UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

MEMORANDUM FOR: Federal Information Security Modernization Act (FISMA) 2020 Report

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.10.27 16:32:49 -04'00'

FROM: Catrina D. Purvis
Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and Director, Office of Privacy and Open Government

SUBJECT: Fiscal Year 2020 Privacy Continuous Monitoring Strategy (PCMS)

The Office of Management and Budget (OMB) Memorandum M-20-04 provides federal agencies with Fiscal Year (FY) 2019-2020 Federal Information Security Modernization Act of 2014 (FISMA) reporting guidance and deadlines. It includes a requirement for the agency SAOP to submit the agency's Privacy Continuous Monitoring Strategy.

The Department follows the process described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, that incorporates information security and privacy risk management activities into the system development life cycle. This process includes privacy continuous monitoring. The DOC PCMS is fully integrated into the overall DOC Privacy Program Plan at Section 7, *Privacy Control Requirements/Continuous Monitoring Strategy*, and as excerpted in Attachment A of this memorandum. The DOC PCMS ensures that privacy controls are implemented, assessed, and effectively monitored on an ongoing basis. Through the privacy continuous monitoring program, the DOC:

- maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks;
- monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII); and
- conducts privacy control assessments systems to verify the continued effectiveness of privacy controls selected/implemented across the Department's risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks.

In addition, the Senior Agency Official for Privacy (SAOP) and the Chief Information Officer (CIO) have designated privacy and security controls which must be assessed annually as part of the DOC Cybersecurity and Privacy continuous monitoring strategies. The list of these controls is provided in Attachment B of this memorandum.

Another important aspect of the DOC PCMS is the privacy policy memorandum, *Departmental Privacy Standards for Commerce Data Loss Prevention (DLP) Security Tools*. This policy establishes a requirement for all bureaus and operating units to configure their DLP security tools to implement privacy control capabilities that meet Departmental privacy DLP standards. This requirement enhances privacy protections and reduces PII breaches/incidents within the

Department. The DLP policy is also incorporated into the overall DOC Privacy Program Plan and included as Attachment C of this memorandum. Furthermore, NIST has technical tools in place to continuously monitor for unauthorized use of PII (e.g., McAfee MVISION DLP for Google and Box cloud storage services, and Microsoft DLP for Microsoft cloud storage services and cloud email). The National Telecommunications and Information Administration (NTIA) uses Data Loss Prevention Endpoint (DLPe) to continuously monitor PII and to detect unauthorized devices connecting to NTIA systems and the National Oceanic and Atmospheric Administration uses a Smartsheet tracker (privacy management tool) that conveys privacy compliance documentation needing to be reviewed and/or updated in which action items are tracked until completed. Additionally, the U.S. Patent and Trademark Office (USPTO) hired three new employees after reassigning the vacant full-time equivalent positions within the Office of the Chief Information Officer, in an effort to improve USPTO's privacy and continuous monitoring program.

Finally, the DOC PCMS includes Privacy Overlays. The DOC Privacy Program leverages privacy overlays established for national security systems as guidance when selecting/assessing effectiveness of privacy protections. An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The purposes of the privacy overlays include providing standard security and privacy control baselines for systems containing PII, ensuring integration of privacy considerations into the system development life cycle and security processes in the early stages, and providing guidance for privacy requirements for protected health information. The Privacy Overlays leveraged by DOC are also incorporated into the overall DOC Privacy Program Plan with summarized information included as Attachment D of this memorandum.

The full list of attachments to the memorandum include the following:

Attachment A – Section 7, Privacy Control Requirements/Continuous Monitoring Strategy - DOC Privacy Program Plan Excerpt
Attachment B – Privacy and Security Controls
Attachment C – Departmental Privacy Standards for Commerce Data Loss Prevention Security Tools
Attachment D – Summarized Information on DOC Privacy Overlays

Attachment A

Section 7, Privacy Control Requirements/Continuous Monitoring Strategy
DOC Privacy Program Plan Excerpt

7 Privacy Control Requirements/Continuous Monitoring Strategy

The DOC ensures compliance with all applicable statutory, regulatory, and policy requirements. The DOC implements the NIST SP 800-53, Rev 4 baseline of security and privacy controls, including Privacy Overlays. The DOC adheres to Section 208 of the E-Government Act of 2002, which requires agencies to conduct Privacy Threshold Analyses (PTAs) and PIAs for electronic information systems and collections. In addition, the DOC meets Privacy Act System of Records Notice (SORN) requirements.

7.1 DOC Appendix J Control Allocation Table

The DOC SAOP designates which privacy controls the Department will treat as program management, common, information system-specific, and hybrid controls. Privacy program management controls are controls that are generally implemented at the agency level and essential for managing the agency's privacy program. Common controls are controls that are inherited by multiple information systems. Information system-specific controls are controls that are implemented for a particular information system or the portion of a hybrid control that is implemented for a particular information system. Hybrid controls are controls that are implemented for an information system in part as a common control and in part as an information system-specific control. The determination as to whether a privacy control is a common, hybrid, or information system-specific control is based on context. The Appendix J Control Allocation Table is found in Appendix E.

7.2 DOC Privacy Overlays

The DOC Privacy Program leverages privacy overlays established for national security systems as guidance when selecting/assessing effectiveness of privacy protections. According to NIST SP 800-53, Revision 4, an overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The purposes of the privacy overlays include providing standard security and privacy control baselines for systems containing PII, ensuring integration of privacy considerations into the system development life cycle and security processes in the early stages, and providing guidance for privacy requirements for protected health information. Summarized information on implementing privacy overlays is found in Appendix F. The entire DOC Privacy Overlays document can be found on the DOC Privacy website at www.commerce.gov/privacy.

7.3 Privacy Threshold Analysis (PTA)

A PTA is a questionnaire used to determine if a system contains PII, whether a PIA is required, whether a SORN is required, and if any other privacy requirements apply to the information system. A PTA is completed when proposing a new information technology system through the budget process that collects, stores, or processes identifiable information; when developing or significantly modifying such a system; or when proposing a new electronic collection of identifiable information. A PTA determines if a PIA is required. The PTA Template is found in Appendix G.

The Department also has a PTA for information collections and forms. The Forms PTA (Appendix H) must accompany all information collections submitted as a part of the Paperwork Reduction Act process.

