U.S. Customs and Border Protection

Attachment S

Compliance Framework NIST SP 800-53 Controls for Privacy Sensitive Systems

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53

CONTENTS

1.0 Introduction

OMB, through Memorandum M-06-16, issued guidance for protecting sensitive agency information based on National Institute of Standards and Technology (NIST) checklist for the protection of remote information. In order to implement the NIST SP 800-53A checklist the Privacy Office, in coordination with the Chief Information Security Office (CISO), has designated the following requirements for protecting Privacy Sensitive Systems1 that permit remote access or allow for the removal of sensitive information outside of internal agency controls:

1. Confirm 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 transported outside the agency's secured, physical perimeter[2];
2. Identify Protection Needs;
3. Identify and Verify Organizational Policies;
4. Implement Protections for PII Being Transported and/or Stored Offsite;
5. Implement Protections for Remote Access to Systems Containing Personally Identifiable Information; and
6. POA&Ms, Exceptions and Waivers for Key Privacy Controls.

Each of these requirements is described 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.

3.0 Compliance Activities

Compliance Activity #1:
Confirm 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 transported outside the agency's secured, physical perimeter

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

- Identify systems containing PII;
- Verify the categorization of that information; and
- Assess whether or not those systems can be remotely accessed; or if PII can be physically transported outside DHS's secured, physical perimeter.

[1] A Privacy Sensitive System is any system that contains personally identifiable information (PII).
[2] Refers to information that may be transported on removable media and on portable/mobile devices such as laptop computers and/or digital assistants outside of the agency's secured physical perimeter.

The Privacy Office has updated the Privacy Threshold Analysis (PTA) to identify IT systems that permit remote access or physical removal of PII. If a component permits remote access to any system then the component must update the PTA using the May 15, 2008 PTA template.

Compliance Activity #2:
Identify Protection Needs

The purpose of this activity is to identify Privacy Sensitive Systems where the loss, corruption, or unauthorized access to information contained in the system could result in serious adverse effect. The following NIST SP 800-53 controls must be implemented to ensure compliance with this activity.

Action Item: Verify information categorization to ensure identification of PII requiring protection when accessed remotely or physically removed.

- PL-5 *Privacy Impact Assessment*

  DHS requires PIAs for systems related to internal government operations (e.g. Human Resource Systems) if the system will eventually be rolled out to all DHS employees. Each program is evaluated by the Privacy Office on a case by case basis. PIA is not necessarily required where information relates to internal government operations (e.g. human resource operations) per OMB Memorandum M-03-22*, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* Attachment A, Section II.B.3.

- RA-2 *Security Categorization (FIPS 199)*

Action Item: Verify existing risk assessments

- RA-4 *Risk Assessment Update*

Compliance Activity #3
Identify and Verify Organizational Policies

Systems Owners should review policies that address downloading PII for transport, remote access of systems containing PII and remote storage of PII. There are three key action items associated with implementing this activity:

Action Item: Identify existing organizational policies that address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.

Action Item: Verify that the existing organizational policy adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.

Action Item: Revise/develop organizational policy as needed.

The following NIST SP 800-53 control-associated guidance should be reviewed to ensure compliance with this activity:

- AC-1 *Access Control Policy and Procedures*
- AT-1 *Security Awareness and Training Policy and Procedures*
- AU-1 *Audit and Accountability Policy and Procedures*
- IA-1 *Identification and Authentication Policy and Procedures*
- MP-1 *Media Protection Policy and Procedures*
- SC-1 *System and Communications Protection Policy and Procedures*

In addition to the above identified guidance, the component should review any and all approved policies or procedures addressing remote access to Privacy Sensitive Systems and/or downloading, transporting and storage of PII.

Compliance Activity #4:
Implement Protections for PII Being Transported and/or Stored Offsite

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

All Privacy Sensitive Systems containing PII data to be transported and/or stored at off site storage facilities should implement the following controls to ensure PII data in transport and/or in offsite storage is in an encrypted form.

Action Item: Implement security controls ensuring that PII is transported to a remote site only in encrypted form.

- MP-5 *Media Transport*
- SC-13 *Use of Validated Cryptography*

Action Item: Implement security controls ensuring that PII is stored at a remote site only in encrypted form.

- PL-4 *Rules of Behavior*
- SC-4 *Information Remnants*
- SC-13 *Use of Validated Cryptography*

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).

