonpublic information is disclosed to unathorized sites or personnel.
AT-01	AWARENESS AND TRAINING	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.		Same as PHEAA SSP	As per CORP-SEC-P018-Security Awareness Policy, Security Awareness Training about roles, responsibilities, and compliance regarding HIPAA, PCI-DSS Standards and SOC 2 Type II are performed at during onboarding and annually thereafter. This is tracked by Halogen (HR management software).
AT-02	AWARENESS AND TRAINING	AT-2	SECURITY AWARENESS TRAINING	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4. References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); Executive Order 13587; NIST Special Publication 800-50.		Same as PHEAA SSP	As per CORP-SEC-P018-Security Awareness Policy, Security Awareness Training about roles, responsibilities, and compliance regarding HIPAA, PCI-DSS Standards and SOC 2 Type II are performed at during onboarding and annually thereafter.
AT-02 (02)	AWARENESS AND TRAINING	AT-2 (2)	SECURITY AWARENESS | INSIDER THREAT	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat. Supplemental Guidance: Potential indicators and possible precursors of insider threat can include 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 employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6. References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); Executive Order 13587; NIST Special Publication 800-50.		Same as PHEAA SSP	Insider threat to company security is included in the security awareness training that is performed upon new hire and annual thereafter.

2017

AT-03	AWARENESS AND TRAINING	AT-3	ROLE-BASED SECURITY TRAINING	The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16. References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50.		Same as PHEAA SSP	As per CORP-SEC-P018-Security Awareness Policy, Security Awareness Training about roles, responsibilities, and compliance regarding HIPAA, PCI-DSS Standards and SOC 2 Type II are performed at during onboarding and annually thereafter.
AT-04	AWARENESS AND TRAINING	AT-4	SECURITY TRAINING RECORDS	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period]. Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14. Control Enhancements:: None. References: None.		Same as PHEAA SSP	Training records are kept with HR and also in Paycom, system that tracks all signed documentation for employees.
AU-01	AUDIT AND ACCOUNTABILITY	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.		Same as PHEAA SSP	DATAMARK has policies and procedures in place that address purpose, scope, roles and responsibilities etc. to internal audit and accountabilityt within each project and site globally to ensure correct security controls are in place.
AU-02	AUDIT AND ACCOUNTABILITY	AU-2	AUDIT EVENTS	The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. 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; c. Provides a rationale for why the auditable events are deemed to be adequate to support after- the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	Yes	Same as PHEAA SSP	Audits are conducted on a yearly occurrence for each project and site globally. Spot checks are conducted informally to ensure security and compliance are maintained. During any test or actualy security incident event, the security team doesn intense checks to ensure security and compliance are maintained and hold appropriate parties accountable to the incident.
AU-02 (03)	AUDIT AND ACCOUNTABILITY	AU-2 (3)	AUDIT EVENTS | REVIEWS AND UPDATES	The organization reviews and updates the audited events [Assignment: organization-defined frequency]. 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.		Same as PHEAA SSP	Formal and informal audits are presented to the Senior Management Team in monthly metrics meetings. They are presented again during quarterly meetings with all of operations.
AU-03	AUDIT AND ACCOUNTABILITY	AU-3	CONTENT OF AUDIT RECORDS	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11. References: None.	Yes	Same as PHEAA SSP	Audit events/logs are created and maintained with the details describing the event.

AU-03 (01)	AUDIT AND ACCOUNTABILITY	AU-3 (1)	CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION	The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information]. 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.	Yes	Same as PHEAA SSP	Audit events/logs contain trail of logins, accesses, failed attempts, etc fo all accounts to include privilege accounts.
AU-04	AUDIT AND ACCOUNTABILITY	AU-4	AUDIT STORAGE CAPACITY	The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements]. Supplemental Guidance: Organizations 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. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4. References: None.		Same as PHEAA SSP	IT allocates storage for backup and audit purposes for internal,client and certifcation audits.
AU-05	AUDIT AND ACCOUNTABILITY	AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]. 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. Organizations may choose to define additional actions for different audit processing failures (e.g., by type; by location; by severity; or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12. References: None.		Same as PHEAA SSP	Alerts are in place to notify in the event of storage or capturing failures should occur.
AU-06	AUDIT AND ACCOUNTABILITY	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Audit review, analysis, and reporting covers information security-related auditing performed by organizations 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 nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7. References: None.		Same as PHEAA SSP	Reviews and anlysis on done on a periodic schedule by the IT team. In the event of unusualy or inappropriate findings, the security team and the IT director are notified immediately to remediate and report any issues of the records and logs.
AU-06 (01)	AUDIT AND ACCOUNTABILITY	AU-6 (1)	AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION	The organization 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 Inspector General audits. Related controls: AU-12, PM-7.		Same as PHEAA SSP	The IT Team utilizes a SIEM and other tools to automate audit reviews and reporting to the appropriate personnel to remediate and notify the security team if an incident or anomoly were to occur
AU-06 (03)	AUDIT AND ACCOUNTABILITY	AU-6 (3)	AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES	The organization analyzes and correlates audit records across different repositories to gain organization-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. Related controls: AU-12, IR-4.	Yes	Same as PHEAA SSP	Organizational wide awareness is present due to the audit records situation in repositores for the required personnel to have access to(HR, Ops, IT, Security)
AU-07	AUDIT AND ACCOUNTABILITY	AU-7	AUDIT REDUCTION AND REPORT GENERATION	The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records. Supplemental Guidance: Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-8. References: None.		Same as PHEAA SSP	Reports on auditbale information can be customized for the availability and legibity for the appropriate personnel to be aware and read.
AU-07 (01)	AUDIT AND ACCOUNTABILITY	AU-7 (1)	AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING	The information system provides the capability to process audit records for events of interest based on [Assignment: organization-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		Same as PHEAA SSP	Reports can be customized to only contain certain information that maybe needed for a given situation.
AU-08	AUDIT AND ACCOUNTABILITY	AU-8	TIME STAMPS	The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement]. Supplemental Guidance: Time stamps generated by the information 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. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12. References: None.		Same as PHEAA SSP	Records are date and time stamped as they are created. Any means to change the time settings are only available through privilege admin accounts.
AU-08 (01)	AUDIT AND ACCOUNTABILITY	AU-8 (1)	TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	The information system: (a) Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period]. Supplemental Guidance: This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.		Same as PHEAA SSP	The internal information systems clock is insynced with the correct time source to ensure accurate time stamps throughout the entire network.

AU-09	AUDIT AND ACCOUNTABILITY	**AU-9**	PROTECTION OF AUDIT INFORMATION	The information system protects audit information and audit tools from unauthorized access, modification, and deletion. Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6. References: None.	Same as PHEAA SSP	Audit information and tools are only given to authorized individuals to prevent any unathorized access modification, or deletion of records and reports. Both physical and logical restrictions are in place to ensure accurate data.
AU-09 (02)	AUDIT AND ACCOUNTABILITY	**AU-9 (2)**	PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS	The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited. 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. Related controls: AU-4, AU-5, AU-11.	Same as PHEAA SSP	All audit records are backed up onto a separate device other than the current system being audited.
AU-09 (04)	AUDIT AND ACCOUNTABILITY	**AU-9 (4)**	PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS	The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users]. 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 be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.	Same as PHEAA SSP	Privileged accounts are separated according to the auditing activities and any changes to the audit records. Separation of duties is established so not one person who can retrieve the records is not the only one who can modify or delete the record or activities.
AU-11	AUDIT AND ACCOUNTABILITY	**AU-11**	AUDIT RECORD RETENTION	The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Supplemental Guidance: Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6. References: None.	Same as PHEAA SSP	Audit records are retained to meet regulatory and operational requirements to stay in compliant with applicable laws.
AU-12	AUDIT AND ACCOUNTABILITY	**AU-12**	AUDIT GENERATION	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. Supplemental Guidance: Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7. References: None.	Same as PHEAA SSP	Audit records are sorted and defined to what is auditable in the specific systesm they belong to.
CA-01	SECURITY ASSESSMENT AND AUTHORIZATION	**CA-1**	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.	Same as PHEAA SSP	DATAMARK reviews and updated policies and procedures regarding internal security and fraud assessments on all projects and totes annualy to ensure compliance at all times.

CA-02	SECURITY ASSESSMENT AND AUTHORIZATION	CA-2	SECURITY ASSESSMENTS	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles]. Supplemental Guidance: Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4. References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137	Yes	Same as PHEAA SSP	As per CORP-SEC-P024–Security Compliance Policy, a security assessment is performed on every customer process and each physical site annually. Unannounced inspections are performed periodically to ensure security protocols are being maintained. The security team tracks and reports results and findings to the senior management team monthly.
CA-02 (01)	SECURITY ASSESSMENT AND AUTHORIZATION	CA-2 (1)	SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS	The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments. Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information 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 information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.		Same as PHEAA SSP	The security team which is separate and impartial to the projects conducts internal audits on all processes and sites and include team members who belong to HR, IT, and Ops to provide evidence to prove compliance.
CA-02 (02)	SECURITY ASSESSMENT AND AUTHORIZATION	CA-2 (2)	SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS	The organization includes as part of security control assessments, [Assignment: organization- defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]]. 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 conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.		Same as PHEAA SSP	Penetration tests are conducted quarterly on DATAMARK's network by a third party QSA partner(Control Case). These assessments ensure that both physical and logical access were properly requested and approved by the appropriate authority.
CA-02 (03)	SECURITY ASSESSMENT AND AUTHORIZATION	CA-2 (3)	SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS	The organization accepts the results of an assessment of [Assignment: organization-defined information system] performed by [Assignment: organization-defined external organization] when the assessment meets [Assignment: organization-defined requirements]. 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.		Same as PHEAA SSP	DATAMARK accepts results of the third party QSA partner(Control Case) when vulnerability and penetration test are performed on our information systems.

CA-03	SECURITY ASSESSMENT AND AUTHORIZATION	CA-3	SYSTEM INTERCONNECTIONS	The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]. Supplemental Guidance: This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4. References: FIPS Publication 199; NIST Special Publication 800-47.	Yes	Same as PHEAA SSP	DATAMARK manages connections through rules and policies set in Active Directory and group Policy.
CA-03 (03)	SECURITY ASSESSMENT AND AUTHORIZATION	CA-3 (3)	SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device]. 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 non-national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).	Yes	Same as PHEAA SSP	AT&T Network Based Firewalls are in place to protect internal network from external networks(the internet)
CA-03 (05)	SECURITY ASSESSMENT AND AUTHORIZATION	CA-3 (5)	SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems. Supplemental Guidance: Organizations can restrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.	Yes	Same as PHEAA SSP	Access to external domains are specific to job duties. It is filtered to by whitelisting to ensure business required connections. Any requests to new domains goes through approval by Security Team.
CA-05	SECURITY ASSESSMENT AND AUTHORIZATION	CA-5	PLAN OF ACTION AND MILESTONES	The organization: a. Develops a plan of action and milestones for the information system to document the organization's 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 b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4. References: OMB Memorandum 02-01; NIST Special Publication 800-37.		Same as PHEAA SSP	Based on any findings from the Security Teams internal audits, operations may improve internal processes to reduce future findings as well as policies and procedures to update to match any remediations.
CA-06	SECURITY ASSESSMENT AND AUTHORIZATION	CA-6	SECURITY AUTHORIZATION	The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency]. Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10. Control Enhancements: None. References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137.		Same as PHEAA SSP	DATAMARK has assigned a Security Officer to oversee all security and compliance controls are in place to protect company and client data.
CA-07	SECURITY ASSESSMENT AND AUTHORIZATION	CA-7	CONTINUOUS MONITORING	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]. Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.	Yes	Same as PHEAA SSP	As per CORP-SEC-P024-Security Compliance Policy, a security assessment is performed on every customer process and each physical site annually. Unannounced inspections are performed periodically to ensure security protocols are being maintained. Results and findings are reported to the senior management team during monthly metrics meetings.

CA-07 (01)	SECURITY ASSESSMENT AND AUTHORIZATION	**CA-7 (1)**	CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT	The organization employs assessors or assessment teams with [Assignment: organization-defined level of 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: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.	Same as PHEAA SSP	DATAMARK employes a QSA(Control Case) to perform vulnerability and penetration tests.They also serve as auditors for our PCI and SOC 2 Certifications.
CA-08	SECURITY ASSESSMENT AND AUTHORIZATION	**CA-8**	PENETRATION TESTING	The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components]. Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12. References: None.		Penetration tests are conducted quarterly on DATAMARK's network by a third party QSA partner(Control Case). These assessments ensure that both physical and logical access were properly requested and approved by the appropriate authority.
CA-08 (01)	SECURITY ASSESSMENT AND AUTHORIZATION	**CA-8 (1)**	PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM	The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components. Supplemental Guidance: Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information 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 information systems that are the targets of the penetration testing. Supplemental guidance for CA-2 (1) provides additional information regarding independent assessments that can be applied to penetration testing. Related control: CA-2.		Penetration tests are conducted quarterly on DATAMARK's network by a third party QSA partner(Control Case). These assessments ensure that both physical and logical access were properly requested and approved by the appropriate authority.
CA-09	SECURITY ASSESSMENT AND AUTHORIZATION	**CA-9**	INTERNAL SYSTEM CONNECTIONS	The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. Supplemental Guidance: This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system 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 smart phones with a specific baseline configuration. Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4. References: None.		DATAMARK authorizes and documents all internal connections to job specific personnel and business processes.
CM-01	CONFIGURATION MANAGEMENT	**CM-1**	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.		There are configuration and maintenance policies and procedures in place to ensure a standard for all equipment is performed before going into production. Reviews and updates are done whenever changes are made and on at least an annual basis to ensure documents are current with latest industry security standards.
CM-02	CONFIGURATION MANAGEMENT	**CM-2**	BASELINE CONFIGURATION	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Supplemental Guidance: This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7. References: NIST Special Publication 800-128.		As per CORP-IT-P028-Standard Network Design Rules and CORP-IT-P010- Server Hardening Policy, we maintain a baseline for the configuration of all standardized equipment using Cisco Prime(network devices), Microsoft Windows(desktops/laptops/servers), and VMWare(virtual infrastructure).
CM-02 (01)	CONFIGURATION MANAGEMENT	**CM-2 (1)**	BASELINE CONFIGURATION | REVIEWS AND UPDATES	The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades. Supplemental Guidance: Related control: CM-5.		Baseline configuration is reviewed and updated at least on an annual basis, when client or new regulation mandate it, or during the a system's component installation and upgrade.

CM-02 (02)	CONFIGURATION MANAGEMENT	CM-2 (2)	BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. 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. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related controls: CM-7, RA-5.	DATAMARK utilizes Active Directory and group policy to maintain automated accurate and readily available configuration baseline for the information systems.
CM-02 (03)	CONFIGURATION MANAGEMENT	CM-2 (3)	BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS	The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback. Supplemental Guidance: Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.	DATAMARK retains previous copies of policies and procedures that support baseline configurations of systems to include all software, hardware, firmware, files and records.
CM-02 (07)	CONFIGURATION MANAGEMENT	CM-2 (7)	BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS	The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals 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. \	DATAMARK has all company mobile equipment (laptops) installed with DRUVA which encrypts laptop and are equipped to be remotely wiped in the event of a loss or theft.
CM-03	CONFIGURATION MANAGEMENT	CM-3	CONFIGURATION CHANGE CONTROL	The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board) that convenes (Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions)] Supplemental Guidance: Configuration change controls for organizational information 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 information 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. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12. References: NIST Special Publication 800-128.	Any changes to the configuration of informations systems goes through an approval process to include managers and the security team. Changes are documented in our policies and procedures which also go through an approval process and past documentation and configurations are kept. Annual Internal Security audits are performed to ensure configurations are made or changed with security in mind.
CM-04	CONFIGURATION MANAGEMENT	CM-4	SECURITY IMPACT ANALYSIS	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. 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. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2. References: NIST Special Publication 800-128.	Security analysis and risk assessments are performed by security team and IT managers/directors to ensure any changes in configuration to the systems maintain security overall.
CM-05	CONFIGURATION MANAGEMENT	CM-5	ACCESS RESTRICTIONS FOR CHANGE	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3. References: None.	DATAMARK performs role based access control to physical and network access to systems. Logs are kept that show any additions and removals of access to any newly changed system.
CM-05 (01)	CONFIGURATION MANAGEMENT	CM-5 (1)	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING	The information system enforces access restrictions and supports auditing of the enforcement actions. Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.	Physical and network access is enforced through access control based on least privilege and is auditable by client and internal security team at all times.
CM-05 (03)	CONFIGURATION MANAGEMENT	CM-5 (3)	ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS	The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. 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. Related controls: CM-7, SC-13, SI-7.	Software and firmware that require a digital signature are utilized for verification of authentication before being used or updated onto the systems.