7.4 Privacy Impact Assessment (PIA)

A PIA is an analysis of how information in identifiable form is collected, maintain, stored, and disseminated, in addition to examining and evaluating the privacy risks and the protections and processes for handling information to mitigate those privacy risks. A PIA is conducted before:

A. Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form, from or about, members of the public; or
B. Initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

If a PIA is required, the Information System Security Officer (ISSO) and System Owner (SO) work closely with the Information Technology Security Officer (ITSO) and Privacy Act Officer (PAO) to complete the PIA Template (Appendix I). Also, a Controls Assessment Worksheet (Appendix J) which identifies the status of the security and privacy controls applicable to the PII Confidentiality Impact Level must be completed and approved by the bureau’s Chief Information Officer. Once these documents are complete and fully signed by the certifying officials, the BCPO submits the PTA, PIA, and Controls Assessment Worksheet to the SAOP/CPO for review. A PIA Compliance Review Board (CRB) meeting is held, if deemed necessary by the Deputy Director for Departmental Privacy Operations. Once the SAOP/CPO approves the PIA, the PTA and PIA are made publicly available on the Department’s privacy website at www.commerce.gov/privacy, unless the Department determines not to make the PIA publicly available if such publication would raise security concerns, reveal issues of national security, classified information, or reveal sensitive information that could be potentially damaging to a national interest, law enforcement effort, or competitive business interest. A flowchart of the PIA process is found in Appendix K.

7.5 PIA Compliance Review Board (CRB) Meetings

The SAOP conducts PIA CRB meetings with the BCPOs, ISSOs, SOs, ITSOs, PAOs, and/or AOs to discuss system/data characterization, information sharing practices, website/mobile application processes, privacy controls, and risk assessments for new systems processing PII/BII and existing systems with changes that create new privacy risks. Examples of these changes include:

1. Conversions – Converting paper-based records to electronic systems;
2. Anonymous to Non-Anonymous – Applying functions to an existing information collection that changes anonymous information into information in identifiable form;
3. Significant System Management Changes – Applying new technologies that significantly change how information in identifiable form is managed in the system
4. Significant Merging – Adopting or altering business processes so government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;
5. New Public Access – Applying new user authenticating technology (e.g., password, digital certificate, biometric) to an electronic information system accessed by members of the public;
6. Commercial Sources – Incorporating databases of information in identifiable form purchased or obtained from commercial or public sources into existing information systems;
7. New Interagency Uses – Working together with other agencies on shared functions involving significant new uses or exchanges of information in identifiable form;
8. Internal Flow or Collection – Altering a business process that results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form
9. Alteration in Character of Data – Raising the risks to personal privacy (e.g., addition of health or financial information) when new information in identifiable form is added to a collection.[1]

The PIA CRB Risk Analysis Guide (Appendix L) outlines the critical areas discussed during these meetings.

Through the continuous monitoring program, PTAs are completed annually to determine if a PII processing system has changes that create new privacy risks. If so, the PIA is updated, a Controls Assessment Worksheet (Appendix J) is completed, and a PIA CRB meeting is held to ensure compliance with applicable laws and regulations. Otherwise, the PTA and latest SAOP approved PIA (with updates only to Section 1.1 (Status of the Information System), Section 6.2 (Limitation on re-dissemination of PII/BII if using template version number 01-2020), Section 8.1 (Administrative and Technological Controls – date of most recent Assessment & Authorization only), and if needed, Sections 12.2 and/or 12.3 (Analysis)) are submitted to the SAOP/CPO, along with the PIA Annual Review Certification Form (Appendix M). A CRB meeting must be conducted every three (3) years.

A SAOP approved PIA is good for one year only. Privacy compliance documentation must be received by the SAOP/CPO at least 60 days in advance of the ATO (new PII/BII processing system), ATO expiration date (existing PII/BII processing system without a current SAOP approved PIA or existing PII/BII processing system and there are changes

[1] OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.*

which create new privacy risks in which a CRB meeting is required), or SAOP approved PIA expiration date (if before ATO expiration date or if after ATO expiration date and the certification process will be used). In order to ensure compliance with FISMA, notifications to the B/OUs will be sent within the following timelines:

90 days – Notification to BCPO requesting submission of privacy compliance documents
60 days – Notification reminder to BCPO if privacy compliance documents are not received
45 days – Notification to the B/OU Deputy Under Secretary or equivalent if privacy compliance documents are not received
30 days – SAOP/CPO non-concurrence memorandum issued

7.6 Contractors and Third Parties

The DOC ensures contractors and third parties that: 1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of the Department; or 2) operate or use information systems on behalf of the Department, comply with the mandated privacy requirements. The DOC Privacy Program coordinates with the Office of Acquisition Management and Enterprise Services Contracting Office to ensure that the applicable privacy clauses, below from the FAR, are included in the terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of information in the possession of the Department:

- FAR Subpart 4.19 – Basic Safeguarding of Covered Contractor Information Systems
  - FAR Clause 52.204-21
- FAR Subpart 24.1 Protection of Individual Privacy
  - FAR Clause 52.224-1 “Privacy Act Notification”
  - FAR Clause 52.224-2 “Privacy Act”
- FAR 39.101 – Acquisition of Information Technology-General-Policy
- FAR 39.105 – Acquisition of Information Technology-General-Privacy
  - FAR Clause 52.239-1 “Privacy or Security Safeguards”
- FAR Subpart 27.4 – Rights in Data and Copyrights

These FAR clauses are also included in the IT Compliance in Acquisition Checklist found in Appendix B.

7.7 System of Records Notice (SORN)

The DOC meets Privacy Act requirements for publishing notices of its systems of records in the Federal Register which are referred to as SORNs. A system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

A SORN is intended to inform the public about what kinds of personal information federal agencies maintain; to limit the uses and disclosures of the information to those compatible with the law permitting its collection; and to describe how an individual might request access to their information or to seek redress otherwise.

