Homeland Security

DHS Policy Directive 4300A, "Information Technology System Security Program, Sensitive Systems"

Attachment S

Compliance Framework for Privacy Sensitive Systems

Version 1.0

April 28, 2022

Protecting the Information that Secures the Homeland

Document Change History

Version	Date	Description
1.0	April 28th , 2022	Initial release updated processes, and authorities - Riley Dean Associate Director Privacy Department, DHS HQ.

Table of Contents

This page intentionally blank

1.0 INTRODUCTION

In 2006, the Office of Management and Budget (OMB) issued guidance in Memorandum M-06-16, "Protection of Sensitive Agency Information." In 2016, OMB revised Circular A-130, "Managing Information as a Strategic Resource," to reflect changes in law and advances in technology. M-06-16 was later rescinded, but the privacy best practices, guidance, and requirements were passed through to Circular A-130. In order to implement the checklist provided by OMB, the Privacy Office, in coordination with the Office of the Chief Information Security Officer (OCISO), established the below requirements for protection of Privacy Sensitive Systems.[2]

1. Confirm that the system maintains, uses, or discloses Personally Identifiable Information (PII) and so is a Privacy Sensitive System and that the system and the PII can be accessed remotely or physically.
2. Identify protection needs.
3. Identify and verify organizational policies.
4. Implement protections for PII being transported or stored offsite.
5. Implement protections for remote access to systems containing PII; and
6. Plans of Action and Milestones (POA&M), Exceptions and Waivers for Key Privacy Controls.

Each of these requirements is described in Section 3.0 below.

2.0 SCOPE

These controls for Privacy Sensitive Systems apply to all DHS Components and DHS Headquarters, and to any company, consultant, partner, or Government agency that is performing a federal function on behalf of DHS.

[2] A Privacy Sensitive System is any system that contains Personally Identifiable Information (PII).

3.0 COMPLIANCE ACTIVITIES

3.1 Compliance Activity #1 – Confirm that the system maintains, uses, or discloses personally Identifiable Information (PII) and so is a Privacy Sensitive System, and that the system and the PII can be accessed remotely or physically.

The DHS Chief Privacy Officer is responsible for designating systems as Privacy Sensitive Systems in the DHS Trusted Agent FISMA[4] (TAF) Inventory. The purpose of Compliance Activity #1 is to:

- Identify systems containing PII
- Verify the categorization of that information
- Determine whether a system permits remote access, and whether PII on the system can be transported outside the secure physical perimeter of DHS

When submitting Privacy Threshold Analysis (PTA), Components must use the June 2020 PTA template (available on the DHS Connect site or by contacting the DHS Privacy Office).

Action Item: Submit PTA to Component Privacy Officer or Privacy Point of Contact (PPOC)

3.2 Compliance Activity #2 – Identify Protection Needs

The purpose of this activity is to identify Privacy Sensitive Systems where loss or corruption of, or unauthorized access to information contained in the system could have serious adverse effects. The NIST SP 800-53 controls identified in this Section must be implemented to ensure the effectiveness of this activity.

Action Item: If required by the DHS Privacy Office, as determined by the PTA, submit a Privacy Impact Assessment (PIA).

- RA-3: Risk Assessment
- RA-8: Privacy Impact Assessment

  DHS requires PIAs for systems in accordance with the E-Government Act, Homeland Security Act, and DHS Privacy Policy. Programs are evaluated by the Privacy Office on a case-by-case basis through the PTA process.

Action Item: Verify existing risk assessments

- RA-3 Risk Assessment

3.3 Compliance Activity #3 – Identify and Verify Organizational Policies

Information system owners should review policies that address storage of PII and downloading PII for transport, remote storage of PII, and remote access to systems containing PII. There are three key action items associated with this compliance activity:

Action Item: Identify existing organizational policies that address needs for protection of PII.

[4] FISMA = Federal Information Systems Management Act, 44 USC 3541 *et seq.*

Action Item: Verify that existing organizational policy adequately addresses needs for protection of PII that is or can be accessed remotely or physically removed.

Action Item: Develop and revise organizational policy as needed. The following NIST SP 800-53 control guidance should be reviewed to ensure the effectiveness of this compliance activity:

- PT-3: Personally Identifiable Information Processing Purposes
- SA-1: Policies and Procedures
- AC-1 Access Control
- AT-1 Security Awareness and Training
- AU-1 Audit and Accountability
- IA-1 Identification and Authentication
- MP-1 Media Protection
- SC-1 System and Communications Protection

In addition to the guidance given above, Components should review all approved policies or procedures that address access to Privacy Sensitive Systems and or downloading, transporting, and storage of PII.