217

CM-05 (05)	CONFIGURATION MANAGEMENT	CM-5 (5)	ACCESS RESTRICTIONS FOR CHANGE	LIMIT PRODUCTION / OPERATIONAL PRIVILEGES	The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges [Assignment: organization-defined frequency]. 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. Related control: AC-2.	Least privilege is in place in making any changes to configurations to system-related information within a production environment. These privileges are reviewed and audited to ensure compliant and if any changes need to be made.
CM-06	CONFIGURATION MANAGEMENT	CM-6	CONFIGURATION SETTINGS		The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. Supplemental Guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security- related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings, and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4. References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: http://nvd.nist.gov, http://checklists.nist.gov, http://www.nsa.gov.	System configurations are set to only allow what a user will required to perform his or her task. These settings are documented in policies and procedures that allow the company to monitor and control any changes that may need to occur. Some examples are lockout enabled, system hardening throught AV and MS patches, and restrictions on network or folder access.
CM-06 (01)	CONFIGURATION MANAGEMENT	CM-6 (1)	CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION		The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components]. Supplemental Guidance: Related controls: CA-7, CM-4.	Configuration settings are done through rules and group policies that allow for easy application, management and verification of accurate system settings.
CM-07	CONFIGURATION MANAGEMENT	CM-7	LEAST FUNCTIONALITY		The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services]. Supplemental Guidance: Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7. References: DoD Instruction 8551.01.	System is configured to allow for least privilege for all users. This include specific folder/network access, ports, protocols, and other services that may have a business need to be enabled. Items not required are restricted unless otherwise approved by manager and security team.
CM-07 (01)	CONFIGURATION MANAGEMENT	CM-7 (1)	LEAST FUNCTIONALITY | PERIODIC REVIEW		The organization: (a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (b) Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure]. 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. Related controls: AC-18, CM-7, IA-2.	The IT and Security Team assess different functions, ports, protocols, etc, to be either secure or not for the company's needs. IF unsecure, the previous examples will be disabled as to not allow any potential vunerabilities open to our network.
CM-07 (02)	CONFIGURATION MANAGEMENT	CM-7 (2)	LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION		The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]. Supplemental Guidance: Related controls: CM-8, PM-5.	Additional programs not part of the job function or initial configuration baseline are restricted from running. If needed, approval process is implemented to include management, IT and Security Teams. Whitelisting is utilized when allowing certain programs to run on the information systems. This is broken up by user and department to allow for least privilege.
CM-07 (05)	CONFIGURATION MANAGEMENT	CM-7 (5)	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING		The organization: (a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: organization- defined frequency]. Supplemental Guidance: 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 or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.	

CM-08	CONFIGURATION MANAGEMENT	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency]. Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, 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. Related controls: CM-2, CM-6, PM-5. References: NIST Special Publication 800-128.	A complete inventory of all hardware and software is maintained by our AMS (asset management system(BMC-TrackIT)). All changes to equipment location, project ownership, replacement, and refresh must go through an approval process that recognizes any potential security risk to systems, data, and personnel. Operations and Accounting work closely together to monitor depreciation cost and end of life on all assets.
CM-08 (01)	CONFIGURATION MANAGEMENT	CM-8 (1)	INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	Through use of BMC-TrackIT, any updates, installations, and removals are tracked accurately and promply regarding the inventory of IS components. DATAMARK is currently doing feasibility studies on several IPS solutions to best meet this criteria
CM-08 (03)	CONFIGURATION MANAGEMENT	CM-8 (3)	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION	The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]]. 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. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.	
CM-08 (05)	CONFIGURATION MANAGEMENT	CM-8 (5)	INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS	The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories. Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.	With the use of AMS (asset management system(BMC-TrackIT)), duplication of any components of the information systems is prevented.
CM-09	CONFIGURATION MANAGEMENT	CM-9	CONFIGURATION MANAGEMENT PLAN	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification. Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10. References: NIST Special Publication 800-128.	As per CORP-IT-P028-Standard Network Design Rules and CORP-IT-P010- Server Hardening Policy, we maintain a baseline for the configuration of all standardized equipment using Cisco Prime(network devices), Microsoft Windows(desktops/laptops/servers), and VMWare(virtual infrastructure). These documents also address roles, responsibilities, and configuration management processes and procedures.
CM-10	CONFIGURATION MANAGEMENT	CM-10	SOFTWARE USAGE RESTRICTIONS	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. 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. Supplemental Guidance: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7. References: None.	Peer-to-peer sharing technology is restricted to only a business need. Any unauthorized uses is tracked and reported to the security team. Items are tracked manually and automatically, and used in accordance with contract agreements and copyright laws.
CM-10 (01)	CONFIGURATION MANAGEMENT	CM-10 (1)	SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE	The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions]. 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. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.	DATAMARK has a policy not allowing the use of open source on the network. Any exceptions go through approval process of IT and Security Teams.
CM-11	CONFIGURATION MANAGEMENT	CM-11	USER-INSTALLED SOFTWARE	The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users; b. Enforces software installation policies through [Assignment: organization-defined methods]; and c. Monitors policy compliance at [Assignment: organization-defined frequency]. Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4. References: None.	DATAMARK policy restricts any software installs except by IT admins. This is to ensure compliance and security for our networks globally.

CP-01	CONTINGENCY PLANNING	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency planning procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.			DATAMARK develops BCP along with any contractural agreements at time of partnership and reviews/updates annually thereafter.
CP-02	CONTINGENCY PLANNING	CP-2	CONTINGENCY PLAN	The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification. Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11. References: Federal Continuity Directive 1; NIST Special Publication 800-34.	Yes	Same as PHEAA SSP	BCP identifies required objectives, roles, responsibilities along with any business and information systems functions. Plan addresses events that would disrupt service and back up and redundancy plans. Plan is reviewed and updated with any changes or contractual agreeemnents.
CP-02 (01)	CONTINGENCY PLANNING	CP-2 (1)	CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS	The organization coordinates contingency plan development with organizational elements 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.	Yes	Same as PHEAA SSP	BCP is developed with potential disasters, crisis, cyber incidents, insider threats that could slow or prevent production.
CP-02 (02)	CONTINGENCY PLANNING	CP-2 (2)	CONTINGENCY PLAN | CAPACITY PLANNING	The organization conducts capacity planning so that necessary capacity for 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.			Capacity planning is included in BCP for information systems, telecommunications, and any environmental support that operations may need.
CP-02 (03)	CONTINGENCY PLANNING	CP-2 (3)	CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS	The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation. 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 resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.			By contractual agreements, if the BCP requires a resumption of any essential business functions, DATAMARK will add to the plan.
CP-02 (08)	CONTINGENCY PLANNING	CP-2 (8)	CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS	The organization identifies critical information system assets supporting 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. Related controls: SA-14, SA-15.	Yes	Same as PHEAA SSP	DATAMARK identifies all critical information system assets through AMS to ensure business/mission functionality.

CP-03	CONTINGENCY PLANNING	CP-3	CONTINGENCY TRAINING	The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that 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 information 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 governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2. References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.	Yes	Same as PHEAA SSP	Training is conducted for BC for employees whose roles and responsibilities are covered at time they take on the role and periodically thereafter. If any changes are made, training is redone to ensure understanding and compliance is adhered.
CP-04	CONTINGENCY PLANNING	CP-4	CONTINGENCY PLAN TESTING	The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed. Supplemental Guidance: Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3. References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.			Contingency testing is done every quarter to ensure business functionality and redundancy on information systems. Results are presented in monthly metrics to senior management team.
CP-04 (01)	CONTINGENCY PLANNING	CP-4 (1)	CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS	The organization coordinates contingency plan testing with organizational elements 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, 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. Related controls: IR-8, PM-8.	Yes	Same as PHEAA SSP	Contingency plan testing is coordinated with cyber incident response plans, BCPs, and DRPs.
CP-06	CONTINGENCY PLANNING	CP-6	ALTERNATE STORAGE SITE	The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site. Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4. References: NIST Special Publication 800-34.			As per CORP-IT-P032-Backup and Recovery Policy, all systems and data are backed up as per customer contract requirements. If no requirements exist, then DATAMARK's standard is 7 dailies, 4 weeklies, 12 monthlies, and 7 yearly backups. These backups are currently performed utilizing Veam software and Dell Data Domain Technologies. Replication of data is performed to multiple BCP locations for enhanced security. Similar security controls are in place at alternate storage site to match main storage site.
CP-06 (01)	CONTINGENCY PLANNING	CP-6 (1)	ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE	The organization identifies 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. Related control: RA-3.			Replication of data is performed to multiple BCP locations for enhanced security.
CP-06 (03)	CONTINGENCY PLANNING	CP-6 (3)	ALTERNATE STORAGE SITE | ACCESSIBILITY	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. 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. Related control: RA-3.			Alternate storage site is also include in the BCP to ensure alternate site is in scope of any potential disaster or incidents that could occur there.
CP-07	CONTINGENCY PLANNING	CP-7	ALTERNATE PROCESSING SITE	The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site. Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. 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. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6. References: NIST Special Publication 800-34.			Per contractual agreements, any additional sites that would need to go hot at moment main site goes down, similar security requirements will be in place to ensure BC and security for client processes.
CP-07 (01)	CONTINGENCY PLANNING	CP-7 (1)	ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE	The organization identifies 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. Related control: RA-3.			Alternate sites that are set as BC sites, are located at different locations that would not be susceptible to same or similar threats.
CP-07 (02)	CONTINGENCY PLANNING	CP-7 (2)	ALTERNATE PROCESSING SITE | ACCESSIBILITY	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. 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. Related control: RA-3.			DATAMARK has seveal sites globally and BCP in place to avoid using a hot site that could also be disrupted by similar disastrous event as main site.

CP-07 (03)	CONTINGENCY PLANNING	CP-7 (3)	ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). 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.			Priority service agreements are in place to ensure proper recovery times in the event of site having issues.
CP-08	CONTINGENCY PLANNING	CP-8	TELECOMMUNICATIONS SERVICES	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization- defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground- based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7. References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: http://www.dhs.gov/telecommunications-service-priority-tsp.	Yes	Same as PHEAA SSP	Alternate telecommunication services are established at all sites using ATT and Verizon telecomms.
CP-08 (01)	CONTINGENCY PLANNING	CP-8 (1)	TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS	The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.			DATAMARK has priority of service agreements with both telecomm services used with ATT and Verizon.
CP-08 (02)	CONTINGENCY PLANNING	CP-8 (2)	TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE	The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Yes	Same as PHEAA SSP	DATAMARK utilizes Verizon as alternate telecom in even primary ATT fails.
CP-09	CONTINGENCY PLANNING	CP-9	INFORMATION SYSTEM BACKUP	The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations. Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13. References: NIST Special Publication 800-34.			As per CORP-IT-P032-Backup and Recovery Policy, all systems and data are backed up as per customer contract requirements. If no requirements exist, then DATAMARK's standard is 7 dailies, 4 weeklies, 12 monthlies, and 7 yearly backups. These backups are currently performed utilizing Veam software and Dell Data Domain Technologies. Replication of data is performed to multiple BCP locations for enhanced security.
CP-09 (01)	CONTINGENCY PLANNING	CP-9 (1)	INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY	The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity. Supplemental Guidance: Related control: CP-4.			Tests on backup are done to ensure reliability and information integrity.
CP-09 (03)	CONTINGENCY PLANNING	CP-9 (3)	INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION	The organization stores backup copies of [Assignment: organization-defined 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 facilites for organizations. Related controls: CM-2, CM-8.			Stored backup copies are located at alternate sites that are separate logically and physically from other information systems needed for operations.
CP-10	CONTINGENCY PLANNING	CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Supplemental Guidance: Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information 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 information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24. References: Federal Continuity Directive 1; NIST Special Publication 800-34.			In the state of disruption or failure, the IT team is able to provide recovery and reconstitution of IS for operational use.
CP-10 (02)	CONTINGENCY PLANNING	CP-10 (2)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY	The information system implements transaction recovery for systems that are transaction-based. Supplemental Guidance: Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.			Transaction recovery is in place for transactional activities such as DBMS.

IA-01	IDENTIFICATION AND AUTHENTICATION	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles] 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency] 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.			DATAMARK addresses both authentication and identification with roles, responsibilities, and management commitment with security Policies and Procedures are reviewed on an annual basis and revised if needed.
IA-02	IDENTIFICATION AND AUTHENTICATION	IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization- controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8. References: HSPD-12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.			As per CORP-SEC-P007-System Access Control Policy, during the onboarding process, employees are assigned a unique user name and complex password(in Active Directory) that is required to be revised every 90-days. This data is replicated to various domain controllers though out DATAMARK's networks. Remote users must apply and be approved for VPN access based on business justification. Applications may be found on "The Source" as an E-form(PerfectForms) called VPN Access Request. Once granted, additional security is enforced utilizing 2-factor authentication.
IA-02 (01)	IDENTIFICATION AND AUTHENTICATION	IA-2 (1)	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS	The information system implements multifactor authentication for network access to privileged accounts. Supplemental Guidance: Related control: AC-6.	Yes	Same as PHEAA SSP	Two-factor authentication is implemented for VPN users who have to be approved to have a business need to do so.
IA-02 (02)	IDENTIFICATION AND AUTHENTICATION	IA-2 (2)	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS	The information system implements multifactor authentication for network access to non- privileged accounts.	Yes	Same as PHEAA SSP	Two-factor authentication is implemented for VPN users who have to be approved to have a business need to do so.
IA-02 (03)	IDENTIFICATION AND AUTHENTICATION	IA-2 (3)	IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS	The information system implements multifactor authentication for local access to privileged accounts. Supplemental Guidance: Related control: AC-6.	N/A	Same as PHEAA SSP	DATAMARK only utilizes MFA for remote access users(company VPN)
IA-02 (05)	IDENTIFICATION AND AUTHENTICATION	IA-2 (5)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION	The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed. Supplemental Guidance: Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators.			All employees use an individual authenticator when gaining physical and network access. No generic or group access provided.
IA-02 (08)	IDENTIFICATION AND AUTHENTICATION	IA-2 (8)	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT	The information system implements replay-resistant authentication mechanisms for network access to 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.			Three levels: ssh is the only approved protocol to manage network devices. Access list are in place to restrict access from any but only network approved administrators. Authentication is approved through Radius server. All network administration is logged for review.
IA-02 (11)	IDENTIFICATION AND AUTHENTICATION	IA-2 (11)	IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE	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 [Assignment: organization-defined strength of mechanism requirements]. 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. Related control: AC-6.			Remote access (VPN) users require multifactor authentication which requires approval and only given through company owned equipment(laptops).
IA-02 (12)	IDENTIFICATION AND AUTHENTICATION	IA-2 (12)	IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS	The information system accepts and electronically verifies 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 agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.	Yes	Same as PHEAA SSP	DATAMARK uses proximity/swipe cards at our U.S locations. These identification/swipe cards are created utilizing Pinnacle Badge Access Software. Badges include name, title, barcode and picture of employee. Logical access is done by user name and complex password which verifies each employee through their PIV. Access is granted on business need only basis.

IA-03	IDENTIFICATION AND AUTHENTICATION	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	The information system uniquely identifies and authenticates [Assignment: organization- defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection. Supplemental Guidance: Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information 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., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5. References: None.	Radius (EAP) authentication is configured for network devices authentication, where network devices have to be defined as valid device. SSH is implemented; telnet is disabled. SNMP is restricted to Monitor server. No Read-write community configured.
IA-04	IDENTIFICATION AND AUTHENTICATION	IA-4	IDENTIFIER MANAGEMENT	The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity]. Supplemental Guidance: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37. References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78	DATAMARK uses Network Access Termination Request(NATR) when removing access from a user, this form generates an automated email to the user's manager who needs to approve the removal, then IT is notified by an automatic email to remove the access. HR submits a Network Access Creation Request (NACR) when requesting new access based on new role/employee. No reuse of identifiers for other personnel.
IA-04 (04)	IDENTIFICATION AND AUTHENTICATION	IA-4 (4)	IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS	The organization manages individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual 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. Related control: AT-2.	The information systems is managed to identify type of individual whom has access to each system.
IA-05	IDENTIFICATION AND AUTHENTICATION	IA-5	AUTHENTICATOR MANAGEMENT	The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes. 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 information 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. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information 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 number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, 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. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-17, SC-13, SC-17, SC-28.	Information systems are authenticate by usernames and passwords. Initial passwords are given by mouth, and are required to change upon initial sign in for each individual. If locked out, only IT admin can unlock and does so only prior to verifying individual and specific access they require. Passwords require complexity with numbers, upper and lower case letters, special character and at least 8 digits. They also expire every 90 days and have a 24 cycle which prevents same password from being used in a short period of time.
IA-05 (01)	IDENTIFICATION AND AUTHENTICATION	IA-5 (1)	AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION	The information system, for password-based authentication: (a) 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]; (b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; (c) Stores and transmits only encrypted representations of passwords; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization- defined numbers for lifetime minimum, lifetime maximum]; (e) Prohibits password reuse for [Assignment: organization-defined number] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password. 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. Related control: IA-6.	Information systems are authenticate by usernames and passwords. Initial passwords are given by mouth, and are required to change upon initial sign in for each individual. If locked out, only IT admin can unlock and does so only prior to verifying individual and specific access they require. Passwords require complexity with numbers, upper and lower case letters, special character and at least 8 digits. They also expire every 90 days and have a 24 cycle which prevents same password from being used in a short period of time.
IA-05 (02)	IDENTIFICATION AND AUTHENTICATION	IA-5 (2)	AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION	The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements 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. Related control: IA-6.	N/A DATAMARK does not utilized PKI within the network.
IA-05 (03)	IDENTIFICATION AND AUTHENTICATION	IA-5 (3)	AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION	The organization requires that the registration process to receive [Assignment: organization- defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].	Registration process needs to be done in person before NACR are sent out with supervisor approval.