- Bureau and Operating Unit (Component) Notices – Component systems of records are records for which a DOC component such as the Census Bureau, writes the SORN for the records for which they have physical custody and maintain. The following characteristics also apply:
    - The physical records contained within the system of records belong to the respective component; and
    - The corresponding SORNs begin with the component's identifier (e.g., CENSUS-1, 2, etc.).
- Department-wide Notices – Systems of records for which the Department writes the SORN for the records, but may not have physical custody as a matter of necessity. The Department's components may use Department-wide SORNs to cover records systems they maintain. The following characteristics apply to Department-wide notices:
    - The physical records contained within the system of records belong to the respective component;
    - The Department may still retain some authority over the records; and
    - The corresponding SORNs begin with the identifier DEPT-1, 2, etc.
- Government-wide Notices – Systems of records for which another Federal agency, such as the Office of Personnel Management (OPM), writes the SORN for the records, but does not have physical custody as a matter of necessity, as in the case of general personnel records. Federal agencies may use Government-wide SORNs to cover Government-wide records systems and the following characteristics apply:
    - The physical records contained within the system of records belong to the respective agency;
    - OPM, for example, still retains some authority over the records; and
    - The corresponding SORNs begin with the identifier GOVT-1, 2, etc.

7.7.1 SORN Reviews and Updates

The DOC ensures that SORNs remain accurate, up-to-date, and appropriately scoped during B/OU PIA reviews and as part of the DOC PIA CRB process. The DOC also uses a CRB meeting to ensure that with respect to SORNs:

- No system of records includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order; and
- Each exemption claimed for a system of records pursuant to 5 U.S.C. § 552a(j) and (k) remains appropriate and necessary.

BCPOs are responsible for obtaining B/OU PAO concurrence with the SORN(s) cited to cover system(s) of records identified in a PIA. When a SORN needs to be amended or created to cover a system of records, the B/OU PAO works with the appropriate B/OU subject matter experts and the Departmental Privacy Act Officer (DPAO) to draft the amended or new SORN(s), ensuring that the SORNs include the information required by and are in the format identified in OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication* *under the Privacy Act*. The template for a new/modified SORN is found in Appendix N. The template for the rescindment of a SORN is found in Appendix O.

7.7.2 Reporting SORNs to OMB and Congress

The SAOP and the DPAO report all significant changes to SORNs and new SORNs to OMB and Congress following requirements identified in OMB Circular A-108. Reports include a transmittal letter signed by the SAOP and a narrative statement, generally prepared by the appropriate B/OU PAO, that contain the following elements:

- A description of the purpose(s) for which the DOC is establishing or modifying the system of records and an explanation of how the scope of the system is commensurate with the purpose(s) of the system;
- The specific authorities (statutes or executive orders) under which the system of records will be maintained. The DOC cites the specific programmatic authorities for collecting, maintaining, using, and disseminating the information;
- An evaluation of the probable or potential effect of the proposal on the privacy of individuals whose information will be maintained in the system of records. The assessment may be derived from applicable PIAs;
- An explanation of how each new or modified routine use satisfies the compatibility requirement of the Privacy Act; and
- Any information collections approved by OMB or submitted to OMB for approval that will be used to collect information that will be maintained in the system of records, along with the relevant names, OMB control numbers, and expiration dates.

7.8 Privacy Act Statement

The DOC ensures that a compliant Privacy Act Statement is provided or available when collecting PII. The Privacy Act Statement is provided on the collection instrument, on a poster that is visible to the individual, or on a separate form that can be retained by the individual prior to the actual collection. A Privacy Act Statement provides an individual with the following:

- Agency’s legal authority to collect the information, such as a statute, executive order, and/or regulation;
- Purpose(s) for collecting the information and how it will be used;
- Routine uses of the information, which describes to whom the Department may disclose information outside of the Department and for what purposes[2]; and
- Whether providing the information is mandatory or voluntary, along with the effects, if any, on the individual of not providing all or any part of the information requested.

[2] The DOC also includes appropriate citation to the relevant SORN(s), including link(s) if practicable.

Attachment B

Privacy and Security Controls

DOC Minimum Privacy Continuous Monitoring Controls	
ID	**Privacy Controls Required to Be Assessed Annually**
AC-3	Access Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-17	Remote Access
AC-19	Access Control for Mobile Devices
AC-21	Information Sharing
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AU-2	Audit Events
AU-6	Audit Review, Analysis, and Reporting
IA-2	Identification and Authentication
MP-2	Media Access
MP-3	Media Marking
MP-4	Media Storage
MP-5	Media Transport
SC-8	Transmission Confidentiality and Integrity
SC-28	Protection of Information at Rest
SE-1	Inventory of Personally Identifiable Information
SI-4	Information System Monitoring

DOC Minimum Security Continuous Monitoring Controls	
ID	**Security Controls Required To Be Assessed Annually**
AC-2	Account Management
AC-18	Wireless Access
AU-3	Content of Audit Records
AU-6	Audit Review, Analysis, and Reporting
CM-4	Security Impact Analysis
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan
CP-2	Contingency Plan
CP-4	Contingency Plan Testing
PL-1	Security Planning Policy and Procedures
PL-2	System Security Plan

RA-3	Risk Assessment
RA-5	Vulnerability Scanning

DOC Appendix J Privacy Control Allocation Table

ID	Privacy Controls	Identified Control Type
AP-1	Authority to Collect	System
AP-2	Purpose Specification	System
AR-1	Governance and Privacy Program	Common
AR-2	Privacy Impact and Risk Assessment	System
AR-3	Privacy Requirements for Contractors and Service Providers	Hybrid
AR-4	Privacy Monitoring and Auditing	Hybrid
AR-5	Privacy Awareness and Training	Hybrid
AR-6	Privacy Reporting	Common
AR-7	Privacy-Enhanced System Design and Development	System
AR-8	Accounting of Disclosures	System
DI-1	Data Quality – Hybrid	System
DI-2	Data Integrity and Data Integrity Board	System
DM-1	Minimization of Personally Identifiable Information	System
DM-2	Data Retention and Disposal	System
DM-3	Minimization of PII Used in Testing, Training, and Research	Hybrid
IP-1	Consent	System
IP-2	Individual Access	Hybrid
IP-3	Redress	System, unless decision made to determine process at enterprise level, then Hybrid
IP-4	Complaint Management	Hybrid
SE-1	Inventory of Personally Identifiable Information	Hybrid
SE-2	Privacy Incident Response	Hybrid
TR-1	Privacy Notice	System
TR-2	System of Records Notices and Privacy Act Statements	System
TR-3	Dissemination of Privacy Program Information	Common
UL-1	Internal Use	System
UL-2	Information Sharing with Third Parties	System

Attachment C -
Departmental Privacy Standards for
Commerce Data Loss Prevention Security Tools

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

APR 15 2016

MEMORANDUM FOR: Heads of Operating Units and Secretarial Officers

FROM: Catrina D. Purvis
Senior Agency Official for Privacy (SAOP) &
Chief Privacy Officer

Ellen Herbst *Ellen Herbst*
Chief Financial Officer &
Assistant Secretary for Administration

SUBJECT: Departmental Privacy Standards for Commerce Data Loss Prevention (DLP) Security Tools

The purpose of this memorandum is to establish a requirement for all bureaus/operating units (BOUs) to configure their Data Loss Prevention (DLP) security tools to implement privacy control capabilities that meet Departmental privacy DLP standards. This requirement will enhance privacy protections and reduce personally identifiable information (PII) breaches within Commerce.