3.4 Compliance Activity #4 – Implement Protection for PII Being Transported or Stored Offsite

PII shall not be removed from a DHS facility without written authorization from the system Authorizing Official (AO)[5] or from a person designated in writing by the AO, or in accordance approved SOPs for handling computer-readable data extracts. PII removed from a DHS facility on a laptop computer or other mobile computing device shall be encrypted unless the information is being sent to the individual in fulfillment of a Privacy Act or Freedom of Information Act (FOIA) request. If PII can be removed from an IT system by printouts, removable media, or other means, the System Security Plan shall document the specific procedures, training, and accountability measures in place to ensure that remote use of the data does not bypass the encryption.

Action Item: Implement security controls ensuring that PII is transported to a remote site only in encrypted form. The following NIST SP 800-53 control guidance should be reviewed to ensure the effectiveness of this compliance activity:

- MP-5 Media Transport
- SC-13 Cryptography Protection

Action Item: Implement security controls ensuring that PII is stored at a remote site only in encrypted form. The following NIST SP 800-53 control guidance should be reviewed to ensure the effectiveness of this compliance activity:

- PL-4 Rules of Behavior
- SC-4 Information in Shared System Resources
- SC-13 Cryptography Protection

[5] The term *Authorizing Official (AO)* replaces the term *Designated Accrediting Authority (DAA*) in accordance with NIST SP 800-37 Rev 2, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."

3.5 Compliance Activity #5 – Implement Protections for Remote Access to PII

All Privacy Sensitive Systems with AO approved remote access are required to ensure remote access is appropriately protected.

Action Item: Implement security controls requiring strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https). The following NIST SP 800-53 control guidance should be reviewed to ensure the effectiveness of this compliance activity:

- AC-17 Remote Access
- IA-5 Authenticator Management

In addition to these controls, DHS uses two-factor authentication through Common Access Cards. Also, remote access via a VPN or mobile device must have a time-out function that requires users to re-authenticate after extended periods of inactivity. Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after 20 minutes of inactivity.

Take the following actions when policy allows PII to be downloaded to a remote location. Components should apply controls necessary to enable and enforce only appropriate downloading.

Action Item: Implement security controls enforcing allowed downloading of PII. The following NIST SP 800-53 control guidance should be reviewed to ensure the effectiveness of this compliance activity:

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-4 Information Flow Enforcement
- AC-6 Least Privilege
- AC-13 Supervision and Review – Access Control
- AU-2 Event Logging
- AU-6 Audit Record Review, Analysis, and Reporting

Every System Owner who maintains a Privacy Sensitive System is responsible for authorizing, approving, and tracking all requests to extract PII data. System security plans for systems that as part of routine business remove PII from an IT system should address the risks associated with the removal and standard operating procedures to mitigate the risks should be attached to the plans. Computer-readable data extracts not included within the boundaries of a system accreditation must be logged and deleted after 90 days or when their use is no longer required. Please reference the sample tracking form provided in Appendix S2: *Sample PII Extract Tracking Log*. The DHS Privacy Office or Component Privacy Officer should work with System Owners to conduct periodic audits to ensure that systems are complying with the requirements of this section.

Action Item: Implement security controls enforcing encrypted remote storage of PII. The following NIST SP 800-53 control guidance should be reviewed to ensure the effectiveness of this compliance activity:

- PL-4 Rules of Behavior
- SC-4 Information in Shared System Resources
- SC-13 Cryptography Protection

All Privacy Sensitive Systems that allow information to be remotely accessed are required to implement the following controls if the information is stored locally. Implementing these controls will result in only the necessary information being transmitted to the remote Component.

Action Item: Implement security controls enforcing NO remote storage of PII.

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-4 Information Flow Enforcement
- AC-6 Least Privilege
- AC-13 Supervision and Review-Access Control
- AC-17 Remote Access
- AT-2 Security Training and Awareness
- AU-2 Event Logging
- AU-6 Audit Record Review, Analysis, and Reporting
- PL-4 Rules of Behavior
- SC-4 Information in Shared System Resources

3.6 Compliance Requirement #6 – POA&Ms, Exceptions, and Waivers for Key Privacy Controls

Components with Privacy Sensitive Systems who have not effectively implemented NIST SP 800-53 control guidance above are required to open Plans of Action and Milestones (POA&Ms) or request waivers or exceptions from the DHS Chief Privacy Officer as the Senior Agency Official for Privacy (SAOP). Any waiver or exception requests from Components must be approved by the DHS Privacy Office before review by the CISO. Waivers or exceptions are not permissible for any privacy controls.