IA-05 (04)	IDENTIFICATION AND AUTHENTICATION	IA-5 (4)	AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION	The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements]. Supplemental Guidance: This control enhancement 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 in IA-5 (1). Related controls: CA-2, CA-7, RA-5.	AD enforces individuals passwords are secure enough by making them have numbers, upper and lowercase letters, and a symbol in order for a new password to be created
IA-05 (06)	IDENTIFICATION AND AUTHENTICATION	IA-5 (6)	AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS	The organization protects authenticators commensurate with the security category of the information to which 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.	Access accounts are categorized by level of physical or logival access based on roles and responsibilities
IA-05 (07)	IDENTIFICATION AND AUTHENTICATION	IA-5 (7)	AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or 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).	Unencrypted static authenticators such as passwords are not embedded in applications or stored on function keys
IA-05 (11)	IDENTIFICATION AND AUTHENTICATION	IA-5 (11)	AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION	The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements]. 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.	Systems that require token-based authentication are user specific and cannot be used by another individual.
IA-06	IDENTIFICATION AND AUTHENTICATION	IA-6	AUTHENTICATOR FEEDBACK	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. Supplemental Guidance: The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. Related control: PE-18. Control Enhancements: None. References: None.	Password authenticators are obscurred with asterisks/dots to ensure no one other than the user knows what is being type, especially if another person is shoulder surfing.
IA-07	IDENTIFICATION AND AUTHENTICATION	IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related controls: SC-12, SC-13. Control Enhancements: None. References: FIPS Publication 140; Web: csrc.nist.gov/groups/STM/cmvp/index.html.	N/A	DATAMARK does not have anything that requries using cryptographic modules for authentication
IA-08	IDENTIFICATION AND AUTHENTICATION	IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Supplemental Guidance: Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non- organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations 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 information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8. References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: http://idmanagement.gov.		DATAMARK has contractors with VPN access that goes through an approval process that utilizes two factor authentication and only allows them the access that is required for their specific task
IA-08 (01)	IDENTIFICATION AND AUTHENTICATION	IA-8 (1)	IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other 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 agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.	N/A	
IA-08 (02)	IDENTIFICATION AND AUTHENTICATION	IA-8 (2)	IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS	The information system accepts 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. Related control: AU-2.	N/A	
IA-08 (03)	IDENTIFICATION AND AUTHENTICATION	IA-8 (3)	IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS	The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] 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. Related control: SA-4.	N/A	
IA-08 (04)	IDENTIFICATION AND AUTHENTICATION	IA-8 (4)	IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES	The information system conforms 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). Related control: SA-4.	N/A	

IR-01	INCIDENT RESPONSE	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.			DATAMARK utilizes policies and procedures to implement security incident response in align with scope, roles, and responsibilities in the event of a security incident. They are reviewed and updated at least on an annual basis and when something helps to improve the response team or process.
IR-02	INCIDENT RESPONSE	IR-2	INCIDENT RESPONSE TRAINING	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. 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 information 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. Related controls: AT-3, CP-3, IR-8. References: NIST Special Publications 800-16, 800-50.			Security Incident Response Training is performed yearly on IT personnel and key operations to describe processes, roles, and reponsibilities on everyone involved.
IR-03	INCIDENT RESPONSE	IR-3	INCIDENT RESPONSE TESTING	The organizaion tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results. 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. Related controls: CP-4, IR-8. References: NIST Special Publications 800-84, 800-115.			A test for responding to a security incident is performed yearly and goes thru an extensive walkthrough of a staged incident from start to finish. Policies and procedures can improve upon after the ending of the test.
IR-03 (02)	INCIDENT RESPONSE	IR-3 (2)	INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS	The organization coordinates incident response testing with organizational elements 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.			Security Incident Response testing takes into account current DR and BCP considering internal and external factors.
IR-04	INCIDENT RESPONSE	IR-4	INCIDENT HANDLING	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information 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 information 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, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7. References: Executive Order 13587; NIST Special Publication 800-61.			Security Incident Handling takes into account steps to remediation that include: Preparation, identification, containment, eradication, recovering and lessons learned. All taking into account current BCP and DRP that DATAMARK has in place internal and with our customers. It takes into account previous tesing and handling of prior incidents.
IR-04 (01)	INCIDENT RESPONSE	IR-4 (1)	INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES	The organization employs automated mechanisms to support the incident handling process. Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.			Automated tools used to assist in incident handling include redundancy and alternate hot sites ready to go in the case of incidents that hinder or stop operations.
IR-05	INCIDENT RESPONSE	IR-5	INCIDENT MONITORING	The organization tracks and documents information system security incidents. Supplemental Guidance: Documenting information 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. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7. References: NIST Special Publication 800-61.	Yes	Same as PHEAA SSP	DATAMARK tracks and maintains all security incidents to include reports of type, remidation, personnel involved and client/data affected. A physical log is printed along with digital log to share with client if requested.
IR-06	INCIDENT RESPONSE	IR-6	INCIDENT REPORTING	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities]. Supplemental Guidance: 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. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8. References: NIST Special Publication 800-61; Web: http://www.us-cert.gov.	Yes	Same as PHEAA SSP	DATAMARK requires all employees to report potential fraud. Reporting information is provided on internal web site called The Source. Fraud reporting posters are posted throughout all sites for non staff employees to be aware of how to report fraud. Awareness is also brought on upon new hire and annually thereafter.

2 of 2

IR-06 (01)	INCIDENT RESPONSE	IR-6 (1)	INCIDENT REPORTING | AUTOMATED REPORTING	The organization employs automated mechanisms to assist in the reporting of security incidents. Supplemental Guidance: Related control: IR-7.			DATAMARK uses Solar winds that alerts when there is any abnormality involved with the network.
IR-07	INCIDENT RESPONSE	IR-7	INCIDENT RESPONSE ASSISTANCE	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.			Fraud posters are posted througout all sites that assist all information system users to know how to report security incidents.
IR-07 (01)	INCIDENT RESPONSE	IR-7 (1)	INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT	The organization employs 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.			Availability on information on reporting a security incident is located on our internal website called The Source.
IR-07 (02)	INCIDENT RESPONSE	IR-7 (2)	INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS	The organization: (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) Identifies organizational incident response team members to the external providers. 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.	N/A	Same as PHEAA SSP	DATAMARK does not use any external providers for protecton of our information systems. Everything is done in house.
IR-08	INCIDENT RESPONSE	IR-8	INCIDENT RESPONSE PLAN	The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification. 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 to 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 information systems. Related controls: MP-2, MP-4, MP-5. Control Enhancements: None. References: NIST Special Publication 800-61.			As per CORP-IT-P011-Security Incident Management Policy, DATAMARK activates a security incident response team to resolve any security incidents that pose risk to DATAMARK facilities, network, and personnel. This team will include personnel from different functional areas and different levels of operational hierarchy. Responses are categorized by risk(Low, Medium, and High) in order to coordinate respective personnel and resources for proper and timely remediation according to risk level SLA. As per above policy, incident response testing is performed annually. Security Incident Response team goes through the following steps during an incident: Preparation, Identification, Containment, Eradication, Recovery and Closure, and Follow-up/Lessons Learned
IR-09	INCIDENT RESPONSE	IR-9	INFORMATION SPILLAGE RESPONSE	The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other [Assignment: organization-defined actions]. Supplemental Guidance: Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information 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 an information 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 information 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. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated. References: None.	Yes	Same as PHEAA SSP	As per CORP-IT-P011-Security Incident Management Policy, DATAMARK activates a security incident response team to resolve any security incidents that pose risk to DATAMARK facilities, network, and personnel. This team will include personnel from different functional areas and different levels of operational hierarchy. Responses are categorized by risk(Low, Medium, and High) in order to coordinate respective personnel and resources for proper and timely remediation according to risk level SLA. As per above policy, incident response testing is performed annually. Security Incident Response team goes through the following steps during an incident: Preparation, Identification, Containment, Eradication, Recovery and Closure, and Follow-up/Lessons Learned.
IR-09 (01)	INCIDENT RESPONSE	IR-9 (1)	INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL	The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.	Yes	Same as PHEAA SSP	DATAMARK assings the Security Team and IT Director to respond to any information spills.
IR-09 (02)	INCIDENT RESPONSE	IR-9 (2)	INFORMATION SPILLAGE RESPONSE | TRAINING	The organization provides information spillage response training [Assignment: organization- defined frequency].	Yes	Same as PHEAA SSP	Information spillage response training is incorporated to the security incident response training.
IR-09 (03)	INCIDENT RESPONSE	IR-9 (3)	INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS	The organization implements [Assignment: organization-defined 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.	Yes	Same as PHEAA SSP	DATAMARK tests and implemnts a BCP with specific clients to ensure personnel can continue to undergo assigned tasks.
IR-09 (04)	INCIDENT RESPONSE	IR-9 (4)	INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL	The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned annes 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.	Yes	Same as PHEAA SSP	Each personnel is aware of reporting fraud and/or any unathorized access to systems not pertinate to their roles and responsibilites.

117

MA-01	MAINTENANCE	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.	DATAMARK has proper maintenance policies and procedures regarding security controls over information systems are in place with risk management in mind. Documents are reviewed and updated on annual and needed basis.
MA-02	MAINTENANCE	MA-2	CONTROLLED MAINTENANCE	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records. Supplemental Guidance: This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal 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. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2. References: None.	As per CORP-SEC-P010-Destruction and Disposal of Sensitive Data Policy, proper disposal, labeling and sanitation procedures are in place with equipment that contains confidential company and/or customer data. DATAMARK follows all DOD standards for sanitizing writable media. A certificate of destruction is required for all disposed assets.
MA-03	MAINTENANCE	MA-3	MAINTENANCE TOOLS	The organization approves, controls, and monitors information system maintenance tools. Supplemental Guidance: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6. References: NIST Special Publication 800-88.	Any and all maintenance tools used for diagnostics or repair go through an proper approval process to mitigate any security concerns that could transport any malware into the information systems.
MA-03 (01)	MAINTENANCE	MA-3 (1)	MAINTENANCE TOOLS | INSPECT TOOLS	The organization inspects 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. Related control: SI-7.	All maintenance tools brought into sites are inpsected prior to any approved modifications to ensure no improper/unathorized malicious code is introduced into our informaton systems.
MA-03 (02)	MAINTENANCE	MA-3 (2)	MAINTENANCE TOOLS | INSPECT MEDIA	The organization checks media containing diagnostic and test programs for malicious code before the media are used in the 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. Related control: SI-3.	DATAMARK tests any approved media for malicous code prior to being introduced to the information systems.
MA-03 (03)	MAINTENANCE	MA-3 (3)	MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from 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.	Authorized removal of maintenance equipment is verified to not have any organizational data, prior to leaving the site.
MA-04	MAINTENANCE	MA-4	NONLOCAL MAINTENANCE	The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed. Supplemental Guidance: Nonlocal 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 information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. 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-4 is accomplished in part by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17. References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.	Any nonlocal maintainence or diagnostic activities are done through an approval process of change control and any processes are made aware of details of any disruption to services. Logs and records are kept for history purposes.

MA-04 (02)	MAINTENANCE	**MA-4 (2)**	NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE	The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.			Nonlocal maintance policy and procedures are reviewed and updated at an annual basis.
MA-05	MAINTENANCE	**MA-5**	MAINTENANCE PERSONNEL	The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. Supplemental Guidance: This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information 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, systems integrators, and consultants, may require privileged access to organizational information 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. Related controls: AC-2, IA-8, MP-	Yes	Same as PHEAA SSP	DATAMARK has established a visitor policy for approved maintenance and vendors to assist in the site. They are escorted at all times by a DATAMARK employee to ensure no unathorized entry or removal of company assests.
MA-05 (01)	MAINTENANCE	**MA-5 (1)**	MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS	The organization: (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (1) 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; (2) 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 (b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. 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 on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems. Related controls: MP-6, PL-2.	Yes	Same as PHEAA SSP	IF a person does not have proper security clearance or proper qualifiacations, they will not be permitted in restricted areas physically and logically.
MA-06	MAINTENANCE	**MA-6**	TIMELY MAINTENANCE	The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure. Supplemental Guidance: Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15. References: None.			Amy maintenance support or agreements are contractually agreed upon along with a vetting process to ensure any vendor support is properly approved.
MP-01	MEDIA PROTECTION	**MP-1**	MEDIA PROTECTION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.			DATAMARK has policies and procedures in place to ensure proper media protecton in regards to the availability, integrity and confidentiality of our information systems. These documents are reviewed on an annual and needed basis to ensure they are up to date with latest security trends and practices.
MP-02	MEDIA PROTECTION	**MP-2**	MEDIA ACCESS	The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.	Yes	Same as PHEAA SSP	All production POs have external mass storage capabilites disabled to prevent the unauthorized transfer of data per CORP-IT-P039-Standard Systems Specifications Policy. DATAMARK utilizes various monitoring tools(Dell Enterprise Management System, TrackIT) to monitor all devices and activity connected to USB ports.
MP-03	MEDIA PROTECTION	**MP-3**	MEDIA MARKING	The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas]. Supplemental Guidance: 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 information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk 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 containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-2, RA-3. Control Enhancements: None. References: FIPS Publication 199.			As per CORP-SEC-P008-Information Labeling Policy, all media is properly stored and labeled(Public, Internal, Confidential, and Restricted) to reflect the confidentiality of the data being stored. If information is sensitive (DATAMARK Confidential or DATAMARK Restricted), from the time it is created until the time it is destroyed or declassified, it must be labeled (marked) with an appropriate Data Security designation. Such markings must appear on all manifestations of the information (hardcopies, flash drives, disk drives, CD-ROMs, etc.).

MJ

MP-04	MEDIA PROTECTION	MP-4	MEDIA STORAGE	The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. 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 provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3. References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.			As per CORP-SEC-P010-Destruction and Disposal of Sensitive Data Policy, proper disposal, labeling and sanitation procedures are in place with equipment that contains confidential company and/or customer data. DATAMARK follows all DOD standards for sanitizing writable media.
MP-05	MEDIA PROTECTION	MP-5	MEDIA TRANSPORT	The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel. Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record retention criteria for the different types of media transport as well as the custody chains of transported media. Related controls: AC-19, CP-9, MP-3.	N/A		DATAMARK does not transport information systems media outside of their designated area for any purpose.
MP-05 (04)	MEDIA PROTECTION	MP-5 (4)	MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. Supplemental Guidance: This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: MP-2. References: FIPS Publication 199; NIST Special Publication 800-60.	N/A	Same as PHEAA SSP	DATAMARK does not transport any portable storage devices with confidential or secret information.
MP-06	MEDIA PROTECTION	MP-6	MEDIA SANITIZATION	The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization- defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. Supplemental Guidance: This control applies to all information system media, both digital and non- digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4. References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.	Yes	Same as PHEAA SSP	As per CORP-SEC-P010-Destruction and Disposal of Sensitive Data Policy, proper disposal, labeling and sanitation procedures are in place with equipment that contains confidential company and/or customer data. DATAMARK follows all DOD standards for sanitizing writable media. A certificate of destruction is required for all disposed assets.
MP-06 (02)	MEDIA PROTECTION	MP-6 (2)	MEDIA SANITIZATION | EQUIPMENT TESTING	The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved. 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).			Along with above, intended sanitized equipment is tested to ensure proper sanitization process and procedures.
MP-07	MEDIA PROTECTION	MP-7	MEDIA USE	The organization [Selection: restricts; prohibits] the use of [Assignment: organization- defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards]. Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), in contrast to MP-2, which restricts user access to media. This control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4. References: None.			All production PCs have external mass storage capabilities disabled to prevent the unauthorized transfer of data per CORP-IT-P039-Standard Systems Specifications Policy. DATAMARK utilizes various monitoring tools(Dell Enterprise Management System, TrackIT) to monitor all devices and activity connected to USB ports.
MP-07 (01)	MEDIA PROTECTION	MP-7 (1)	MEDIA USE | PROHIBIT USE WITHOUT OWNER	The organization prohibits the use of portable storage devices in organizational information 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). Related control: PL-4.			