BACKGROUND

DLP is a term that refers to both the policy and information security tools used to identify, restrict, monitor, and protect sensitive data in use, in motion, and at rest. DLP security tools detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, without authorization. On July 7, 2010, Departmental guidance announcing the implementation of a DLP program was issued in a document titled "Immediate Enablement of a DLP Security Tool."

On December 17, 2014, the Commerce Privacy Council's DLP Working Group (commissioned by the then-General Counsel) produced a *Privacy DLP Working Group Recommendations Report*. In furtherance of the 2010 guidance, the report recommended requiring all BOUs to implement DLP-based privacy control capabilities and provided minimum privacy DLP standards for electronic transmissions of sensitive PII (incoming and outgoing email messages or internet postings). Implementation of these standards results in all unsecured electronic transmission of sensitive PII attempts on any Commerce system to be blocked and redirects senders to use an approved secured transmission method. Many BOUs have implemented the recommended privacy DLP standards across all of their systems and others have made significant progress toward that end. This memorandum formally requires all BOUs to implement privacy DLP capabilities that satisfy the existing minimum standards set forth in the working group's attached report.

REQUIRED ACTIONS

Accordingly, the following actions are required and must be submitted to the Commerce Senior Agency Official for Privacy at CPO@doc.gov within 120 days from the date of this memorandum:

- BOUs with existing DLP security tool capabilities – Provide a confirmation email that the minimum privacy DLP control standards identified in the DLP Working Group Report have been implemented.
- BOUs with no existing DLP security tool capabilities – Provide an implementation plan to meet the minimum Privacy DLP Standards within one (1) year. (The implementation plan may propose an alternative method/process to achieve the standards).

Please direct any questions regarding this memorandum to Lisa Martin, Deputy Director of Departmental Privacy Operations, who can be reached at (202) 482-2459 and lmartin1@doc.gov.

cc: BOU Chief Privacy Officers
Chief Information Officers
Chief Financial Officers

Attachment:
DOC Privacy DLP Working Group Recommendations

United States Department of Commerce

Office of Privacy & Open Government

Privacy Program

Privacy Data Loss Prevention (DLP) Working Group Recommendations

December 17, 2014

DOC Privacy DLP Working Group Members:

Byron Crenshaw (Chair) – Census
Stephen Edwards, USPTO
Jun Kim, DOC
Ida Mix, BIS
Carolyn Schmidt, NIST
Solanki Shashikant, BEA
Eric Williams, NOAA

Office of Privacy and Open Government
Privacy Data Loss Prevention Working Group
Recommendations

Table of Contents

SUMMARY

This document contains recommendations from the Department of Commerce (DOC) inter-agency network based Privacy Data Loss Prevention (DLP) Working Group for implementing a DOC wide DLP privacy program. Information in this recommendation will change as we gain greater experience using DLP email scan, new technologies are introduced, and new OMB requirements are implemented. As a result, it is the recommendation of the Privacy DOC DLP Working Group that these recommendations be reviewed annually and updated as appropriate.

The DOC inter-agency Privacy DLP Working Group was commissioned to research, investigate, and propose recommendations for implementing a department wide DLP privacy program. The group's primary objective was to provide high-level recommendations for a department wide DLP privacy program that will minimize the number of sensitive personally identifiable information (PII) email incidents while considering the level of technical, human, and financial resources needed to implement a DLP privacy program. DLP accomplishes these tasks using automated tools that implement policies and processes to identify where sensitive information is stored throughout the department's network, restrict access to that sensitive information, and monitor transmission of sensitive data in and out of the network boundary.

The privacy DLP working group consisted of a small group of privacy advocates from the Department of Commerce, the Bureau of Industry and Security (BIS), the Bureau of Economic Analysis (BEA), the U.S. Census Bureau, the National Oceanic and Atmospheric Administration (NOAA), the National Institute of Standards and Technology (NIST), and the U.S. Patent and Trademark Office (USPTO). Byron Crenshaw, Privacy Compliance Chief of the U.S. Census Bureau, chaired this group.

This document describes the following recommendations from the Privacy DLP Working Group:

1. Security/Sensitivity Classification of DLP Personnel
2. Department-wide Privacy DLP Standard Process
3. DLP Minimum Scanning (filtering) Configuration – Incoming & Outgoing Mail
4. Filtering Criteria
5. Internet Postings
6. Handling of False Positives
7. Email Message Alerts to the Email Sender
8. Implementation Plan & Deadline
9. Reporting Requirements

SCOPE

The recommendations of this document are for all unencrypted HTTP entities and messaging traffic (incoming or outgoing email messages or internet postings) that are leaving or entering a DOC network.

RECOMMENDATIONS

1. Security/Sensitivity Classification of DLP Personnel

Standard DLP operating procedures may allow DLP personnel access to confidential and/or sensitive information pertaining to persons, government or private entities. The DOC Privacy DLP Working Group recommends that DLP personnel sign a non-disclosure form prior to working with DLP technologies, acknowledging the requirements and responsibilities for information that is handled and made available. In addition, agencies may consider conducting additional security/suitability clearances for personnel involved with DLP.