APPENDIX 1 – COMPLIANCE ACTIVITIES CONTROLS AND PROCEDURES

Source: The controls and procedures in the following tables are taken from NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations""

Compliance Activity #1: Confirm that the system maintains, uses, or discloses personally Identifiable Information (PII) and so is a Privacy Sensitive System, and that the system and the PII can be accessed remotely or physically.	
<u>Action Item:</u> Submit or update the Privacy Threshold Analysis (PTA) to identify IT systems.	
Control	*Procedures*
Privacy Threshold Analysis (PTA)	The Component must submit or update their PTA using the 2020 PTA template.
Compliance Activity #2: **Identify Protection Needs**	
<u>Action Item:</u> If required by the DHS Privacy Office, as determined by the PTA, submit a Privacy Impact Assessment (PIA).	
Control	*Procedures*
RA-8 *Privacy Impact Assessment*	DHS requires PIAs for systems in accordance with the E-Government Act, Homeland Security Act, and DHS Privacy Policy. Programs are evaluated by the Privacy Office on a case-by-case basis through the PTA process.

RA-3 Risk Assessment	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. c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the chief information officer, senior information security officer, information system owner, mission owners, and information owners/stewards. The organization also considers 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 in categorizing the information system. The security categorization process facilitates the creation of an *inventory* of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted. Related controls: CM-8, MP-4, SC-7.
Action Item: Verify existing risk assessments	
Control	*Procedures*
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]; and d. 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: A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals 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. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. Risk assessments (either formal or informal) can be conducted by organizations at various steps in the Risk Management Framework including information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control 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 the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.
#3: Identify and Verify Organizational Policies	
Action Item: Identify existing organizational policies that address needs for protection of PII	
Action Item: Verify that existing organizational policy adequately addresses needs for protection of PII that is or can be accessed remotely or physically removed.	
Action Item: Revise/develop organizational policy as needed.	
Control	*Procedures*

AC-1 *Access Control*	The organization develops, disseminates, and periodically reviews/updates *[Assignment: organization-defined frequency]:* a. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.
AT-1 *Security Awareness and Training*	The organization develops, disseminates, and periodically reviews/updates [*[Assignment: organization-defined frequency]:* a. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. Related control: PM-9.
AU-1 *Audit and Accountability*	The organization develops, disseminates, and periodically reviews/updates *[Assignment: organization-defined*

	frequency]: a. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. Related control: PM-9.
IA-1 *Identification and Authentication*	The organization develops, disseminates, and periodically reviews/updates *[Assignment: organization-defined frequency]*: a. A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. Related control: PM-9.
MP-1 *Media Protection*	The organization develops, disseminates, and periodically reviews/updates *[Assignment: organization-defined*

	frequency]: a. Formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. Related control: PM-9.
SC-1 *System and Communications Protection Policy and Procedures*	The organization develops, disseminates, and periodically reviews/updates *[Assignment: organization-defined frequency]:* a. A formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.
#4: Implement Protections for Personally Identifiable Information Being Transported and/or Stored Offsite	

Action Item: Implement security controls ensuring that PII is transported only in encrypted form.	
Control	*Procedures*
MP-5 *Media Transport*	The organization: a. Protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures]. b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media. 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). Related controls: AC-19, CP-9.
SC-13 *Cryptography Protection*	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Supplemental Guidance: None.
Action Item: Implement security controls ensuring that PII is stored only in encrypted form.	
Control	*Procedures*
PL-4 *Rules of Behavior*	The organization: a. Establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. b. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information. Supplemental Guidance: The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior. Related control: PS-6.
SC-4 *Information in Shared System Resources*	The information system prevents unauthorized and unintended information transfer via shared system resources. Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where

	shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.
SC-13 *Cryptography Protection*	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Supplemental Guidance: None.
#5: Implement Protections for Remote Access to PII	
Action Item: Implement security controls requiring authenticated, virtual private network (VPN) connection or equivalent encryption.	
Control	*Procedures*
AC-17 *Remote Access*	The organization: a. Documents allowed methods of remote access to the information system. b. Establishes usage restrictions and implementation guidance for each allowed remote access method. c. Monitors for unauthorized remote access to the information system. d. Authorizes remote access to the information system prior to connection. e. Enforces requirements for remote connections to the information system. Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.