MJ

PE-01	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.			DATAMARK Reviews and updates polices and procedures pertaining to the physical environment protection according to applicable city and country specific laws.
PE-02	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Removes individuals from the facility access list when access is no longer required. 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 level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3. References: None.	Yes	Same as PHEAA SSP	Physical access is given based on role-based access and least privilege. At time of reassignment or termination, employee's access is reevaluated to reflect correct role or none, whichever is applicable. Access is granted by use of proximity/swipe cards. Scheduled audits by HR and Security team to ensure policies and procedures for physical access are compliant.
PE-03	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-3	PHYSICAL ACCESS CONTROL	The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. 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. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information 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, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3. Supplemental Guidance: Related controls: CA-2, CA-7.	Yes	Same as PHEAA SSP	DATAMARK verifies physical access via proximity/smart card/badges for employees. Visitors must show proper ID before being issues a visitors badge and are escorted at all times while present at the site. Visitor logs are present for the site and data centers where unauthorized persons require access to secure areas. Any physical keys for the site are kept only by the site leader and facilities manager of the site.
PE-04	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards]. Supplemental Guidance: Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8. Control Enhancements: None. References: NISTISSI No. 7003.			Physical access to data center and other critical wiring for the information systems is restricted to business need only to applicable IT teams.
PE-05	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. 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. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18. References: None.	Yes	Same as PHEAA SSP	All information system output devices are only accesa by authorized personnel only with respect to least privilege.
PE-06	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-6	MONITORING PHYSICAL ACCESS	The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability. Supplemental Guidance: Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours, (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8. References: None.			Physical access logs are kept and restrict unathorized access at non business hours. Any detection of this will alert third party alarm service to facilites and site manager.

MZ

PE-06 (01)	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-6 (1)	MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT	The organization monitors physical intrusion alarms and surveillance equipment.	Site monitores CCTV everytime by several different personnel. Intrudion alarms are monitored by third party to ensure safety and security.
PE-08	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-8	VISITOR ACCESS RECORDS	The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency]. 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. References: None.	A visitor log is kept to ensure tracking of authorized visitors to any site. Paper log is kept at min of 90 days and is filled out entirely to track any visitors.
PE-09	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-9	POWER EQUIPMENT AND CABLING	The organization protects power equipment and power cabling for the information system from damage and destruction. Supplemental Guidance: Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4. References: None.	Diesel generators are proteced outside by fence and lock. Necessary power equipment and cabling is locked in secure closet in the sites to prevent tampering or misuse of equipment.
PE-10	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-10	EMERGENCY SHUTOFF	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related control: PE-15. References: None.	Access to any emergency shutoff is locked and secure to authorized individuals who can access it.
PE-11	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-11	EMERGENCY POWER	The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss. Supplemental Guidance: Related controls: AT-3, CP-2, CP-7. References: None.	Sites have diesel generators in place that can run up to 72 hours in the case of a longterm power outage. There are vendors availble to facilitate additional fuel delivery when needed.
PE-12	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-12	EMERGENCY LIGHTING	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7. References: None.	Emergency lighting is automatically activated in the case of power outage to light up emergency exits and routes particularly for the data centers as well.
PE-13	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-13	FIRE PROTECTION	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. References: None.	Fire detection/suppression is present for the sites according to local laws to include fire extinguishers, fire detectors, sprinklers and alarms to a third party who can assist in case of large fire.
PE-13 (02)	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-13 (2)	FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS	The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]. 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.	Fire suppression systems are linked to third party when activated. They then send notification to facilities manager and site leader to respond to the incident.
PE-13 (03)	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-13 (3)	FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION	The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	Automatic fire suppression is presently activated during non business hours.
PE-14	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-14	TEMPERATURE AND HUMIDITY CONTROLS	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency]. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3. References: None.	Data center is equipped with temperature and humidity controls that alert third party when conditions are outside certain conditions. Third party then sends alerts to facilities and site leader to initiate the response.
PE-14 (02)	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-14 (2)	TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS	The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.	See above
PE-15	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-15	WATER DAMAGE PROTECTION	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations. Related control: AT-3. References: None.	Our Data Center is monitored for moisture and temperature that is tested annually.

PE-16	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-16	DELIVERY AND REMOVAL	The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items. Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12. References: None.	As per ELP-FAC-P003-Facilities Security Policy, a 24X7 Surveillance system w/CCTVs(currently 150 DATAMARK wide) is in place to capture all entrance points and areas where confidential data is being received, processed and stored. Camera Logs along with physical and electronic Access Logs are kept for a minimum of 90-days in a secure location.
PE-17	PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-17	ALTERNATE WORK SITE	The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. Supplemental Guidance: Alternate work sites may include, for example, government 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. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative. Related controls: AC-17, CP-7. Control Enhancements: None. References: NIST Special Publication 800-46.	DATAMARK establishes alternate/hot/cold sites when contractually required by specific clients.
PL-01	PLANNING	PL-1	SECURITY PLANNING POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-18, 800-100.	DATAMARK reviews and updates policies and procedures related to security planning to include all personnel to maintain security with the information systems.
PL-02	PLANNING	PL-2	SYSTEM SECURITY PLAN	The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification. Supplemental Guidance: Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements 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, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17. References: NIST Special Publication 800-18.	DATAMARK designs all the systems to ensure the separation(physical and logical) of all individual client information. System architectural is planned with security in mind to ensure availability, confidentiality and integrity of the data.
PL-02 (03)	PLANNING	PL-2 (3)	SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities. 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 includes emergency and nonemergency (i.e., planned or nonurgent 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. Related controls: CP-4, IR-4.	Any activities pertaining to informaton systems go thru an approval process regardless if it is emergency or non-emergency situation.

PL-04	PLANNING	PL-4	RULES OF BEHAVIOR	The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. Supplemental Guidance: This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5. References: NIST Special Publication 800-18.	All employees are communicated their roles and responsibilities pertaining to acceptable system use according to their job description
PL-04 (01)	PLANNING	PL-4 (1)	RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS	The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non- public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.	As per CORP-SEC-P025-Staff Communication Systems and Information Security Policy and CORP-SEC-P029-NS Communication Systems and Info Sec, security planning includes training of employees to encompass a security behavior at work to include restrictons on social media.
PL-08	PLANNING	PL-8	INFORMATION SECURITY ARCHITECTURE	The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. Supplemental Guidance: This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role; unique security requirements; the types of information processed, stored, and transmitted by the information system; restoration priorities of information and information system services; and any other specific protection needs. In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-8, PL-2, PM-7, SA-5, SA-17, Appendix J. References: None.	DATAMARK designs all the systems to ensure the separation(physical and logical) of all individual client information. System architectural is planned with security in mind to ensure availability, confidentiality and integrity of the data
PS-01	PERSONNEL SECURITY	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.	DATAMARK implements security policies and procedures that ensure the safety and security of all its personnel to include employees, clients, visitors, and contractors.
PS-02	PERSONNEL SECURITY	PS-2	POSITION RISK DESIGNATION	The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: organization-defined frequency]. Supplemental Guidance: Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances). Related controls: AT-3, PL-2, PS-3. Control Enhancements: None. References: 5 C.F.R. 731.106(a).	As per CORP-HR-P035-Hiring Policy. DATAMARK ensures safety and security of all personnel by starting with the pre-screening and hiring of employees. All prospective employee must undergo an extensive background check and drug screening before hire.

PS-03	PERSONNEL SECURITY	PS-3	PERSONNEL SCREENING	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening]. Supplemental Guidance: Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. Related controls: AC-2, IA-4, PE-2, PS-2. References: 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78, ICD 704.	Yes	Same as PHEAA SSP	As per CORP-HR-P035-Hiring Policy, DATAMARK ensures safety and security of all personnel by starting with the pre-screening and hiring of employees. All prospective employee must undergo an extensive background check and drug screening before hire.
PS-03 (03)	PERSONNEL SECURITY	PS-3 (3)	PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES	The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: (a) Have valid access authorizations that are demonstrated by assigned official government duties; and (b) Satisfy [Assignment: organization-defined additional 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.	Yes	Same as PHEAA SSP	After employees have been approved for hire, they are only granted valid access that is link to their job duties and responsibilities.
PS-04	PERSONNEL SECURITY	PS-4	PERSONNEL TERMINATION	The organization, upon termination of individual employment: a. Disables information system access within [Assignment: organization-defined time period]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]. Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6. References: None.			As per CORP-HR-P078-Termination of Employment Policy all access levels are removed and all company equipment is returned and refreshed.
PS-05	PERSONNEL SECURITY	PS-5	PERSONNEL TRANSFER	The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]. Supplemental Guidance: This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts. Related controls: AC-2, IA-4, PE-2, PS-4. Control Enhancements: None. References: None.			DATAMARK's security team performs annual audits that include reviewing both physical and logical accesses for each project and site. HR performs internal review monthly to ensure all accesses are accurate.
PS-06	PERSONNEL SECURITY	PS-6	ACCESS AGREEMENTS	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency]. Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8. References: None.			All employees sign acceptable use, rules of behavior, and non disclosure prior to being given physical and logical access to the information systems. All employee records are kept in Paycom for storage, retention, and review.
PS-07	PERSONNEL SECURITY	PS-7	THIRD-PARTY PERSONNEL SECURITY	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and e. Monitors provider compliance. Supplemental Guidance: Third-party providers include, for example, service bureaux, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21. Control Enhancements: None. References: NIST Special Publication 800-35.	Yes	Same as PHEAA SSP	DATAMARK does not allow for third parties to have any physical or logical access to our information systems.

PS-08	PERSONNEL SECURITY	PS-8	PERSONNEL SANCTIONS	The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. Supplemental Guidance: Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, polices, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6. Control Enhancements: None. References: None.	DATAMARK initiates formal verbal and written process for employees who do not comply with security policies and procedures up to and include termination
RA-01	RISK ASSESSMENT	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-30, 800-100.	DATAMARK reviews and updates policies and procedures pertaining to risk assessment on any new or updated processes to the information systems or personnel.
RA-02	RISK ASSESSMENT	RA-2	SECURITY CATEGORIZATION	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7. Control Enhancements: None. References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.	Security categories for information systems are listed as Public, DATAMARK internal, DATAMARK Secret, and DATAMARK Confidential to in order to ensure the confidentiality, integrity and availability of our data.
RA-03	RISK ASSESSMENT	RA-3	RISK ASSESSMENT	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the 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. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9. Control Enhancements: None. References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web idmanagement.gov.	As per CORP-SEC-P024-SOP002 - Information Security Risk Management Procedure, risk assessments are performed on every project prior to going live and annually thereafter to reduce risk and strengthen security

RA-05	RISK ASSESSMENT	RA-5	VULNERABILITY SCANNING	The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Supplemental Guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information 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. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2. References: NIST Special Publications 800-40, 800-70, 800-115; Web: http://cwe.mitre.org, http://nvd.nist.gov.	Yes	Same as PHEAA SSP	As per CORP-SEC-P024-Security Compliance Policy, risk assessments are performed with every project. Vulnerability scans are performed internally by information Security and externally using a third party QSA partner(Control Case).
RA-05 (01)	RISK ASSESSMENT	RA-5 (1)	VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. 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. Related controls: SI-3, SI-7.	Yes	Same as PHEAA SSP	DATAMARK utilizes Retina Scan for internal vulnerabilities.
RA-05 (02)	RISK ASSESSMENT	RA-5 (2)	VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED	The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]. Supplemental Guidance: Related controls: SI-3, SI-5.	Yes	Same as PHEAA SSP	Any remediations needed to be fixed are done prior to new scan from being performed
RA-05 (03)	RISK ASSESSMENT	RA-5 (3)	VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE	The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).	Yes	Same as PHEAA SSP	Internal and external vulnerability scans are performed periodically with a specific scope in mind
RA-05 (05)	RISK ASSESSMENT	RA-5 (5)	VULNERABILITY SCANNING | PRIVILEGED ACCESS	The information system implements privileged access authorization to [Assignment: organization- identified information system components] for selected [Assignment: organization-defined 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.	Yes	Same as PHEAA SSP	Scanning is done by a third party QSA and internally by Security Team.
RA-05 (06)	RISK ASSESSMENT	RA-5 (6)	VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES	The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. Supplemental Guidance: Related controls: IR-4, IR-5, SI-4.	Yes	Same as PHEAA SSP	Past scans are compared to current ones to determine any discrepancies or room for improvement when concerning any vulnerabilites found.
RA-05 (08)	RISK ASSESSMENT	RA-5 (8)	VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS	The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited. Supplemental Guidance: Related control: AU-6.	Yes	Same as PHEAA SSP	Logs are analyzed for potential vulnerabilites that are found to see if they have been exploited in the past.
SA-01	SYSTEM AND SERVICES ACQUISITION	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.			DATAMARK reviews and updates policies and procedures related to systems and services acquisition.
SA-02	SYSTEM AND SERVICES ACQUISITION	SA-2	ALLOCATION OF RESOURCES	The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation. Supplemental Guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11. Control Enhancements: None. References: NIST Special Publication 800-65.			Information security is included in all projects that require acquisition of resources and allocated costs for production.

SA-03	SYSTEM AND SERVICES ACQUISITION	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities. Supplemental Guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8. Control Enhancements: None. References: NIST Special Publications 800-37, 800-64.	DATAMARK holds the highest standards in application development regarding security in all steps of the SDLC process.
SA-04	SYSTEM AND SERVICES ACQUISITION	SA-4	ACQUISITION PROCESS	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria. Supplemental Guidance: Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle. Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12. References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: http://www.niap-ccevs.org, http://fips201ep.cio.gov, http://www.acquisition.gov/far.	DATAMARK acquires information technology that coincides with security standard and configuration prior to processing, storing, and transmitting data within and outside of the network.
SA-04 (01)	SYSTEM AND SERVICES ACQUISITION	SA-4 (1)	ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.	DATAMARK holds the highest standards in application development. In order to utilize any third party application during our development process, we must adhere to the following steps: DATAMARK holds the highest standards in application development regarding security in all steps of the SDLC process.
SA-04 (02)	SYSTEM AND SERVICES ACQUISITION	SA-4 (2)	ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS	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: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail]. Supplemental Guidance: 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/resilience, 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	
SA-04 (08)	SYSTEM AND SERVICES ACQUISITION	SA-4 (8)	ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN	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 that contains [Assignment: organization-defined level of detail]. 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. Related control: CA-7.	DATAMARK holds the highest standards in application development regarding security in all steps of the SDLC process to include continuous monitoring over all steps.
SA-04 (09)	SYSTEM AND SERVICES ACQUISITION	SA-4 (9)	ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE	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. 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-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.	Identification of all functions/services are in place in all parts of the SDLC process.

SA-04 (10)	SYSTEM AND SERVICES ACQUISITION	SA-4 (10)	ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS	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. Supplemental Guidance: Related controls: IA-2, IA-8.	N/A		DATAMARK does not have any FIPS products for the information systems.
SA-05	SYSTEM AND SERVICES ACQUISITION	SA-5	INFORMATION SYSTEM DOCUMENTATION	The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to reconstruct selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4. References: None.			DATAMARK implements policies, procedures and work instructions on proper configuration, installation, and operation of all system components in regards to security controls stated
SA-08	SYSTEM AND SERVICES ACQUISITION	SA-8	SECURITY ENGINEERING PRINCIPLES	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Supplemental Guidance: Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles 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: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) 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 (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3. Control Enhancements: None.			Identification of all functions/services are in place in all parts of the SDLC process.
SA-09	SYSTEM AND SERVICES ACQUISITION	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis. Supplemental Guidance: External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations 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. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, 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. Related controls: CA-3, IR-7, PS-7. References: NIST Special Publication 800-35.	Yes	Same as PHEAA SSP	DATAMARK does not use external sources to process, store, or transmit customer data. In the case that we may do so in the future, they third party will go through our vendor policy to ensure they are vetted through same security measures that DATAMARK is responsible in implementing as well
SA-09 (01)	SYSTEM AND SERVICES ACQUISITION	SA-9 (1)	EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS	The organization: (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services. Related controls: CA-6, RA-3.	Yes	Same as PHEAA SSP	No service acquisitions are permitted for production areas or other areas that may view, have access to, or touch any client sensitive data. Other vendors that maybe required for buildouts, setup of equipment, or recruiting must follow vendor policy stated above.
SA-09 (02)	SYSTEM AND SERVICES ACQUISITION	SA-9 (2)	EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES	The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services. Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7.	Yes	Same as PHEAA SSP	No service acquisitions are permitted for production areas or other areas that may view, have access to, or touch any client sensitive data. Other vendors that maybe required for buildouts, setup of equipment, or recruiting must follow vendor policy stated above.
SA-09 (04)	SYSTEM AND SERVICES ACQUISITION	SA-9 (4)	EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS	The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational 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 (i.e., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities.	Yes	Same as PHEAA SSP	No service acquisitions are permitted for production areas or other areas that may view, have access to, or touch any client sensitive data. Other vendors that maybe required for buildouts, setup of equipment, or recruiting must follow vendor policy stated above.