2. Department-Wide DLP Standards

It is the recommendation of the DOC Privacy DLP Working Group that the DOC adopt the following practice as standard DLP privacy operating procedures:

- all unencrypted electronic messages (email messages or internet postings) that are leaving or entering a DOC network be filtered through the DLP solution (minimum scanning configuration is described in Section 3);
- suspected sensitive PII detected by the DLP shall be quarantined for a specified number of days as determined by the department or the OU;
- for each day an email is stored in quarantined, the email sender shall be sent an auto-generated email message from the DLP stating that his/her email will be deleted on [specified date] unless action is taken;
- if no action is taken on email messages quarantined by the DLP within the pre-determined number of days, the email message shall be deleted and the sender shall be notified;
- to resolve a suspected false positive, the email sender can either:
  - retransmit the email message with proper encryption,
  - redact the message of all sensitive information and retransmit, or,
  - contact the privacy staff to resolve suspected false positive (described in Section 6 – Handling of False Positives).

3. DLP Minimum Scanning Configuration

A successful department wide DLP privacy program must begin with a standard set of personally identifiable information (PII) items that each operating unit must consistently treat with special handling procedures during electronic transmission. The identification of sensitive PII is often based on the context of how the information is used. Since there are limitations on contextual understanding by DLP software, the list of sensitive PII identified by the DOC inter-agency Privacy DLP Working Group will consist primarily of single (standalone) sensitive PII items, with some basic grouping or combination of other PII or commonly associated text. Examples of these items are listed in Table 1.

A. Egress Scanning

It is the recommendation of the DOC Privacy DLP Working Group that all outgoing email messages sent from a DOC network be subject to DLP filtering for sensitive PII based on the minimum filtering criteria as outlined in this document.

Note on Agencies' Rights: DOC operating units must reserve the right to add additional PII to their DLP filter as necessary. However, minimum DLP items identified by the DOC DLP Team cannot be detracted.

B. Ingress Scanning

Historical research by DOC operating units that are currently using a DLP software has revealed that incoming email messages will sometime contain sensitive PII which can go undetected by the operating unit. It is not until the operating unit attempts to reply or forward the message outside of the DOC network that the sensitive PII in the e-mail message is detected. It was also revealed that sometimes the incoming e-mail message will be copied and filed in an unsecure environment because the sensitive PII within the e-mail message remained undetected.

To address this problem, it is the recommendation of the DOC Privacy DLP Working Group that all e-mail messages coming into DOC networks be subject to the same DLP filtering criteria as outgoing email messages. Incoming e-mail messages containing sensitive PII as identified by the DLP filtering scan shall be blocked by the DLP from entering the DOC network. It is recommended that electronic notification be sent to the sender describing the policy prohibition, with instructions for using DOC approved encryption software (i.e., Accellion). In addition, it is also recommended that the intended recipient of the blocked email message be electronically notified that an incoming e-mail message has been blocked from receipt into the DOC network because of a possible DLP policy prohibition. Recommended suggestions for the wording of these notification messages are included in Appendix A.

4. Filtering Standard

The DOC Privacy DLP Working Group has identified a minimum standard for DLP privacy implementation. This filtering standard includes sensitive PII, and non-sensitive PII combined with other information, such as financial and/or medical information, which when combined, becomes sensitive PII.

DOC operating units must include these items in the standard filters of their DLP filtering items, additional filtering items can be added by DOC operating units as necessary.

If a quarantined message matches for more than one DLP filter item, the DLP scanning rules should terminate examination and trigger countermeasures on the first matching item.

It is the recommendation of the DOC Privacy DLP Working Group that the DLP filtering hierarchy be in this order.

1. Social security number
2. Passport number
3. Driver's license/state identification number
4. Bank account/credit card number
5. Medical/HIPAA Information
6. Date of birth
7. Mother's maiden name

This order means if there is an email message that has content that recognize the SSN and HIPPA Patient Identification Number, the DLP would recognize the SSN as the violation and not continue processing for the HIPAA Patient Identifier.

4.1 U.S. Social Security Number Filters

The U.S. Social Security Number classifier requires a properly formatted number as well as other supporting data, such as a date of birth, name, or the text string "SSN".

U.S. SSN Examples:

- 123-45-6789 (No match because of no supporting information)
- 123-45-6789 July 4 (Match because a partial date is linked to 9-digit string number)
- 123-45-6789 7/4/1980 (Match because a possible date is linked to 9-digit string number)
- 123-45-6789 7/4 (No match)
- 123-45-6789 987-65-4321 (Match because of more than one 9-digit string number increases risk, threat, and harm)
- SSN: 123-45-6789 (Match)
- Joe Smith 123-45-6789 (Match because name linked to 9-digit number)
- 123-45-6789 CA 94066 (Match because state and zip code associated with 9-digit number)

4.2 Passport Number

The Passport Number filter requires inspection for the word "Passport," in English and Spanish, followed by a string of digits.

4.3 Driver's License/State Identification Number

Driver's license or other state identification number must be filtered by the words "Driver's License" or "State Identification," followed by a string of numeric or alphanumeric values.

String of numeric data including punctuation (dashes, periods, etc.).

4.4 Financial Account/Credit Card Number

The words “routing,” “accounting,” “credit card,” or “cc,” followed by a string of numbers with or without dashes.

4.5 Medical and Health Insurance Portability and Accountability (HIPAA) Filters

It is the recommendation of the DOC Privacy DLP Working Group that medical and other HIPAA considerations be included in the DLP data dictionary. The Medical/HIPAA DLP scan shall require a match on the medical classifier AND a match on a personal information identifier such as full name, U.S. Social Security Number, U.S. National Provider Identifier, or custom patient identification number, to be considered a Medical/HIPAA DLP violation.

Medical Information Examples:

personal identifier such as, full name, SSN, national provider identifier, or custom patient identification number -

- ADHD
- AIDS
- Arthritis
- Asthma
- Autism
- Cancer
- Chlamydia
- Diabetes
- Epilepsy
- Flu (Influenza)
- Herpes
- Giardiasis
- Gonorrhea
- Heart Disease
- Hepatitis
- HIV
- HPV (Human papillomavirus)
- Influenza
- Meningitis
- MRSA (Methicillin Resistant Staphylococcus aureus)
- Obesity
- Salmonella
- Scabies

- Sexually Transmitted Diseases
- Stroke
- Trichomonas
- Trichomoniasis
- Tuberculosis (TB)

4.6 Date of Birth

Date of birth filter must include a combination of numeric or alphanumeric dates associated with the words "date of birth", "DOB", or "birth date," and must be linked with a unique personal identifiable such as name or social security number.