	Control Enhancements: **(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.** Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy. **(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.** Enhancement Supplemental Guidance**:** The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13. **(3) The information system routes all remote accesses through a limited number of managed access control points.** Enhancement Supplemental Guidance: Related control: SC-7.
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 and/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 upon information system installation. f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate). g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]. h. Protecting authenticator content from unauthorized disclosure and modification. i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Supplemental Guidance: User 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). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user 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 verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.
<u>Action Item:</u> Implement security controls enforcing allowed downloading of PII.	
Control	*Procedures*
AC-2 *Account Management*	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); establishing conditions for group membership. b. Identifying authorized users of the information system and specifying access privileges. c. Requiring appropriate approvals for requests to establish accounts. d. Establishing, activating, modifying, disabling, and removing accounts; specifically authorizing and monitoring the use of guest/anonymous and temporary accounts. e. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. f. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users.

	g. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage. and (iii) other attributes as required by the organization or associated missions/business functions. h. Reviewing accounts [Assignment: organization-defined frequency]. Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.
AC-3 *Access Enforcement*	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy. 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) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. 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, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.
AC-4 *Information Flow Enforcement*	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. 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. A few examples of flow control restrictions include keeping export-controlled information from being transmitted in the clear to the

	Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.
AC-6 *Least Privilege*	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.
AU-2 *Event Logging*	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of 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 list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency

	of (or situation requiring) auditing for each identified event]. Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are to be *audited* at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.
AU-6 *Audit Record Review, Analysis, and Reporting*	The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.
Action Item: Implement security controls enforcing encrypted remote storage of PII	
Control	*Procedures*
PL-4 *Rules of Behavior*	The organization: Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

	b. Receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. Supplemental Guidance: The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior.
SC-4 *Information in Shared System Resources*	The information system prevents unauthorized and unintended information transfer via shared system resources. Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence, which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.
SC-13 *Cryptography Protection*	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Supplemental Guidance: None.
Action Item: Implement security controls enforcing NO remote storage of PII.	
Control	*Procedures*
AC-2 *Account Management*	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary). b. Establishing conditions for group membership; identifying authorized users of the information system and specifying access privileges;

	c. Requiring appropriate approvals for requests to establish accounts. d. Establishing, activating, modifying, disabling, and removing accounts. e. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts. f. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. g. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users. h. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and i. Reviewing accounts [Assignment: organization-defined frequency]. Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.
AC-3 *Access Enforcement*	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy. Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. 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, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.
AC-4 *Information Flow Enforcement*	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. 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. A few examples of flow control restrictions include keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.
AC-6 *Least Privilege*	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.
AC-17 *Remote Access*	The organization: a. Documents allowed methods of remote access to the information system. b. Establishes usage restrictions and implementation guidance for each allowed remote access method;

	c. Monitors for unauthorized remote access to the information system. d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network, when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.
AT-2 *Security Training and Awareness*	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter. Supplemental Guidance: The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization 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 as it relates to the organization's information security program. 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.
AU-2 *Event Logging*	The organization determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events; provides a

	rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents; and determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*]. Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are to be *audited* at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.
AU-6 *Audit Record Review, Analysis, and Reporting*	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.
PL-4 *Rules of Behavior*	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage. b. Receives signed acknowledgement from users indicating that they have read, understand, and

	agree to abide by the rules of behavior, before authorizing access to information and the information system. Supplemental Guidance: The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior.
SC-4 *Information in Shared System Resources*	The information system prevents unauthorized and unintended information transfer via shared system resources. Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.
#6: POA&Ms, Exceptions and Waivers for Key Privacy Controls	
Action Item: Open Plans of Actions and Milestones (POA&Ms) or request waiver or exceptions	
Control	*Procedures*
Plans of Actions and Milestones (POA&Ms)	Open Plans of Actions and Milestones (POA&Ms) or request waiver or exceptions via the DHS Chief Privacy Officer as the Senior Agency Official for Privacy (SAOP). Any waiver or exception requests from Components must be approved by the DHS Privacy Office before review by the CISO. Waivers or exceptions are not permissible for any privacy controls.

APPENDIX 2 - SAMPLE PII EXTRACT TRACKING LOG

Control Number	Date & Time	Originator	Recipient	Description	Media Type	Purpose	Encryption Y/N	Label "SPII"	Comment	Final Disposition	Approval