SA-09 (05)	SYSTEM AND SERVICES ACQUISITION	SA-9 (5)	EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION	The organization restricts the location of [Selection (one or more): information processing; information/data; information system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions]. 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 information security 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.	Yes	Same as PHEAA SSP	DATAMARK restricts the data center that houses all storage and services with physical access, 24X7 camera coverage
SA-10	SYSTEM AND SERVICES ACQUISITION	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. Supplemental Guidance: This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2. References: NIST Special Publication 800-128.			DATAMARK holds the highest standards in application development regarding security in all steps of the SDLC process to include continuous monitoring over all steps.
SA-10 (01)	SYSTEM AND SERVICES ACQUISITION	SA-10 (1)	DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION	The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components. Supplemental Guidance: This control enhancement allows organizations 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. Related control: SI-7.			The system components are configured with access control tied to least privilege and a business need to gain access.
SA-11	SYSTEM AND SERVICES ACQUISITION	SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation. Supplemental Guidance: Developmental security testing/evaluation occurs at all post design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2. References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: http://nvd.nist.gov, http://cwe.mitre.org, http://cve.mitre.org, http://capec.mitre.org.			DATAMARK holds the highest standards in application development regarding security in all steps of the SDLC process.
SA-11 (01)	SYSTEM AND SERVICES ACQUISITION	SA-11 (1)	DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS	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. 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.			DATAMARK holds the highest standards in application development regarding security in all steps of the SDLC process.
SA-11 (02)	SYSTEM AND SERVICES ACQUISITION	SA-11 (2)	DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES	The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service. 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 systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to 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. Related controls: PM-15, RA-5.			DATAMARK holds the highest standards in application development. In order to utilize any third party application during our development process, we must adhere to the following steps: Penetration Testing results must be provided by Master Developer Vulnerability testing and history must be reviewed
SA-11 (08)	SYSTEM AND SERVICES ACQUISITION	SA-11 (8)	DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS	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. 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 into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications.			DATAMARK holds the highest standards in application development regarding security in all steps of the SDLC process

SC-01	SYSTEM AND COMMUNICATIONS PROTECTION	SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.			DATAMARK updates and reviews policies and procedures that address scope and responsibilities to the protection of communications in regard to security.
SC-02	SYSTEM AND COMMUNICATIONS PROTECTION	SC-2	APPLICATION PARTITIONING	The information system separates user functionality (including user interface services) from information system management functionality. Supplemental Guidance: Information 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 information 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 information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3. References: None.			DATAMARK utilizes separation of duties in regards to management of information systems.
SC-04	SYSTEM AND COMMUNICATIONS PROTECTION	SC-4	INFORMATION IN SHARED RESOURCES	The information system prevents unauthorized and unintended information transfer via shared system resources. 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 resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6. References: None.			Per use of the shared systems/folders, the access is set to users with a business need through group policies and any requests for additional acces must be approved by the document owner.
SC-05	SYSTEM AND COMMUNICATIONS PROTECTION	SC-5	DENIAL OF SERVICE PROTECTION	**The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].** 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 information 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. Related controls: SC-6, SC-7. References: None.	Yes	Same as PHEAA SSP	DATAMARK's information systems is set with network redundancy and structured to prevent DOS attacks.
SC-06	SYSTEM AND COMMUNICATIONS PROTECTION	SC-6	RESOURCE AVAILABILITY	The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]]. Supplemental Guidance: Priority protection helps prevent lower-priority processes from delaying or interfering with the information 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 information system components for which there are only single users/roles. Control Enhancements: None. References: None.			Network is setup with QoS to ensure proper priority for the resources to be used by their intended purpose.
SC-07	SYSTEM AND COMMUNICATIONS PROTECTION	SC-7	BOUNDARY PROTECTION	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third-party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13. References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.			Network is setup with firewalls, redundant routers, and subnets for both physical and virtual network infrastructure.
SC-07 (03)	SYSTEM AND COMMUNICATIONS PROTECTION	SC-7 (3)	BOUNDARY PROTECTION | ACCESS POINTS	The organization limits 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.			DATAMARK limits VPN usage to a business need and with proper approval.

207

SC-07 (04)	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-7 (4)**	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8.	Yes	Same as PHEAA SSP	VPN usage is only allowed for business need and only access is to staff services, not production data for each client processes.
SC-07 (05)	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-7 (5)**	BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION	The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.	Yes	Same as PHEAA SSP	Information systems are set to only provide access that serves least privilege and business need. If additional access is required, requests must be approved.
SC-07 (07)	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-7 (7)**	BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES	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. 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 information. The use of VPNs for remote connections, when adequately provisioned with 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.			All approved remote access to network must utilize company VPN which is only approved for a business need.
SC-07 (08)	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-7 (8)**	BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces. Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.	Yes	Same as PHEAA SSP	The information systems routes all web traffice through web content filtering that prevents any unathorized access to specific URLs.
SC-07 (12)	SYSTEM AND COMMUNICATIONS PROTECTION	SC-7 (12)	BOUNDARY PROTECTION | HOST-BASED PROTECTION	The organization implements [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined information system components]. Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.			The information systems implements host-based firewalls to protect endpoints such as servers, PCs, and company laptops.
SC-07 (13)	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-7 (13)**	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS	The organization isolates [Assignment: organization-defined information security 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. 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. Related controls: SA-8, SC-2, SC-3.			DATAMARK isolates internal physical separate networks using VLANs to manage interaces of the system.
SC-07 (18)	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-7 (18)**	BOUNDARY PROTECTION | FAIL SECURE	The information system fails securely in the event of an operational failure of a boundary protection device. Supplemental Guidance: 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. Related controls: CP-2, SC-24.			Information systems keep protected devices, secured within the boundary of users intended limits.
SC-08	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-8**	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4. References: FIPS Publication 140-2, NIST Special Publication 800-52, 800-77, 800-81, 800-113, CNSS Policy 15, NSTISSI No. 7003.	Yes	Same as PHEAA SSP	The information systems protects the confidentiality, integrity and availability of all information transmitted internally and externally.
SC-08 (01)	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-8 (1)**	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. 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. Related control: SC-13.			Information sytems implement VPN for encryption with external access. Physical access and logical acces are implemented to prevent unathorized access to tranmissions of data.
SC-10	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-10**	NETWORK DISCONNECT	The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity. Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses. Control Enhancements: None.			Network devices configured with 15 minutes time-out after inactivity. VPN configured for 30 minutes time-out after inactivity.

m7

SC-12	SYSTEM AND COMMUNICATIONS PROTECTION	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] 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 federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17. References: NIST Special Publications 800-56, 800-57.				Proper key management and storage is implemented per client request on certain processes.
SC-12 (02)	SYSTEM AND COMMUNICATIONS PROTECTION	SC-12 (2)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS	The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.			For processes required cryptographic keys, DATAMARK produces, controls, and distributes required keys.
SC-12 (03)	SYSTEM AND COMMUNICATIONS PROTECTION	SC-12 (3)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS	The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].			For processes required cryptographic keys, DATAMARK produces, controls, and distributes required keys.
SC-13	SYSTEM AND COMMUNICATIONS PROTECTION	SC-13	CRYPTOGRAPHIC PROTECTION	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7. References: FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.	Yes	Same as PHEAA SSP	When cryptography is required by client, DATAMARK utilizes them in accordance with federal laws and regulations.
SC-15	SYSTEM AND COMMUNICATIONS PROTECTION	SC-15	COLLABORATIVE COMPUTING DEVICES	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices. Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. Related control: AC-21. References: None.			The information systems prohibits collaborative computing devices to our network. All users are explained proper system usage when accessing DATAMARK information systems.
SC-17	SYSTEM AND COMMUNICATIONS PROTECTION	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	The organization issues public key certificates under an [Assignment: organization- defined certificate policy] or obtains public key certificates from an approved service provider. Supplemental Guidance: For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12. Control Enhancements: None. References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.			DATAMARK utilizes trusted sources for public key certificates that are required for certain client processes.
SC-18	SYSTEM AND COMMUNICATIONS PROTECTION	SC-18	MOBILE CODE	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system. Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information 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., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3. References: NIST Special Publication 800-28; DoD Instruction 8552.01.			DATAMARK prohibits specifice mobile code within the information systems. Accepted mobile code technologies are listed in policies and procedures that are reviewed and updated at least annually.
SC-19	SYSTEM AND COMMUNICATIONS PROTECTION	SC-19	VOICE OVER INTERNET PROTOCOL	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system. Supplemental Guidance: Related controls: CM-6, SC-7, SC-15. References: NIST Special Publication 800-58.			Usage and restrictions of VOIP within our information systems is controlled by our IT teams.
SC-20	SYSTEM AND COMMUNICATIONS PROTECTION	SC-20	SECURE NAME /ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	The information system: a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. Supplemental Guidance: 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. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22. References: OMB Memorandum 08-23; NIST Special Publication 800-81.			External DNS configured with static names. Internal DNS refers to internal resources within DATAMARK to reflect real client names. Services configured in Internal DNS statically, preventing changing their IP/Name relationship.

SC-21	SYSTEM AND COMMUNICATIONS PROTECTION	SC-21	SECURE NAME /ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. Supplemental Guidance: Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data. Related controls: SC-20, SC-22. References: NIST Special Publication 800-81.				Internal clients update DNS dynamically, except when static names are defined.
SC-22	SYSTEM AND COMMUNICATIONS PROTECTION	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. Supplemental Guidance: Information 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 (i.e., 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 (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., 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). Related controls: SC-2, SC-20, SC-21, SC-24. Control Enhancements: None. References: NIST Special Publication 800-81.				External DNS relies in an External Names provider (godaddy), external Names provider have their redundancy systems in place Internal DNS has redundancy: with at least two DNS servers at each location.
SC-23	SYSTEM AND COMMUNICATIONS PROTECTION	SC-23	SESSION AUTHENTICITY	The information system protects the authenticity of communications sessions. 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. Related controls: SC-8, SC-10, SC-11. References: NIST Special Publications 800-52, 800-77, 800-95.	Yes	Same as PHEAA SSP		DATAMARK implements proper protection over sessions into the network via username and complex password, establish via active directory.
SC-28	SYSTEM AND COMMUNICATIONS PROTECTION	SC-28	PROTECTION OF INFORMATION AT REST	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. 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 information 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, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. 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 and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7. References: NIST Special Publications 800-56, 800-57, 800-111.	Yes	Same as PHEAA SSP		The information systems protects the confidentiality, integrity and availability of data at rest.
SC-28 (01)	SYSTEM AND COMMUNICATIONS PROTECTION	SC-28 (1)	PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION	The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [Assignment: organization-defined 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. Related controls: AC-19, SC-12.	Yes	Same as PHEAA SSP		All company laptops utilize cryptographic mechanisms.
SC-39	SYSTEM AND COMMUNICATIONS PROTECTION	SC-39	PROCESS ISOLATION	The information system maintains a separate execution domain for each executing process. Supplemental Guidance: Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through 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. Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3. References: None.				Each customer has their own Address domain. Where applies, address domains are secured behind a firewall. Windows domains, if required, a customer gets a Windows domain, for their own processes, no trust relationship with DATAMARK. Unless specifically stated in the work relationship, customers get to use DATAMARK domain for authentication. DATAMARK reviews and updates policies and procedures dealing with system integrity.
SI-01	SYSTEM AND INFORMATION INTEGRITY	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency]. 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 federal laws, Executive Orders, directives, 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 information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.				DATAMARK reviews and updates policies and procedures dealing with system integrity.

SI-02	SYSTEM AND INFORMATION INTEGRITY	SI-2	FLAW REMEDIATION	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization- defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, 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 information 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. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical; for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5,	MS patches and other firmware updates are tested in virtual environment prior to patching live equipment.
SI-02 (02)	SYSTEM AND INFORMATION INTEGRITY	SI-2 (2)	FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS	The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation. Supplemental Guidance: Related controls: CM-6, SI-4.	As per CORP-IT-P009-Patching and Antivirus Policy, DATAMARK ensures all servers and desktops connected to the DATAMARK network have proper virus protection software(Sophos), current virus definition libraries and the most recent operating system security patches using WSUS and Cisco Prime.
SI-02 (03)	SYSTEM AND INFORMATION INTEGRITY	SI-2 (3)	FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS	The organization: (a) Measures the time between flaw identification and flaw remediation; and (b) Establishes [Assignment: organization-defined benchmarks] for taking corrective actions. Supplemental Guidance: This control enhancement requires organizations to determine the current time it takes on the average to correct information system flaws after such flaws have been identified, and subsequently establish organizational benchmarks (i.e., 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.	As per CORP-IT-P009-Patching and Antivirus Policy, DATAMARK ensures all servers and desktops connected to the DATAMARK network have proper virus protection software(Sophos), current virus definition libraries and the most recent operating system security patches using WSUS and Cisco Prime. DATAMARK uses Sophos for AV, protection against malicious code. Updates are automaticly occuring every 10 mins.
SI-03	SYSTEM AND INFORMATION INTEGRITY	SI-3	MALICIOUS CODE PROTECTION	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of malicousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. References: NIST Special Publication 800-83.	DATAMARK uses Sophos for AV, protection against malicious code. Updates are automaticly occuring every 10 mins.
SI-03 (01)	SYSTEM AND INFORMATION INTEGRITY	SI-3 (1)	MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT	The organization centrally manages malicious code protection mechanisms. Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.	DATAMARK uses Sophos for AV, protection against malicious code. Updates are automaticly occuring every 10 mins.
SI-03 (02)	SYSTEM AND INFORMATION INTEGRITY	SI-3 (2)	MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES	The information system automatically updates malicious code protection mechanisms. Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.	DATAMARK uses Sophos for AV, protection against malicious code. Updates are automaticly occuring every 10 mins.
SI-03 (07)	SYSTEM AND INFORMATION INTEGRITY	SI-3 (7)	MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION	The information system implements nonsignature-based malicious code detection mechanisms. N/A 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 (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.	DATAMARK is currently doing feasibility studies on several IPS solutions to best meet this criteria.

SI-04	SYSTEM AND INFORMATION INTEGRITY	SI-4	INFORMATION SYSTEM MONITORING	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]]. Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7. References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.	DATAMARK utilizes Sophos, WSUS, Barracuda and Solarwinds to protect and secure the data that is being processed and at rest. Alerts are configured to identify any abnormalities or potential threats on the network and are used to notify the Information Technology Support Teams.
SI-04 (01)	SYSTEM AND INFORMATION INTEGRITY	SI-4 (1)	INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM	The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.	DATAMARK is currently doing feasibility studies on several IPS solutions to best meet this criteria DATAMARK utilizes Solar Winds LEM and Orion to monitor real time analysis of network devices.
SI-04 (02)	SYSTEM AND INFORMATION INTEGRITY	SI-4 (2)	INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	The organization employs automated tools to support near real-time analysis of events. Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.	
SI-04 (04)	SYSTEM AND INFORMATION INTEGRITY	SI-4 (4)	INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions. Supplemental Guidance: Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.	DATAMARK utilizes Solar Winds LEM and Orion to monitor real time analysis of network devices.Solar winds sends alerts with any anomolies.
SI-04 (05)	SYSTEM AND INFORMATION INTEGRITY	SI-4 (5)	INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization- defined compromise indicators]. 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. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.	DATAMARK utilizes Solar Winds LEM and Orion to monitor real time analysis of network devices.Solar winds sends alerts with any anomolies.
SI-04 (14)	SYSTEM AND INFORMATION INTEGRITY	SI-4 (14)	INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION	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. 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. Related controls: AC-18, IA-3.	No IDS is in place to detect rogue access points, but personnel check daily for what access points are present to ensure no rogue access points are present. DATAMARK is currently doing feasibility studies on several IPS solutions to best meet this criteria
SI-04 (16)	SYSTEM AND INFORMATION INTEGRITY	SI-4 (16)	INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION	The organization correlates information from monitoring tools employed throughout the information system. 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. Related control: AU-6.	DATAMARK utilizes Sophos, WSUS, Barracuda and Solarwinds to protect and secure the data that is being processed and at rest. Alerts are configured to identify any abnormalities or potential threats on the network and are used to notify the Information Technology Support Teams.
SI-04 (23)	SYSTEM AND INFORMATION INTEGRITY	SI-4 (23)	INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES	The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined 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.	DATAMARK utilizes Sophos, WSUS, Barracuda and Solarwinds to protect and secure the data that is being processed and at rest. Alerts are configured to identify any abnormalities or potential threats on the network and are used to notify the Information Technology Support Teams.