5. Internet Postings

Sensitive PII posted for consumption via private or public websites can present a much greater risk of harm than sensitive PII transmitted through email because of the potential for a wider audience and exposure. It is the recommendation of this group that Internet traffic be scanned for DLP filtering items. This includes posts from DOC controlled networks going out to official DOC social media websites and pages, and posts inbound to DOC controlled and monitored websites and pages, i.e., Web forums. Attempted postings containing information prohibited by DLP filter criteria shall be blocked from release on the DOC controlled websites and pages, to the Internet.

6. Handling of False Positives

For the purpose of this recommendation, a "false positive" is defined as an electronic message that was falsely quarantined by the DLP solution.

If a sender suspects that his/her email message has been falsely quarantined by the DLP, it is the recommendation of the DOC Privacy DLP Working Group that the following actions be taken:

- the sender shall notify the privacy staff of the suspected false positive;
- a privacy professional will review the email to determine if the quarantined email message is a DLP false positive;
- upon confirmation by privacy professional that the email message was falsely quarantined by the DLP, the email message will be released by the privacy professional to the addressee(s);
- the sender shall be notified that the message has been reviewed by a privacy staff member and released to the intended recipient(s).

If the privacy professional determines that the email message is not a false positive, i.e., contains PII that is prohibited from unencrypted electronic transmission, it is the recommendation of this group that the following actions be taken:

- the email message will be manually deleted by the privacy staff;
- the sender will be notified that the message has been reviewed by a privacy staff member and found to contain information that is prohibited by policy from unencrypted email transmission.

If no action is taken by the sender for a message that has been quarantined by the DLP after a specified number of days (as defined by either the department or the OU), it is the recommendation of this group that the following actions be taken:

- the email message be automatically deleted by the DLP solution;
- the sender shall receive an auto-generated email message from the DLP solution stating that the email message [email subject and date] has been deleted by the DLP.

7. Email Messages

It is the recommendation of the DOC Privacy DLP Working Group that when an email message is quarantined by the DLP email scan, the sender shall receive an auto-generated email message describing the possible violation, the quarantine of the email message, and the steps to take to release the email message to the intended recipients. If the employee suspects the DLP quarantined the email in error (false positive) and contacts the privacy office for assistance, another email message will be sent stating the results of the privacy review. An example of each of these letters is included under the Email Messages section of the Appendix A.

8. Implementation Plan & Deadline

It is the recommendation of the DOC Privacy DLP Working Group that a department-wide policy be written based on these recommendations. All DOC operating units shall be given one year from date of issue to comply with the policy.

9. Reporting Requirements

Incidents captured by the DLP are not released from a DOC controlled environment. Since they remain within the control of the DOC, the DOC Privacy DLP Working Group recommends that DLP incidents be considered an attempted violation of policy and not an actual breach. Therefore, DLP incidents shall not be required for CIRT reporting.

To monitor the effectiveness of the DLP program, it is the recommendation of the DOC Privacy DLP Working Group that all operating units maintain record of the number of incidents captured by the DLP, the number of false positives, the number of avoid breaches, and the number of attempted self disclosed sensitive information.

Table 1
Examples of Specific Sensitive Items

Item	Sensitive By Itself	Sensitive When Combined With Other Identifying Information
Name		X
Address		X
Telephone (cell/land)		X
Date of Birth		X
Mother's maiden name		X
Social Security Number	X	
Bio-metric (fingerprint, palm print, hand geometry, iris recognition, retina, etc.)		X
Medical information, except brief references to absences from work		X
Passport Number		X
Bank Account/Credit Card Number or Account	X	
Driver's license/state identification number		X
Potentially sensitive employment information, e.g., personnel ratings, disciplinary actions, and results of background investigations		X
Criminal history		X
Any information that may stigmatize or adversely affect an individual		X

This list is not exhaustive, and other data may be sensitive depending on specific circumstances. Social Security Numbers, including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual.

Appendix A

Related Laws, Regulations, Policies, and Documents

- Privacy Act of 1974
- U.S. Department of Commerce Office of the Chief Information Officer, Electronic Transmission of Personally Identifiable Information
- U.S. Department of Commerce Office of the Chief Information Officer, IT Privacy Policy
- Office of Management and Budget Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- Office of Management and Budget Memorandum M-06-19, Reporting Incidents Involving PII
- Office of Management and Budget Memorandum M-06-16, Protection of Sensitive Agency Information
- Office of Management and Budget Memorandum M-06-15, Safeguarding PII
- Commerce CIO's Memorandum on Safeguarding PII

Table 2

DLP Solutions by DOC Operating Unit

	None	RSA	Iron Port	ScanMail	Secure Zip (Google cloud solution)	Trend Micro	Websense	Axways
BEA						X		
BIS	X							
Census			X					
DOC							X	
NIST	X							
NOAA	X							
PTO				X				X[1]

[1] Used for email messages coming and going to the internet.

Appendix B

Email Messages

Employees can potentially receive two of the three DLP email messages:

1. **Message #1 - alerts the user that his/her message, and if appropriate any attachments, have been quarantined by the DLP. This message is to be sent each day until the quarantined email is either released by the privacy office or deleted.**

   EXAMPLE

   Subject: Email Message Temporarily Quarantined: [original email subject with date]

   *A scan by the **[insert name of agency]** Data Loss Prevention (DLP) system has detected that your email with the subject: **[subject]**, dated **[date email was sent]** may contain sensitive information that by policy is prohibited from email transmission without proper encryption. As a result, your email has been placed in quarantine for [specified] days. Please take one of the following actions to resolve this issue:*

   1. *Re-transmit your message using approved email encryption; or,*
   2. *Contact the privacy staff on (777) 777-7777, if you think your email was quarantined by the DLP email scan in error.*

   *Sending unencrypted email messages containing sensitive PII, including personal messages sent from a Department of Commerce email systems, is a violation of the Department of Commerce's "Electronic Transmission of Personally Identifiable Information" policy. Additional information regarding acceptable use of government IT systems is contained in the **[insert the name of agency's IT Acceptable Use Policy]**. A copy of this policy can be found on **[insert http address]**.*

   *In the future, to avoid delays in email transmissions, please ensure that emails containing sensitive personally identifiable information or sensitive financial information are transmitted using approved encryption software, such as Accellion – Secure File Sharing software, or other approved secure transmission **[insert link to other encryption software approved by the agency]**.*