- AC-17 *Remote Access, with enhancements (1), (2), and (3)*
- IA-5 *Authenticator Management*

In addition to the controls listed above, DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Remote access via a VPN and mobile devices must have "time-out" functions requiring 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.

Implement the following controls when the policy allows PII to be downloaded to a remote location. The component should apply necessary controls to enable and enforce only appropriate downloading.

Action Item: Implement security controls enforcing allowed downloading of PII

- AC-3 *Access Enforcement*
- AC-4 *Information Flow Enforcement*
- AC-6 *Least Privilege*
- AC-13 *Supervision and Review – Access Control*
- AU-2 *Auditable Events*
- AU-6 *Audit Monitoring, Analysis, and Reporting*

Every System Owner who maintains a Privacy Sensitive System is responsible for authorizing, approving and tracking any requests to extract PII data. Systems that as part of routine business remove PII from one IT system should address in the system security plan the risks associated with this removal as part of the system security plan and attach standard operating procedures to mitigate the risk. Computer-readable data extracts not included within the boundaries of a system accreditation must be logged and deleted after 90 days or its use is still required. Please reference the sample tracking form provided in Appendix S2: *Sample PII Extract Tracking Log*. The DHS Privacy Office or Component Privacy Officer will conduct periodic audits to ensure System Owners are complying with the requirements of this section.

Action Item: Implement security controls enforcing encrypted remote storage of PII.

- PL-4 *Rules of Behavior*
- SC-4 *Information Remnants*

- SC-13 *Use of Validated Cryptography*

All Privacy Sensitive Systems that allow information to be remotely accessed, but only if not stored locally, are required to execute the following controls. 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-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 Awareness*
- AU-2 *Auditable Events*
- AU-6 *Audit Monitoring, Analysis, and Reporting*
- PL-4 *Rules of Behavior*
- SC-4 *Information Remnants*

Compliance Requirement #6

POA&Ms, Exceptions and Waivers for Key Privacy Controls

Components with Privacy Sensitive Systems who have not implemented the above referenced NIST SP 800-53 controls are required to open Plans of Actions and Milestones (POA&Ms) or request waiver or exception via the DHS Chief Privacy Officer as the Senior Agency Official for Privacy (SAOP). Any component waiver or exception requests must first be approved by the DHS Privacy Office before review by the CISO. Approved system or program waivers or exceptions are required to be uploaded into TAF in order to close a POA&M which addresses a Privacy control weakness.

Appendix S1 – Compliance Activities Controls and Procedures

#1: Confirm 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 transported outside the agency's secured, physical perimeter	
Action Item: Update the Privacy Threshold Analysis (PTA) to identify IT systems that permit remote access or physical removal of sensitive information.	
Control	*Procedures*
Privacy Threshold Analysis (PTA)	If a component permits remote access to any system then the component must update their PTA using the 2008 PTA template.
#2: Identify Protection Needs	
Action Item: Verify information categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed.	
Control	*Procedures*
PL-5 *Privacy Impact Assessment*	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.
RA-2 *Security Categorization (FIPS 199)*	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations. Supplemental Guidance: The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST Special Publication 800-60 provides guidance on determining the security categories of the information types
Action Item: Verify existing risk assessments	
Control	*Procedures*
RA-4 *Risk Assessment Update*	The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever

	there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system. Supplemental Guidance: The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.
#3: Identify and Verify Organizational Policies	
<u>Action Item:</u> Identify existing organizational policies that address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.	
<u>Action Item:</u> Verify that the existing organizational policy adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.	
<u>Action Item:</u> Revise/develop organizational policy as needed.	
Control	*Procedures*
AC-1 *Access Control Policy and Procedures*	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST Special Publication 800-12 provides guidance on security policies and procedures.
AT-1 *Security Awareness and Training Policy and Procedures*	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.
AU-1	*Audit and Accountability Policy and Procedures*	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST Special Publication 800-12 provides guidance on security policies and procedures.
IA-1	*Identification and Authentication Policy and Procedures*	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
MP-1	*Media Protection Policy and Procedures*	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. Supplemental Guidance: The media protection policy and procedures are consistent with applicable laws,

	Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST Special Publication 800-12 provides guidance on security policies and procedures.
SC-1 *System and Communications Protection Policy and Procedures*	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST Special Publication 800-12 provides guidance on security policies and procedures.
#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 protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, 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 computers, personal digital assistants, cellular telephones) 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 exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the

	specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate 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).
SC-13 *Use of Validated Cryptography*	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Supplemental Guidance: The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.
Action Item: Implement security controls ensuring that PII is stored only in encrypted form.	
Control	*Procedures*
PL-4 *Rules of Behavior*	The organization 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. 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: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.
SC-4 *Information Remnants*	The information system prevents unauthorized and unintended information transfer via shared system resources. Supplemental Guidance: Control of information system remnants, sometimes referred to as object reuse, or data remnants, prevents 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.

SC-13 *Use of Validated Cryptography*	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Supplemental Guidance: The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.
#5: Implement Protections for Remote Access to PII	
Action Item: Implement security controls requiring authenticated, virtual private network (VPN) connection.	
Control	*Procedures*
AC-17 *Remote Access, with enhancements (1), (2), and (3)*	The organization authorizes, monitors, and controls all methods of remote access to the information system. Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2.
IA-5 *Authenticator Management*	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others,

	and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
Action Item: Implement security controls enforcing allowed downloading of PII	
Control	*Procedures*
AC-3 *Access Enforcement*	The information system enforces assigned authorizations for controlling 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 controlling 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 a controlled, audited, and manual 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. Related security control: SC-13.
AC-4 *Information Flow Enforcement*	The information system enforces assigned 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, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: 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. Related security control: SC-7.
AC-6 *Least Privilege*	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Supplemental Guidance: 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, organizational assets, and individuals.
AC-13 *Supervision and Review – Access Control*	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.
AU-2 *Auditable Events*	The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*]. Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. 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. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The

	checklists and configuration guides at http://csrc nist.gov/pcig/cig html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.
AU-6 *Audit Monitoring, Analysis, and Reporting*	The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. 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, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. 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: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.
SC-4 *Information Remnants*	The information system prevents unauthorized and unintended information transfer via shared system resources. Supplemental Guidance: Control of information system remnants, sometimes referred to as object reuse, or data remnants, prevents 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.
SC-13 *Use of Validated Cryptography*	Control: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

	Supplemental Guidance: The applicable federal standard for employing cryptography in nonnational security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc nist.gov/cryptval.
Action Item: Implement security controls enforcing NO remote storage of PII.	
Control	*Procedures*
AC-3 *Access Enforcement*	The information system enforces assigned authorizations for controlling 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 controlling 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 a controlled, audited, and manual 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. Related security control: SC-13.
AC-4 *Information Flow Enforcement*	The information system enforces assigned 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, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: 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. Related security control: SC-7.
AC-6 *Least Privilege*	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Supplemental Guidance: 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, organizational assets, and individuals.
AC-13 *Supervision and Review-Access Control*	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.
AC-17 *Remote Access*	The organization authorizes, monitors, and controls all methods of remote access to the information system. Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2.
AT-2 *Security Awareness*	The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, 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 based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.
AU-2 *Auditable Events*	The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*]. Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. 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. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc nist.gov/pcig/cig html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.
AU-6 *Audit Monitoring, Analysis, and Reporting*	The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. 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 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. 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: Electronic signatures are acceptable for use in acknowledging rules of behavior

	unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.
SC-4 *Information Remnants*	The information system prevents unauthorized and unintended information transfer via shared system resources. Supplemental Guidance: Control of information system remnants, sometimes referred to as object reuse, or data remnants, prevents 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.
#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 component waiver or exception requests must first be approved by the DHS Privacy Office before review by the CISO. Approved system or program waivers or exceptions are required to be uploaded into TAF in order to close a POA&M which addresses a Privacy control weakness.

Control Categorization

AC=Access Control
AT=Awareness & Training
AU=Audit & Accountability
CA=Certification, Accreditation & Security Assessment
CM=Configuration Management
CP=Contingency Planning
IA=Identification and Authentication
IR=Incident Response
MA=Maintenance
MP=Media Protection
PE=Physical & Environmental Protection
PL = Planning
PS=Personal Security
RA=Risk Assessment
SA=Systems & Services Acquisition
SC=System and Communications Protection
SI=System and Information Integrity

Appendix S2 - Sample PII Extract Tracking Log

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