SI-05	SYSTEM AND INFORMATION INTEGRITY	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2. References: NIST Special Publication 800-40.	DATAMARK utilizes Sophos, WSUS, Barracuda and Solarwinds to protect and secure the data that is being processed and at rest. Alerts are configured to identify any abnormalities or potential threats on the network and are used to notify the Information Technology Support Teams.
SI-06	SYSTEM AND INFORMATION INTEGRITY	SI-6	SECURITY FUNCTION VERIFICATION	The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative actions(s)]] when anomalies are discovered. Supplemental Guidance: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.	N/A	IF there is a failed attempt or lock out of system, the user needs to call the help desk to verify themselves to reset password and access only what is considered a business need.
SI-07	SYSTEM AND INFORMATION INTEGRITY	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information]. Supplemental Guidance: 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. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3. References: NIST Special Publications 800-147, 800-155.	Authorized changes are controlled by admin access that is only granted to business need and role.
SI-07 (01)	SYSTEM AND INFORMATION INTEGRITY	SI-7 (1)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS	The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization- defined frequency]]. 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.	System restarts and shutdown are initiated during security related events.
SI-07 (07)	SYSTEM AND INFORMATION INTEGRITY	SI-7 (7)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE	The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational 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. Related controls: IR-4, IR-5, SI-4.	Any unathorized change are tracked and kept in security incident folder, both logically and physically.
SI-08	SYSTEM AND INFORMATION INTEGRITY	SI-8	SPAM PROTECTION	The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3. References: NIST Special Publication 800-45.	DATAMARK utilizes spam filtering with Barracuda.
SI-08 (01)	SYSTEM AND INFORMATION INTEGRITY	SI-8 (1)	SPAM PROTECTION | CENTRAL MANAGEMENT	The organization centrally manages 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. Related controls: AU-3, SI-2, SI-7.	DATAMARK utilizes spam filtering with Barracuda which is managed centrally.
SI-08 (02)	SYSTEM AND INFORMATION INTEGRITY	SI-8 (2)	SPAM PROTECTION | AUTOMATIC UPDATES	The information system automatically updates spam protection mechanisms.	DATAMARK utilizes spam filtering with Barracuda which is managed centrally with automatic updates.
SI-10	SYSTEM AND INFORMATION INTEGRITY	SI-10	INFORMATION INPUT VALIDATION	The information system checks the validity of [Assignment: organization-defined information inputs]. Supplemental Guidance: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker- supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks. References: None.	Software Development team practices software quality assurance through code review to ensure secure coding practices to include OWASP Guidelines, PCI DSS and other application standards.

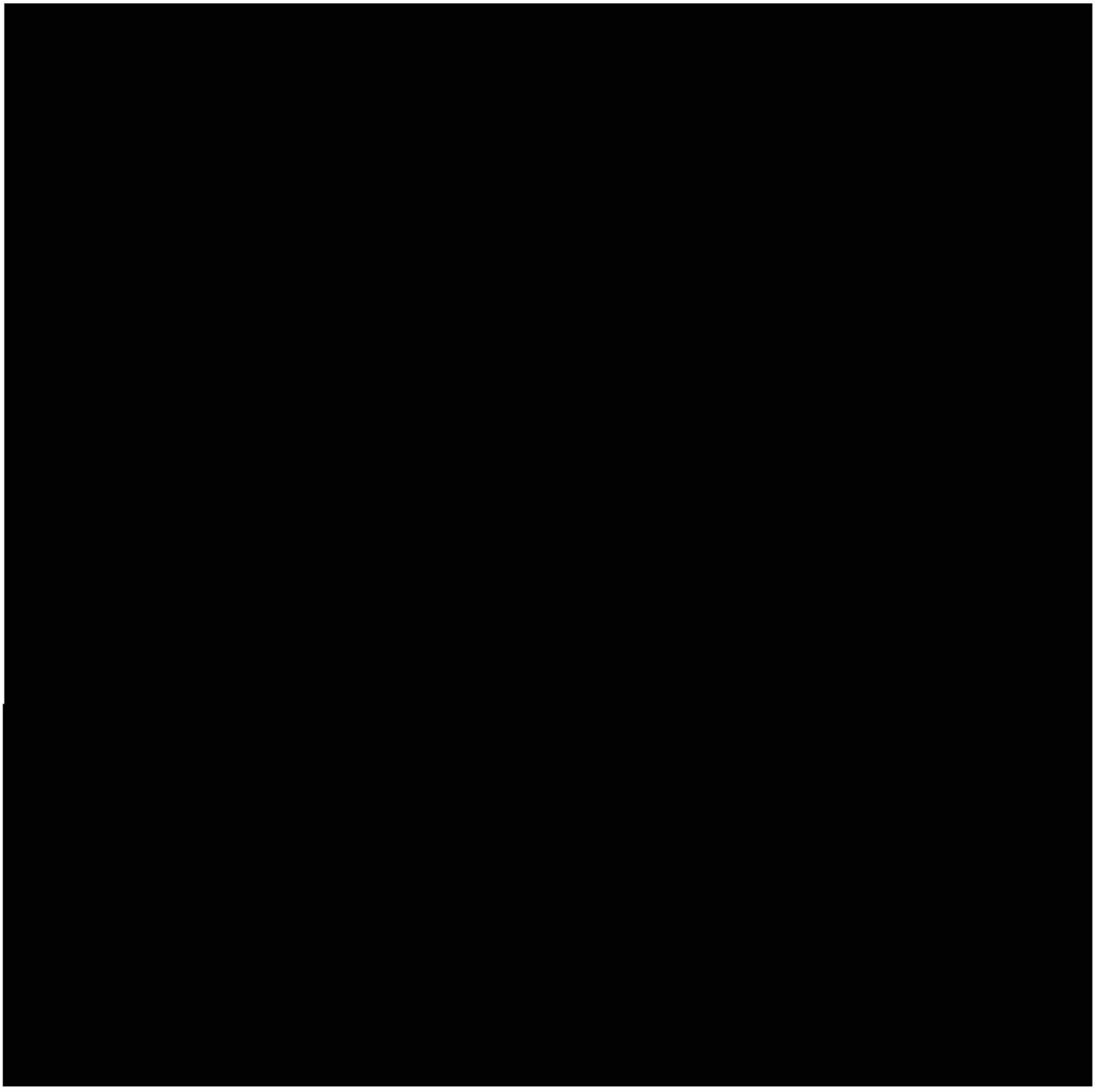
217

SI-11	SYSTEM AND INFORMATION INTEGRITY	SI-11	ERROR HANDLING	The information system a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/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. Related controls: AU-2, AU-3, SC-31. Control Enhancements: None. References: None.	The information systems are setup to generate error messages that do no reveal confidential or secret information.
SI-12	SYSTEM AND INFORMATION INTEGRITY	SI-12	INFORMATION HANDLING AND RETENTION	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4. Control Enhancements: None. References: None.	Standards also meet industry accepted standards such as SANS, NIST, and CIS
SI-16	SYSTEM AND INFORMATION INTEGRITY	SI-16	MEMORY PROTECTION	The information system implements [Assignment: organization-defined security safeguards] to protect its 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. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3. Control Enhancements: None. References: None.	Software Development team practices software quality assurance through code review to ensure secure coding practices to include OWASP Guidelines, PCI DSS and other application standards.

1 of 2

DATAMARK
INCORPORATED

Attachment 2 to SOW 3, ME17-076-003



Note: All PHEAA owned equipment will be replaced with vendor-owned equipment during the course of SOW3.

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

ML

DATAMARK
INCORPORATED

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

DATAMARK
INCORPORATED

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

2 of 2

DATAMARK
INCORPORATED

Network Diagram

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

1 of 1

DATAMARK
INCORPORATED

Attachment 4 to SOW 3, ME17-076-003

Process Flow

I. Receipt of Documents for Processing

a. USPS Mail:

i. Post Office Pickups:

1. 3:30 am – Federal Mail
2. 5:00 am – Commercial Mail

ii. Incoming Mail Counts:

1. Manual tray counts are taken each day by PO Box
2. Counts are entered upon receipt into DTS for tracking purposes.

iii. Accountable Mail:

1. Defined as mail that has a unique trackable barcode, to include Express mail and special service mail such as Certified Mail.
2. All certified envelopes will be out-sorted within 1 hour of receipt for prioritized processing.
3. Certified mail will be processed according to the diagram below.

iv. Undeliverable Mail:
    1. Defined as mail returned due to an invalid address or insufficient postage; identified by having a yellow label attached to the envelope that indicates return to sender or includes a forwarding address
    2. If a received item does not have a printed barcode, it shall be scanned and processed under a specific document type designation for undelivered un-barcoded mail.
    3. If a received item has a printed barcode, CONTRACTOR will:
        a. Scan the barcode
        b. Systematically call API of CLIENT system in order to determine next steps.
        c. If next steps require full capture of new address info, the new address info shall be captured and transmitted via API call to CLIENT system.

v. Mis-Directed Mail:
    1. Defined as mail sent to AES in error; will be delivered to Mail Services at the PHEAA Home Office at 11:00 a.m. each day.

vi. PHEAA Home Office Delivery: Delivered to Mail Services at the PHEAA Home Office at 11:00 am each day
    1. Defined as mail received at the DATAMARK facility that is to be delivered to PHEAA Headquarters.
    2. Mail addressed to FedLoan Servicing Management Staff
    3. Mail addressed to CEO Executive Management Staff
    4. Letters from the Office of the Attorney General, Members of Legislature, or Congress
    5. Collateral Mail: Defined as any correspondence containing an agreement to make payment to PHEAA, this could include promissory notes, addendums, etc.
    6. Envelopes with checks: sorted out and kept in their original envelope with all original corresponding documentation. Check envelopes will be delivered to Mail Services at the PHEAA Home Office at 11:00 am each day. A check log will be signed by a receiving agent in Mail Services to document the chain of custody of all checks.
    7. Envelopes with cash: Recorded to the cash log, kept in a locked cash bag, and delivered to Mail Services at the PHEAA Home Office at 11:00 am each day. The cash log must be signed by a receiving agent in Mail Services in order to verify the chain of custody of all cash.

b. Mail received from Mail Services:
    i. Credit Disputes:
        1. Picked up from Mail Services at the PHEAA Home Office each morning at 11:00 am

2. Provided keys are used to unlock the bags once the bags are back at the Contractor off-site processing facility
3. Manual counts are taken
4. Counts are entered by 12:30 pm into the Document Tracking System (DTS) for tracking purposes

ii. Accountable Mail:
1. Contractor will process each item into DTS according to the Accountable Mail process flow above.
2. PHEAA will received tracking info for each document via metadata received from Contractor.
3. PHEAA will have access to DTS repository in order to search for any accountable mail item by tracking number in order to retrieve its history.
4. Additional accountable mail received directly by Mail Services is picked up in the Mail Services area on the first floor each morning at 11:00 am.

c. Documents received from other PHEAA Business Unit employees:
i. Claims
1. Box(es) are dropped off by the Claims department to the Mail Services area before 11:00 am each morning
ii. Consolidations
1. Individual documents are dropped off by various people before 11:00 am to the Mail Services department
iii. Archive Work - Boxes dropped off periodically throughout the day/week to the Mail Services department
1. Defined as any correspondence received directly from PHEAA business units to be provided to DATAMARK for imaging.
2. GIR
3. Conversions
4. Other Archive

- Document Processing
  - CONTRACTOR shall provide services according to the following Process Flow diagram:

Mail Prepping

- If an item received contains an original legal document OR a request to return the documents included, CONTRACTOR shall:
  - Make a copy of the given document(s) in order to include in the prepped document for scanning.
  - Prep the given original/requested document in an envelope with a pre-formatted cover letter for outbound mail.
  - Count and track each outbound item for reporting and chargeback purposes.
- The envelope of each piece of mail shall be quality assured to ensure all correspondence was extracted. This step shall be performed within the specified time period provided by CLIENT.

- Mail Scanning
  - The received date for each document scanned shall be recorded for reporting purposes and must be applied clearly on the correspondence
  - Each document shall be imprinted with a unique document control number according to agreed format and location specifications.

MA

- The corresponding image for each document shall be annotated with the equivalent document control number according to agreed format and location specifications.
- All documents shall be rotated to be readable in an upright fashion.
- The front and back of all documents shall be imaged and blank pages shall be deleted.
- The number of pages per document shall be counted and logged for reporting and verification purposes.
- The envelope of each document received shall be imaged.

- Fax/Electronic Receipt
  - CONTRACTOR shall provide an Application Programming Interface (API) for CLIENT to transmit received faxes to.
  - Each fax shall be logged with the received date/time.
  - Each fax shall be annotated with a unique document control number according to agreed format and location specifications.
  - Where possible, a fax image will be enhanced in order to promote optimal Optical Character Recognition (OCR) processing.
  - All documents shall be rotated to be readable in an upright fashion.
  - Blank pages shall be deleted.
  - The number of pages per document shall be counted and logged for reporting and verification purposes.
- Data Capture
  - CONTRACTOR will leverage OCR in order to electronically recognize required data where possible.
  - Indexing shall be completed according to the requirements detailed in Attachment 5.
- Data formatting:
  - CONTRACTOR will consolidate the image and all captured data for a document into an agreed JSON format.
  - Additional metadata will be provided for each document as per the Technical Specifications in Attachment 6 – Indexing Requirements.
- Transmission
  - CLIENT shall provide an API for CONTRACTOR to transmit document images and data.
  - Documents shall be transmitted one-by-one as they are completed in real-time.
  - Upon receipt of each completed document, CLIENT shall run verification and integrity checks to ensure that document data is received as expected and shall provide an acknowledgment or reject response as appropriate.
  - CONTRACTOR shall log all successful acknowledgements for tracking and reporting purposes.
  - CONTRACTOR shall perform activities necessary to correct and resend any rejected documents.
- Document Storage, Retrieval and Destruction
  - After successful acknowledgement, electronic images and capture data for completed documents shall be deleted as per the security specifications

- After scanning, physical documents will be stored in barcoded boxes and logged for tracking and reporting purposes.
    - Promissory Notes that have reached their retention period shall be returned to CLIENT headquarters immediately after successful acknowledgement of electronic files.
- The system shall manage document retention and automatically mark individual documents for destruction or return, by document type, once the required retention period of thirty (30) days has elapsed.
- All other documents that have reached their retention period shall be destroyed.
- Destruction of documents shall be logged per item for comprehensive reconciliation and reporting.

- Reporting
    - Reporting will be provided by CONTRACTOR per Attachment 5.
    - Time Reporting System (TRS) time tracking will no longer be used.
    - The PHEAA QA module will no longer be used.

- Business Continuity
    - The CONTRACTOR shall provide a CONTRACTOR facility, which can be located anywhere within the US, as their designated cold BCP target location.
    - The CONTRACTOR shall provide Records Management operations at the DATAMARK target location within 72 hours of a declared disaster with possibility of 24 hour data loss.
    - The CONTRACTOR shall include the cost of business continuity services with the transactional pricing model.
    - The CONTRACTOR shall create a BCP plan which will define the scope of BCP services. The plan will be developed as part of SOW 3 project execution.
    - The CONTRACTOR BCP plan shall include the scope of required test cases to support determined disaster scenarios.
    - The CONTRACTOR shall execute an annual BCP drill utilizing the scope of required test cases.
    - The CONTRACTOR annual BCP drill testing shall not require mail rerouting by USPS to the designated BCP location.
    - The CONTRACTOR annual BCP drill shall require personnel with approved Federal clearances as participants at their BCP location.
    - The CONTRACTOR shall obtain approved Federal clearances for the scope of personnel who will be participants in the annual BCP drill. This activity will occur prior to execution of the drill tests.
    - The CONTRACTOR shall have the discretion to determine if any personnel located within the CONTRACTOR's Harrisburg location are required to co-locate to the BCP location for participation in the annual BCP drill.

- The CONTRACTOR BCP plan shall be formatted along the lines of the NIST disaster recovery / business recovery documentation.
- The CONTRACTOR BCP target location shall not require ATO certification. This meets current Client expectations previously established with their Sterling Forrest location.
- The CONTRACTOR shall define resource relocation requirements within their BCP plan
- The CONTRACTOR shall identify their BCP target location within their BCP plan
- The CONTRACTOR and CLIENT shall work collaboratively to define the new mail rerouting process which will be included within the BCP plan.
- The CLIENT shall keep CONTRACTOR aware of future changes in their overall disaster recovery strategy as CLIENT moves to a future cloud based infrastructure as a service. This may result in more rigid recovery time objectives. Changes required to the CONTRACTOR BCP plan will be addressed as part of the overall MSA change management process.

Attachment 5 to SOW 3, ME17-076-003

Reporting Requirements

Reporting scope must address two main reporting areas of need:

1. Records Management Operational Reporting
    - Reports consistent with what those provided today in PHEAAs as-is reporting system
2. Vendor Management Reporting
    - Reports required by PHEAA's vendor management and business operations to ensure SLAs documented within Appendix 8 are accurately reported.

High Level Goals for Reporting Success

1. Provide the required records management operational reporting using Contractor's future state reporting mechanism at the date of implementation of the DATAMARK integrated solution.
2. Provide vendor management reporting mechanism that ensures SLA metrics in Appendix 8 are accurately reported.
3. Ensure the future state reporting solution will support client's future state enterprise reporting approach.
4. Minimize the need for vendor activities with reporting governance by providing a governance approach that will allow the client to manage their reporting changes.

Records Management Operational Reporting

The following provides information on alignment of PHEAA's as-is reporting system with contractor's specific future state reporting system. Although formatting may be different between existing reports and new reports, data provided across the new reports will provide a reasonable facsimile of the data provided in the existing reports such that equivalent information can be derived.

PHEAA will be granted direct access to the Vendor Document Tracking System (DTS) Reporting portal in order to pull and review real-time reports as desired. The terms of this SOW will cover PHEAA's access; no additional click-through or browse-wrap terms will be imposed upon PHEAA portal users.