   *Please direct any questions to the **[insert privacy office's name and telephone number]**.*

2 **Message #2 – is sent to the email sender who requested review by a privacy professional because a false positive is suspected, and after review, the message is released to the intended recipients.**

EXAMPLE

Subject: Email Message Temporarily Quarantined: [original email subject with date]

YOUR EMAIL MESSAGE HAS BEEN SENT

The below email has been reviewed by the ***[name of agency's privacy office]*** *and released to the intended receiver(s) on [date original message released].*

If you have any questions, please contact the ***[insert privacy office's name and telephone number]****.*

3. **Message #3 - alerts the user that his/her email message, and any attachments, has been deleted and not sent. This message is to be sent after a quarantined message has not been acted upon after the pre-determined period of time.**

EXAMPLE

Subject: Email Message Temporarily Quarantined: [original email subject with date]

The detention period of your quarantined email message has expired and your message has been deleted. Your message was not sent to the intended recipient.

Sending unencrypted email messages containing sensitive PII, including personal messages sent from a Department of Commerce email systems, is a violation of the Department of Commerce's "Electronic Transmission of Personally Identifiable Information" policy. Additional information regarding acceptable use of government IT systems is contained in the ***[insert the name of agency's IT Acceptable Use Policy]****. A copy of this policy can be found on* ***[insert http address]****.*

In the future, to avoid delays in email transmissions, please ensure that emails containing sensitive personally identifiable information or sensitive financial information are transmitted using approved encryption software, such as Accellion – Secure File Sharing software, or other approved secure transmission ***[insert link to other encryption software approved by the agency]****.*

Please direct any questions to the ***[insert privacy office's name and telephone number]****.*

Appendix C

DEFINITIONS

Business Identifiable Information (BII): consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal "basic commercial operations" but includes any records [or information] in which the submitter has a "commercial interest" and can include information submitted by a nonprofit entity. Or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C. 9).

False Positive: messages quarantined by the DLP that were later determined to not have contained any information that is prohibited from electronic transmission.

Personally Identifiable Information (PII): OMB Memorandum M-07-16 states that PII "refers to information which can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Sensitive But Unclassified (SBU): is a designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. It also includes Internal Revenue Service materials like individual tax records, systems information, and enforcement procedures. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not.

Sensitive Personally Identifiable Information (SPII): Department of Commerce's policy on Electronic Transmission of PII states that "sensitive PII is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Further, in determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a government newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. As well as context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother's maiden name, but each of these elements would not be sensitive independent of one another."

Sensitive Security Information (SSI): is a category of sensitive but unclassified information under the United States government's information sharing and control rules, often used by TSA and CBP. SSI is information obtained in the conduct of security activities whose public disclosure would, in the judgment of specified government agencies, harm transportation security, be an unwarranted invasion of privacy, or reveal trade secrets or privileged or confidential information.

UNCLASSIFIED/FOUO: is used for documents or products that contain material that is exempt from release under the Freedom of Information Act. It is treated as confidential, which means it cannot be discarded in the open trash, made available to the general public, or posted on an uncontrolled website. It can, however, be shared with individuals with a need to know the content, while still under the control of the individual possessing the document or product.

UNRESOLVED ISSUES

Issue 1: Identify BII DLP requirements.

Resolution: Pending

Issue 2: How to resolve false positives of incoming email messages?

Resolution: Pending

RESOLVED ISSUES

Issue 1: Definition of a DLP breach:

Resolution: The official OMB definition of a breach is *"The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic."*

The loss of PII email incidents captured by the DLP shall not be considered breaches since the email containing the PII has never left our control.

Issue 2: Treatment of truncated IDs (SSNs, Passports numbers, credit card numbers, etc.)

Resolution: Page 2 of the Department of Commerce Policy on the Electronic Transmission of Personally Identifiable Information states the following:

"Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed."

The treatment of truncated SSNs will be handled in accordance with the official DOC policy until such time when this requirement is rescinded by the department.

Other truncated numbers, i.e., passport numbers, credit card numbers, shall not be considered sensitive unless it is accompanied by other identifying information. (This adds to the DOC policy, since the policy does not address the use of truncated numbers other than SSN).

Issue 3: How to handle DLP incidents flagged after hours.

Resolution: The automated email alert will immediately notify the sender that his/her email message has been quarantined. The message shall provide instructions for the sender to re-transmit the email using approved encryption software or through Accellion to successful transmit the email. Secure FTP.

Issue 4: Treatment of incoming messages containing sensitive PII.

Resolution: The Privacy DLP Working Group recommends incoming messages be subject to DLP filtering, however, the decision to flag and quarantine incoming email messages containing sensitive PII shall be at the discretion of each operating unit.

Issue 5: Treatment of messages posted on agency's social media site

Resolution: Traffic to the internet should be considered.

Issue 6: Shall we consider one DLP solution for all DOC OUs?

Resolution: No. Each operating unit must be able to employ a DLP solution that is compatible with existing technical capabilities and polices.

Attachment D
Summarized Information on DOC Privacy Overlays

Implementing Privacy Overlays

Introduction

This document is comprised of four Privacy Overlays that identify security and privacy control specifications required to protect personally identifiable information (PII), including protected health information (PHI), in DOC systems and reduce privacy risks to individuals throughout the information lifecycle.[1] The Privacy Overlays support implementation of but are not intended to, and do not, supersede privacy requirements of statute, regulation, or Office of Management and Budget (OMB) policy.

Since the Privacy Act of 1974 established the requirement for "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" and "to protect… the integrity" of systems, both the technology and threats thereto have evolved and organizations have had to change the way they protect their information.[2] The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4 provides the underlying controls necessary to protect PII processing systems within DOC. Based on the Fair Information Practice Principles (FIPPs)[3] and federal privacy requirements, these Privacy Overlays provide a consistent approach for ensuring implementation of "appropriate administrative, technical, and physical safeguards" to protect PII in information systems irrespective of whether the PII is maintained as part of a system of records.[4] The Privacy Overlays provide a method within existing NIST structures to implement the security and privacy controls necessary to protect PII in today's technology-dependent world.