DTS immediately begins producing real time mailroom reports that will be available to PHEAA personnel on a secured Internet Web site during the initial mail receipt process. The reports are generated and continually updated in DTS as the documents move through each mailroom process. The reports generated from this initial Mail Receipt process detail the exact number of USPS units received. This establishes the starting point for the daily

incoming receipt report. This report, along with all reports from the Vendor shall be available via a secure, Internet site (online portal). The Vendor shall provide comprehensive data that:

- Maintains Receipt Date Integrity
- Tracks & Reconciles all incoming volume received by the Vendor

Report Name	Description
End of Day (EOD) Production Snapshot Start of Shift (SOS) Snapshot)	Online report that provides comprehensive pending volumes broken down by process and/or line of business, and therein by received date, indicating compliance to turn-around-time requirements
Records Management (RM) Workload – Conversions	Online Document Tracking System (DTS) report for "Volume by Document Type" filtered to provide the oldest received date for pending: • Conversions Archive work
RM Workload - Grants	Online DTS report for "Volume by Document Type" filtered to provide the oldest received date for pending: • Grants Correspondence • Grants Status Notices
RM Workload – FLS Workflow	Online DTS report for "Volume by Document Type/Source" filtered to provide the oldest received date and volumes for pending: • For FLS Correspondence • For FLS Faxes
RM Workload Status - PHEAA Loan Correspondence	Online DTS report for "Volume by Document Type" filtered to provide the oldest received date and volumes for pending: • PHEAA Loan Correspondence.
RM Workload – Treasury Adjustments	Online DTS report for "Volume by Document Type" filtered to provide the oldest received date and volumes for pending: • Federal Adjustments • Commercial Adjustments

RM Workload Status - Commercial Servicing & Guarantor Insurer Relations (GIR) (Archive)	Online DTS report for "Volume by Document Type" filtered to provide the oldest received date and volume for pending: • Loan Servicing • GIR • Graduate and Professional Services (GPS)
RM Workload Status - Archive Treasury Adjustments	Online DTS report for "Volume by Document Type" filtered to provide the oldest received date and volume for pending: • Commercial Adjustments • FLS Treasury Archive
Records Management Workload – Direct Loan Consolidation Origination (DLCO)	Online DTS report for "Volume by Document Type/Source" filtered to provide the oldest received date and volumes for pending: • DLCO Correspondence • DLCO Faxes
RM Workload – AES Servicing	Online DTS report for "Volume by Document Type" filtered to provide the oldest received date for pending • For AES Loan Servicing Correspondence: Provides the oldest received date of pending mail • For AES Servicing Faxes: Provides the pending volume for each pending received date
RM Workload – Undeliverable Mail	Online DTS report for "Volume by Source" filtered to provide the oldest received date for pending: • FLS Undeliverable Mail • Commercial Servicing (CS) Undeliverable Mail
RM Workload – Death, Disability, Bankruptcy (DDB) Processing	Online DTS report for "Volume by Source" filtered for: • DDB Processing • DDB Error Log
RM Workload – Credit Disputes	Online DTS report for "Volume by Source" filtered to provide the oldest received date for pending: • Commercial Credit Disputes • Federal Credit Disputes • PHEAA Credit Disputes
Incoming Mail Report	Online DTS report for "Volume by Source" filtered to provide the oldest received date and volumes for pending

	• FLS Servicing (PO Box 69184) • FLS Undeliverable (PO Box 69184) • AES Servicing (PO Box 2461) • AES Undeliverable Mail (PO Box 2461) • PHEAA Credit Disputes (PO Box 61017) • PHEAA (PO Box 8147) • Grants (PO Box 8157) • DDB (PO Box 8183) • AES Network Consolidation (PO Box 8139) • AES Credit Disputes (PO Box 61047) • FLS Credit Disputes (PO Box 60610) • FLS Direct Debits (PO Box 3661) • FLS DLCO (PO Box 69186)
Return to Business Unit (RTB)	Online DTS report provided to track and list all physical DDB documents returned to PHEAA per defined business rules.

Vendor Management Reporting

- PHEAA may create, and DATAMARK, subject to the MSA's change provision, may be required to contribute to, additional Vendor Management Reports for the verification of SLA metrics.

Go Live

Upon the date of implementation of the DATAMARK integrated solution, Contractor will implement the reports listed above in the "Records Management Operational Reporting" section, as well as the all standard reports available from the Contractor "Document Tracking System" (DTS), as part of their web based reporting solution.

•

DATAMARK
INCORPORATED

Attachment 6 to SOW 3, ME17-076-003

INDEXING REQUIREMENTS

Basic Indexing Fields

All documents categorized as 'Basic Indexing' for transactional pricing purposes will have at a minimum the 'Document Type' indexing attribute classified by the CONTRACTOR. Additionally, CONTRACTOR will be required to classify additional attributes from the below table based upon the specific document type, with the total indexing attributes provided not to exceed fifteen for each document.

Index Field	Description/Notes	Example
documentType*	• Unique document type/description • **Required for all document types**	'UnemploymentDeferment'
ssn	• Social Security Number available on the document • Will be passed from PHEAA to DATAMARK for outbound electronic documents if documentSource = 'EXTUPLOAD' or 'LAN'	'123456789'
accountNumber	• Account Number available on the document • May be passed from PHEAA to DATAMARK for some electronic document types.	'1234567890'
oeCode	• Federal school code (OE Code) available on the document.	'00123456'
einCode	• Employer Identification Number code available on the document. • Applicable to Grants document types	'999999999','999999999-001'
lenderCode	• Lender code available on the document	'000111'
guarantorCode	• Guarantor code available on the document • Applicable to DDB documents	'0001234'
academicYear	• Academic Year available on the document.	'2018', 'S18'

Index Field	Description/Notes	Example
	• Applicable to Grants document types	
majorBatch	• Major batch code available on the document • Applicable to Conversions document types	'ABCD04152019'
minorBatch	• Minor batch code available on the document • Applicable to Conversions document types.	'12345'
mrdfBarCode	• Mail Run Data File (MRDF) barcode that may be available on the document • Scanned in order to determine business logic/processing for all returned mail.	'99991234567890'

Additional Metadata

In addition to the 'Basic Indexing' fields to be provided by the CONTRACTOR based on the Document Type, CLIENT and/or CONTRACTOR will provide additional metadata indexing related to the intake of each document.

Field	Description/Notes	Example
dateReceived	• Date the document was received by DATAMARK • **Required for all document types** • Must be valid date/time format	"2018-10-01T08:30:00.5555"
scanDate	• Date the document was scanned by DATAMARK • **Required for all document types** • Must be valid date/time format.	"2018-10-01T09:15:30.4444"
Dcn	• 17 digit Document Control Number assigned by PHEAA to each outbound electronic document. • Required if documentOriginator = 'PHEAA' • Must be 17 numeric digits	'99918278053657429'
documentSource	• Intake channel via which the document was receive (mail/paper, fax,	'FAX', 'SCAN,

DATAMARK
INCORPORATED

	upload, PHEAA LAN) • **Required for all document types.**	'EXTUPLOAD', 'LAN'
documentOriginator	• Originator of the document (PHEAA or DATAMARK) • **Required for all document types**	'PHEAA' or 'DMI'
documentInput	• PO Box (for paper documents), fax number (for faxed documents) or upload channel (for web/mobile upload documents) via which the document was received. • PHEAA will provide this value to DATAMARK for all outbound electronic documents sent for scanning/indexing. • DATAMARK will assign value for all scanned paper documents. • **Required for all document types.**	'61047'
ocaSource	• Intake channel for OCA documents • Required for OCA correspondence only	'MAIL'
Icn	• Unique document identifier assigned by DATAMARK to all documents. • **Required for all document types.**	'00018278053657429'
correspondenceGroupID	• Unique group identifier assigned to all paper and electronic documents processed by DATAMARK. • Documents received together and split by DATAMARK for scanning and indexing purposes will all be assigned the same correspondenceGroupID. • **Required for all document types**	'067e6162'
customerContactID	• Unique customer contact identifier assigned by PHEAA to all outbound electronic documents. • Required for all document types where documentOriginator = 'PHEAA'	'12345'
certifiedMailTrackingNumber	• Certified mail tracking number provided by the Certified Mail Carrier. • Required for all paper documents received via certiifed mail delivery.	'11111-11111-11111-11111-AB'
certifiedMailCarrier	• Certified mail carrier that delivered the document.	'USPS', 'UPS', 'FEDEX'

	• Required for all paper documents received via Certified mail delivery.	
certifiedMailReceiptDate	• Date/time certified mail was received by DMI • Required for all paper documents received via Certified Mail delivery	"2018-10-01T09:15:30.4444"
mimeType	• Mime type of the document • Required if documentOriginator = 'DMI' • Required if imageContent provided and documentOriginator != 'DMI'	'application/pdf'
imageContent	• Content of the image in base64 encoded format • Required if documentOriginator = 'DMI'	[base64 encoded file]
dataCaptureType	• Category of data capture performed on the document	

Basic Indexing/Metadata Field Specifications

Field	Datatype	Allow Null from DMI	Validations/Rules/Comments
documentType	String	No	Required for all document types
Ssn	String	Yes	Capture if available based on document type
accountNumber	String	Yes	Capture if available based on document type
oeCode	String	Yes	Capture if available based on document type
pheaaCode	String	Yes	Grants documents
einCode	String	Yes	Grants documents
lenderCode	String	Yes	DDB documents
guarantorCode	String	Yes	DDB documents
majorBatch	String	Yes	Conversions documents
minorBatch	String	Yes	Conversions documents
academicYear	String	Yes	Grants documents
mrdfBarCode	String	Yes	Required to be scanned if present on undelivered mail
dcn	String	Yes	17 digit numeric; will be required if documentOriginator = 'PHEAA'
dateReceived	Date	No	Required for all document types; Must be valid date/time format; No future

			date allowed;
scanDate	Date	No	Required for all document types; Must be valid date/time format; No future date allowed;
correspondenceGroupID	String	No	Required for all document types
customerContactID	String	Yes	Required if documentOriginator = 'PHEAA'
documentSource	String	No	Required for all document types; assign based on intake channel ('SCAN', 'FAX', 'EXTUPLOAD', or 'LAN')
documentOriginator	String	No	Required; must = 'PHEAA' or 'DMI'
documentInput	String	No	Required for all document types
ocaSource	String	Yes	Required for OCA correspondence
icn	String	No	Required for all document types
mimeType	String	Yes	Required if documentOriginator ='DMI'; Required if imageContent provided and documentOriginator != 'DMI'
imageContent	String	Yes	Required if documentOriginator = 'DMI'; binary encoded
certifiedMailTrackingNumber	String	Yes	Required for all document types received via certified mail delivery
certifiedMailCarrier	String	Yes	Required for all document types received via certified mail delivery
certifiedMailReceiptDate	Date	Yes	Required for all document types received via certified mail delivery

DATAMARK
INCORPORATED

Attachment 7 to SOW 3, ME17-076-003

ELECTRONIC DOCUMENTS REQUIREMENTS

The transfer of data shall be accomplished by the CONTRACTOR utilizing mutually agreed upon telecommunication circuits using PHEAA-approved security protocols to ensure confidentiality of the information being transmitted. The CONTRACTOR shall be responsible for providing redundancy of servers, LANs and internal connectivity to ensure timely creation, transfer and execution of files. Additional security requirements are outlined in Attachment 1 – Security Requirements.

Transmission of basic indexing data, full data capture, document images, and other related data will be sent to the CLIENT data processing center as soon as it is completed by the CONTRACTOR. A Handshake Process will be established for the transmission process wherein each file successfully received by CLIENT will result in an acknowledgement confirming successful transmission of the file. Any file that is not successfully received by the CLIENT will result in a rejection acknowledgement and the document will not be accepted by the CLIENT or its systems. In the event the data output does not conform to CLIENT specifications, the CONTRACTOR will be required to recreate and transmit files within original TAT.

The CONTRACTOR shall maintain the electronic data backups of all data and images processed as per Attachment 1 – Security Requirements.

- Electronic Documents
  - Documents that are received by the CLIENT from its customers are transmitted to the CONTRACTOR for classification and/or data capture.
  - Any attributes associated with images sent from PHEAA to DATAMARK will be returned to PHEAA with the data extracted/captured from that image by DATAMARK. .
  - See Data Formatting section for minimum attributes to be transmitted with the document.

- Data Capture
  - CONTRACTOR will leverage OCR in order to electronically recognize required data where possible.
  - Basic Indexing: Data will be captured as specified in Attachment 6 – Indexing Requirements under section – "Basic Indexing Fields".
  - Metadata Indexing: System level metadata will be captured as specified in Attachment 6 – Indexing Requirements under section – "Metadata Indexing".
  - Full Data Capture: For agreed document types, additional capture will be performed as per the specification that will be detailed for each document or group of documents that will be migrated to CONTRACTOR.

7 of 7

- Any updates or revisions to captured data will follow the established Change Control process.

- Data Formatting
  - The electronic images will be captured at a resolution of "at least" 200 dpi, bi-tonal.
  - The electronic image data format will be TIFF Multipage CCITT Group 4
  - Data that will be transmitted from CLIENT to CONTRACTOR will include:
    - The document image
    - Data attributes to be defined in follow-up requirements, with specifications regarding required/optional and data types.
  - Data that will be transmitted from CONTRACTOR to CLIENT will include:
    - The document image
    - Data attributes, from Attachment 6 – Indexing Requirements, to be defined in follow-up requirements, with specifications regarding required/optional and data types.
  - Split multiple embedded documents, by documentType classifications
    - Assign a unique icn to each split document
    - Assign a common documentGroupID
  - Copy documents that match multiple documentType classifications
    - Assign a unique icn to each copied document
    - Assign a common documentGroupID
  - Transmit all the data received from CLIENT for each document along with all the other attributes that would be returned as part of document classification and data capture.

- Transmission
  - CLIENT shall provide an API for CONTRACTOR to transmit document images and data.
  - CONTRACTOR shall provide an API for CLIENT to transmit document images and data.
  - CLIENT shall provide an API for CONTRACTOR to determine processing for returned mail.
  - Documents shall be transmitted one-by-one as they are completed in real-time.
  - Upon receipt of each completed document, CLIENT shall run verification and integrity checks to ensure that document data is received as expected and shall provide an acknowledgment or reject response as appropriate.
  - CONTRACTOR shall log all successful acknowledgements and unsuccessful attempts for tracking and reporting purposes.
  - CONTRACTOR shall perform activities necessary to correct and resend any rejected documents.

MR

- System Integration
  - CLIENT and CONTRACTOR services will be REST API services with JSON data encoding.
  - The JSON object specification for document specific data will be defined jointly for each document or group of documents that will be migrated to CONTRACTOR.
  - Images will be encoded using base64 encoding within JSON
  - API service endpoints may be separated by line of business, such that Federal and Non-Federal data shall be transmitted via separate API endpoints. This may be specified in follow-up requirements.
  - CLIENT and CONTRACTOR services will have a health monitoring endpoint that allows the determination of whether the service is offline for maintenance or an outage.
    - In the case of maintenance and unexpected outages, it will be the responsibility of the service client to suspend and then retry submission when the outage ends.

DATAMARK
INCORPORATED

Attachment 8 to SOW 3, ME17-076-003

Service Level Agreements

CONTRACTOR and CLIENT agree that the CONTRACTOR will track, monitor and report on the following Performance Criteria to CLIENT, at the specified intervals, to keep CLIENT informed of performance progress. CONTRACTOR understands and agrees that **time is of the essence** in meeting the Deliverable date(s), timelines, and SLAs set forth in this SOW, and will provide CLIENT with periodic updates.

Service Level Agreements and Credits/Incentives

The following are Service Level Agreements and Credits to the SOW 3. If Contractor fails to comply with the Performance Requirement for each Performance Metric, Contractor shall provide Client with the Service Level Credit against the next invoice as set forth in the chart below:

	Performance Metric	**Goal**	***Performance Requirements***	***Calculation***	**Frequency of Review**	**Service Level Credits (Applicable to all Service Level Agreements)**	**Incentives (Applicable to all Service Level Agreements)**
1	All correspondence for Commercial Servicing (Workflow) is processed within defined	Varies (See SLA chart)	100%	Defined by hours, the due date/time shall be measured from the date/time received by calculating	A weekly review will be performed to monitor the prior week's activities and ensure	Individual SLA achievement levels will be calculated monthly as a percentage. Percentages will be averaged. If Monthly average of all SLA achievement levels is below 94%, the following Service	Individual SLA achievement levels will be calculated monthly as a percentage. Percentages will be averaged. If Monthly average of all SLA achievement levels exceeds 96%, a Service Level Incentive will apply: 99.1% - 100% [redacted]

DATAMARK
INCORPORATED

	Performance Metric	Goal	*Performance Requirements*	*Calculation*	Frequency of Review	Service Level Credits (Applicable to all Service Level Agreements)	Incentives (Applicable to all Service Level Agreements)
	SLAs			the equivalent number of hours forward from the date/time of receipt based on relevant work type, Receipt Time, and SLAs listed in Table 1.	SLAs were met for the prior week.	Level Credit will apply: 93%-93.9% -1.25% 92%-92.9% -2.50% 91%-91.9% -3.75% 90%-90.9% -5.0%	98.1% - 99.0% [redacted] 97.1% - 98% 96.1% - 97%
2	All correspondence for FedLoan Servicing (Workflow) Business	Varies (See SLA chart)	100%	If defined by hours, the due date/time shall be measured from the date/time	A weekly review will be performed to monitor the prior week's		

27

	Performance Metric	Goal	*Performance Requirements*	*Calculation*	Frequency of Review	Service Level Credits (Applicable to all Service Level Agreements)	Incentives (Applicable to all Service Level Agreements)
	Line is processed within defined SLAs			received by calculating the equivalent number of hours forward from the date/time of receipt based on relevant work type, Receipt Time, and SLAs listed in Table 1.	activities and ensure SLAs were met for the prior week.		
3	All correspondence for Public Service	Varies (See SLA chart)	100%	If defined by hours, the due date/time shall be measured	A weekly review will be performed to monitor		

	Performance Metric	Goal	*Performance Requirements*	*Calculation*	Frequency of Review	Service Level Credits (Applicable to all Service Level Agreements)	Incentives (Applicable to all Service Level Agreements)
	(Workflow) is processed within defined SLAs			from the date/time received by calculating the equivalent number of hours forward from the date/time of receipt based on relevant work type, Receipt Time, and SLAs listed in Table 1.	the prior week's activities and ensure SLAs were met for the prior week.		
4	All correspondence for	Varies (See SLA chart)	100%	If defined by hours, the due date/time	A weekly review will be		

	Performance Metric	Goal	*Performance Requirements*	*Calculation*	Frequency of Review	Service Level Credits (Applicable to all Service Level Agreements)	Incentives (Applicable to all Service Level Agreements)
	PHEAA Loan Asset Management is processed within defined SLAs			shall be measured from the date/time received by calculating the equivalent number of hours forward from the date/time of receipt based on relevant work type, Receipt Time, and SLAs listed in Table 1.	performed to monitor the prior week's activities and ensure SLAs were met for the prior week.		
5	All back-end	Varies	100%	Defined by	A weekly		

2nd

	Performance Metric	Goal	*Performance Requirements*	*Calculation*	Frequency of Review	Service Level Credits (Applicable to all Service Level Agreements)	Incentives (Applicable to all Service Level Agreements)
	(Archive) documents are imaged timely as defined within SLAs	(See SLA chart)		days, the due date/time shall be measured from the date/time received by calculating the equivalent number of days forward from the time of receipt. Receipt Time and SLAs listed in Table 1.	review will be performed to monitor the prior week's activities and ensure SLAs were met for the prior week.		
6	All Undeliverable mail is	Varies (See SLA chart)	100%	Defined by days, the due date/time	A weekly review will be		

2n2

	Performance Metric	Goal	*Performance Requirements*	*Calculation*	Frequency of Review	Service Level Credits (Applicable to all Service Level Agreements)	Incentives (Applicable to all Service Level Agreements)
	addressed within defined SLAs			shall be measured from the date/time received by calculating the equivalent number of days forward from the time of receipt. Receipt Time and SLAs listed in Table 1	performed to monitor the prior week's activities and ensure SLAs were met for the prior week.		
7	All Specialized documents and processes are	Varies (See SLA chart)	100%	Defined by days, the due date/time shall be measured	A weekly review will be performed to monitor		

2n1

	Performance Metric	Goal	*Performance Requirements*	*Calculation*	Frequency of Review	Service Level Credits (Applicable to all Service Level Agreements)	Incentives (Applicable to all Service Level Agreements)
	addressed and completed within defined SLAs			from the date/time received by calculating the equivalent number of days forward from the time of receipt. Receipt Time and SLAs listed in Table 1	the prior week's activities and ensure SLAs were met for the prior week.		

1. Service Level Credits/Incentives shall not exceed 5% of invoice amount in any one month.
2. All Service Levels listed are based on received volumes within the volumes detailed in Table 2 and Table 3. Should volumes exceed the expected volumes by more than 10% on a monthly average, Contractor and Client will negotiate Service Level Credits; Service Level Credits

JM2

will continue to apply. Should volumes decrease by more than 10% on a monthly average, Service Level Incentives will be negotiated and agreed upon by both parties; Service Level Credits will continue to apply.

Table 1 – Service Levels

Contractor shall comply with the following SLAs:

Work Type	Receipt Method	Receipt Time	SLA
AES Commercial Servicing (Workflow)			
Commercial Servicing (PO Box 2461)	USPS Pickup	5:30 am	1 day
Graduate Services (PO Box 2461)	USPS Pickup	5:30 am	1 day
Loan Origination (PO Box 2465)	USPS Pickup	5:30 am	1 day
Network Consolidation (PO Box 2165)	USPS Pickup	5:30 am	1 day
Commercial Adjustments (PO Box 8139)	PHEAA Home Office Pickup	7:30 am	1 day
Guarantor Insurer Relations DDB (PO Box 8183)	PHEAA Home Office Pickup	7:30 am	1 day
Commercial Servicing Faxes	Electronic	Date Stamp	1 day
Loan Origination Faxes	Electronic	Date Stamp	1 day
AES Credit Disputes	PHEAA Home Office Pickup	7:30 am	1 day
FedLoan Servicing (Workflow)			
FedLoan Servicing Correspondence (PO Box 69184)	USPS Pickup	3:30 am	1 day

2 of 2

DATAMARK
INCORPORATED

Federal Adjustments (PO Box 3661)	PHEAA Home Office Pickup	7:30 am	1 day
FedLoan Servicing DDB	USPS Pickup	3:30 am	1 day
FedLoan Servicing Faxes	Electronic	Date Stamp	1 day
FedLoan Servicing Credit Disputes (PO Box 60610)	PHEAA Home Office Pickup	7:30 am	1 day
Direct Lending Consolidation (PO Box 69186)	USPS Pickup	3:30 am	1 day
Public Service (Workflow)			
Grant Status Forms (PO Box 8157)	USPS Pickup	3:30 am	6 hours
Grant Correspondence	USPS Pickup	3:30 am	6 hours
Grant Faxes	Electronic	Date Stamp	1 day
PHEAA Loan Asset Management			
PHEAA Loan Asset Mgmt Corr (PO Box 8147)	USPS Pickup	5:30 am	1 day
PHEAA DDB Correspondence	USPS Pickup	3:30 am	1 day
PHEAA Credit Disputes (PO Box 61017)	PHEAA Home Office Pickup	7:30 am	1 day

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

DATAMARK
INCORPORATED

AES Commercial Servicing (Archive)			
Commercial Servicing	PHEAA Home Office Pickup	11:00 am	7 days
Graduate Services	PHEAA Home Office Pickup	11:00 am	7 days
Guarantor Insurer Relations	PHEAA Home Office Pickup	11:00 am	7 days
Conversions	PHEAA Home Office Pickup	11:00 am	15 days
Loan Originations	PHEAA Home Office Pickup	11:00 am	15 days
Network Consolidation	PHEAA Home Office Pickup	11:00 am	15 days
Commercial Adjustments	PHEAA Home Office Pickup	11:00 am	15 days
FedLoan Servicing (Archive)			
FedLoan Servicing Correspondence	PHEAA Home Office Pickup	11:00 am	7 days
FedLoan Servicing DDB	PHEAA Home Office Pickup	11:00 am	7 days
FedLoan Servicing Conversions	PHEAA Home Office Pickup	11:00 am	10 days
Direct Lending Consolidation	PHEAA Home Office Pickup	11:00 am	15 days
Public Service (Archive)			
Grant Correspondence	PHEAA Home Office Pickup	11:00 am	3 days

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

MZ

DATAMARK
INCORPORATED

Undeliverable			
Commercial Servicing Undeliverable Mail	USPS Pickup	5:30 am	3 days
FedLoan Servicing Undeliverable Mail	USPS Pickup	3:30 am	3 days
PHEAA Undeliverable Mail	PHEAA Home Office Pickup	7:30 am	3 days
Specialized			
Claims	PHEAA Home Office Pickup	11:00 am	4 hours
Certified (all)	PHEAA Home Office Pickup	11:00 am	same day
DDB Faxes	Electronic	Date Stamp	1 days

123 W. Mills Avenue, Suite 400, El Paso, TX 79901 USA
1-877-667-2151
www.DATAMARK.net

DATAMARK
INCORPORATED

Volumes

The volumes set forth below in Tables 2 and 3 are estimates based on Client's historical data. Volumes are consistent on average throughout the year, with Mondays being significantly higher in volume than any other day of the week. Client makes no representations or warranties that Contractor will experience the same volumes.

Table 2 – Paper Volumes

Work Type	Average Weekly Volume	Average Monday Volume
Workflow		
Commercial Servicing	2,400 documents	850 documents
AES Credit Disputes	100 documents	30 documents
Loan Asset Management	850 documents	250 documents
PHEAA Credit Disputes	6 documents	
Grants	2,500 documents	850 documents
AES – Loan Consolidation	6 documents	
FedLoan Servicing	17,000 documents	7,000 documents
FLS – Direct Lending Consolidation	1,500 documents	300 documents
DDB	8,500 documents	3,500 documents
AES and FLS Receipt Ops – Direct Debits	550 documents	200 documents
FLS Credit Disputes	4,200 documents	1,800 documents

MJ

DATAMARK
INCORPORATED

Undeliverable Mail	40 trays	
Archive		
Commercial Servicing	16 documents	
DDB	2,500 documents	
Receipt Operations	200 documents	
Loan Asset Management	5 documents	
Grants	600 documents	
AES – Loan Consolidation	1 document	
AES – Conversions	6,000 documents	
FedLoan Servicing	3 documents	
FLS – Direct Lending Consolidation	80 documents	
FLS – Conversions	30 documents	

2 of 2

DATAMARK
INCORPORATED

Table 3 – Fax Volumes

The average volume per business day for faxes (includes weekends and holidays for Mondays or days after holidays).

Work Type	Avg. Volume
FedLoan Servicing	4,500 / day
Commercial Servicing	450 / day
Loan Origination	1-2 / day
Loan Asset Management	60 / day
Grants	95 / day

Non-Scannable Return Mail TAT

The CONTRACTOR shall return non-scannable mail (i.e. mail not included in the scope of work for processing under this or any subsequent SOW) received in mailroom to CLIENT by noon within 1 business day of receipt. TAT will be measured in accordance with the day on which the non-scannable mail is shipped to CLIENT. Mail will be dropped off and picked at PHEAA Headquarters via a daily mail run.

Non-scannable mail shall be handled in accordance with the security requirements and shall be treated as Confidential Information.

Application Server Availability

CONTRACTOR will maintain an Application Server guaranteed availability of 99% during business hours for any monthly billing period. Business hours are defined as Monday through Friday, 3:00 AM - 1:00 AM EST, excluding CLIENT-observed holidays.

2nd

DATAMARK
INCORPORATED

Website Availability

CONTRACTOR will maintain website guaranteed availability of 99.5% during business hours for any monthly billing period. Business hours are defined as Monday through Friday, 7:30 AM – 5:00PM EST, excluding CLIENT-observed holidays.

Disaster Recovery (DR)

The CONTRACTOR shall conduct a successful Disaster Recover test annually in conjunction with CLIENT and will document the results. Disaster Recovery testing will be scheduled to take place at least annually to ensure the Disaster Recovery site is ready.

Organization Management/Problem Notification

If SLA targets are not being attained, and/or at CLIENT's request, the CONTRACTOR will provide additional management resources to support operations. CONTRACTOR will notify the CLIENT Vendor Manager immediately by telephone and via e-mail including but not limited to any of the following conditions:

- Mail is received in poor condition and cannot be scanned or data keyed
- Unscanned documents are located which have exceeded expected TAT
- Mail is not received or delayed due to weather conditions, or mail carrier mis-routing
- CONTRACTOR experiences software, hardware, telecommunication or power problems impacting transmission, web reporting, turnaround time or data quality
- CONTRACTOR modifies any aspect of their established production workflow in the course of normal business operations or due to emergency/disaster recovery conditions

Quality Control and Audit Process

CLIENT will assess CONTRACTOR performance via a random selection of documents using the Internal Control Number (ICN) assigned to each document. Field, image, and transmission discrepancies identified during document processing or technical issues will be tracked and included in the overall results to be tabulated weekly and summed monthly for field and document accuracy. In order for Service Level Incentives to be assessed Quality standards must be met.

MJ

DATAMARK
INCORPORATED

Field Accuracy – Non-Critical Field Level Requirement: 99.5% and Critical Field Level Accuracy is 99.9%

Field Accuracy is defined as the data captured from the documents that are an actual representation of the data contained on the paper form or the electronic channel image. Image quality is assessed based on the resolution/alignment of the document. Documents identified as being blurred, folded, or overlapped will be tracked. Critical fields are the social security number and account number located on the document; all other fields will be considered non-critical fields.

Error(s) are charged per field for inaccurate, incomplete, or missing data as a result of the data entry or prep/scan/image process. The accuracy result is calculated in this manner:

$$\frac{\text{[Total number of fields audited] – [Number of fields in error]}}{\text{Total number of fields audited}}$$

Audit Sample

The audit sample will be based on product and CONTRACTOR population size for products imaged and data captured. The population size for a monthly reporting period will be selected for a precision of not less than +/- 2% or 400-500 audits per month. A random generated report can be utilized to provide the daily audit sample. The data keyed will be compared to the imaged product and the raw data transmitted daily by the CONTRACTOR to the CLIENT System.

Field Accuracy and Image Quality Audit Process

Audits performed are based on the audit methodology for each field that requires data capture, as well as document attributes and source type. Each field is audited for data accuracy and adherence to capture guidelines provided by CLIENT. Additionally, any additional information that is required based on business specifications as related to CONTRACTOR is audited. All discrepancies are noted and counted as an error.

DATAMARK
INCORPORATED

Audit Rebuttal and Remediation Process

A monthly report will summarize all audit activity and audit findings to the CONTRACTOR in order to provide the CONTRACTOR with an opportunity to review and research the cause of noted discrepancies. Subsequently, researched discrepancies reported to CLIENT, which are found to be unrelated to the CONTRACTOR process, will be removed from the audit summary, with the accuracy results adjusted accordingly. Discrepancies reported to the CONTRACTOR deemed valid will require subsequent remediation and corrective actions which will be outlined and provided to the CLIENT. Depending on severity and frequency of CONTRACTOR errors could result in additional remediation to be implemented depending on impact to CLIENT.

In support of the CONTRACTOR rebuttal process, the CONTRACTOR will be responsible for reviewing all information reported on the CONTRACTOR rebuttal worksheet provided by CLIENT. The CONTRACTOR must submit to CLIENT by the agreed upon weekly delivery date/time all errors which are being rebutted. If the CONTRACTOR fails to report rebutted errors by the agreed upon date/time, the errors will remain.

MJ

DATAMARK
INCORPORATED

Attachment 9 to SOW 3, ME17-076-003

Pricing and Fees

A. Transactional Pricing:
The transactional pricing below provides optimal pricing for the scope of Mailroom Services requested by PHEAA. All previously identified assumptions remain in place and the following additional assumptions apply:

- All paper documents received via incoming mail or for Archive_GIR, Archive_Conversions, or Archive_Other will be scanned.
- All paper documents for scanning are assumed to be an average of five (5) pages per document.
- All paper documents for scanning will be stored for a designated retention period and then securely shredded.
- Electronic documents will be received via Fax and Doc_Upload.
- PSLF and IDR mail documents only will be fully data captured per agreed capture elements.
- All other documents, including DDB, Proof of Income, and Borrower Correspondence documents, as well as all PSLF and IDR documents received via Fax and/or Doc_Upload shall only have their Document Category and Social Security Number (SSN) captured, if present.
- For all Doc_Category/SSN capture documents, if the SSN is not present, the document image will be returned to PHEAA with only the Doc_Category in order to be further processed directly by PHEAA in subsequent work queues in their system.
- One (1) Delivery per Day is included in overall transactional pricing at no additional cost. Any additional deliveries or pickups required by PHEAA will be at the below Price per Delivery.

Mailroom Function	Price	Unit
Mail Handling (all document types)		Per Document
Electronic Receipt (Fax + Doc Upload)		Per Document
Returns (pull and mail delivery)		Per Document
Delivery back to home office		Per Delivery
Scan		Per Page
Storage and Destruction		Per Page
Accountable Mail		Per Document
Undeliverable		Per Document
Archive - GIR		Per Document
Archive - Conversions		Per Document
Archive - Other		Per Document
Data Capture - PSLF		Per Document
Data Capture - IDR		Per Document
Data Capture - All Other (SSN and Category Only)		Per Document

2nd

DATAMARK
INCORPORATED

B. Rate Card

The below Hourly Rates table is established for certain SOW#3 services, and other special services, where approved, as indicated. DATAMARK will evaluate the Level of Effort (LOE) of each individual request and the hours will be multiplied by the rates below to determine overall cost for a project or Change Request.

Service	Hourly Rate
Software Development/Programming	[redacted]
Testing & Validation	
Information Technology Services	
Business Engineering Services	
Special Projects - Data Handling	