All PII is not equally sensitive and therefore all PII does not require equal protection. PII with higher sensitivity requires more stringent protections, while PII with lower sensitivity requires less stringent protections. There are three overlays that address the varying sensitivity of PII; Low, Moderate, and High. PHI is a subset of PII and in addition to sensitivity considerations, PHI requires a minimum set of protections that are based on the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Rules. Therefore, PHI is addressed under a fourth overlay, which is applied on top of the Privacy Overlay determined by the sensitivity of the PHI, i.e., Low, Moderate, or High.

[1] For additional information about PII and PHI, see Section 7, "Definitions."

[2] "Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any unanticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. §552a(e) (10).

[3] Committee Report No. 93-1183 to accompany S. 3418 (Sep 26, 1974), p 9.

[4] "[A system of records is] a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. §552a(a)(5).

Overlays Summary

The table contains a summary of the security and privacy control specifications as they apply in the Privacy Overlays. The detailed specifications and tailoring considerations for each control can be found in the sections that follow. The symbols used in the table are as follows:

- A plus sign ("+") indicates the control should be selected.
- Two "dashes" ("--") indicates the control should not be selected.[18]
- The letter "E" indicates there is a control extension.[19]
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter "V" indicates this overlay defines a value for an organizational-defined parameter for the control.
- The letter "R" indicates there is at least one regulatory/statutory reference that affects the control selection or that the control helps to meet the regulatory/statutory requirements.

Controls that include an E, G, V, or R specification without a "+" or a "--" are not required, but they do have privacy implications when implemented for other reasons. Please see the Tailoring Considerations section for more information regarding these specifications.

[18] AC-2(8) includes regulatory/statutory references that prohibit its selection of this control for systems that maintain PII with a PII Confidentiality Impact Level of Moderate or High and for PHI.

[19] Control extensions will be submitted to NIST for consideration when updating the NIST SP 800-53 catalog.

Table: Privacy Overlays Security and Privacy Controls

CONTROL	PRIVACY OVERLAS			
	PII Confidentiality Impact Level			PHI
	LOW	MODERATE	HIGH	
AC-1	+GR	+GR	+GR	+ER
AC-2	+EGVR	+EGVR	+EGVR	+EGR
AC-2(8)		--R	--R	
AC-2(9)	GVR	GVR	GVR	R
AC-2(13)	+R	+R	+R	+R
AC-3	+EGR	+EGR	+EGR	+GR
AC-3(9)		+EVR	+EVR	+R
AC-3(10)	GVR	GVR	GVR	
AC-4		+GR	+GR	+R
AC-4(8)			+VR	
AC-4(12)				+GR
AC-4(15)		+GR	+GR	+R
AC-4(17)		+GVR	+GVR	
AC-4(18)		+GR	+GR	+R
AC-5		+GR	+GR	+GR
AC-6		+GR	+GR	+GR
AC-6(1)			+GR	+R
AC-6(2)		+GR	+GR	+R
AC-6(3)			GR	
AC-6(5)			+R	+R
AC-6(7)	+VR	+VR	+VR	+VR
AC-6(9)		+R	+R	+R
AC-6(10)		+R	+R	
AC-8	GR	GR	GR	GR
AC-11	+EVR	+EVR	+EVR	+GR
AC-12				+GR
AC-14		GR	GR	GR
AC-16	+GVR	+GVR	+GVR	+GVR
AC-16(3)	+GVR	+GVR	+GVR	+GVR
AC-17	+GR	+GR	+GR	+GR
AC-17(1)	+GR	+GR	+GR	+R
AC-17(2)	+R	+R	+R	+GR
AC-18(1)	+GR	+GR	+GR	
AC-19	+ER	+ER	+ER	+GR

	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
CONTROL	LOW	MODERATE	HIGH	PHI
AC-19(5)	+EVR	+EVR	+EVR	+GVR
AC-20	+EGR	+EGR	+EGR	+R
AC-20(1)	+R	+R	+R	+R
AC-20(3)	+EGVR	+EGVR	+EGVR	
AC-21	+GR	+GR	+GR	+GR
AC-22	+GR	+GR	+GR	+R
AC-23	EGR	EGR	EGR	
AT-1	+GR	+GR	+GR	+R
AT-2	+ER	+ER	+ER	+GR
AT-3	+ER	+ER	+ER	+R
AT-4	+GR	+GR	+GR	+R
AU-1	+GVR	+GVR	+GVR	+R
AU-2	+GVR	+GVR	+GVR	+GR
AU-3	+GR	+GR	+GR	+R
AU-4		+GR	+GR	+R
AU-4(1)		GR	GR	R
AU-6		+GR	+GR	+R
AU-6(3)		+R	+R	
AU-6(10)		+GR	+GR	
AU-7	+R	+R	+R	+R
AU-7(1)		+R	+R	+R
AU-7(2)		+R	+R	+R
AU-9	+GR	+GR	+GR	+R
AU-9(3)		+GR	+GR	+GR
AU-9(4)		GR	GR	
AU-10		+GR	+GR	+R
AU-10(1)		+GR	+GR	+R
AU-11(1)		GR	GR	
AU-12		+R	+R	+R
AU-12(3)		+VR	+VR	+VR
AU-14		GR	GR	
AU-14(2)		GR	GR	
AU-14(3)		GR	GR	
AU-16(2)				+GVR
CA-1	+GR	+GR	+GR	+R

	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
CONTROL	LOW	MODERATE	HIGH	PHI
CA-2	+GR	+GR	+GR	+VR
CA-3		+R	+R	+GVR
CA-3(3)	+VR	+VR	+VR	+R
CA-3(5)	+VR	+VR	+VR	+R
CA-6	+EGR	+EGR	+EGR	+GR
CA-7		+GR	+GR	+GR
CA-8			+GVR	
CA-9		+GVR	+GVR	+VR
CA-9(1)		+GR	+GR	+R
CM-3(6)	+GVR	+GVR	+GVR	+GVR
CM-4	+GR	+GR	+GR	+R
CM-4(1)		+GR	+GR	
CM-4(2)		+R	+R	+R
CM-8(1)				+R
CP-1	+R	+R	+R	+R
CP-2	+R	+R	+R	+GR
CP-2(5)				+R
CP-2(8)				+GR
CP-4				+GR
CP-7		GR	GR	GVR
CP-9		+ER	+ER	+ER
CP-10		+R	+R	+R
IA-2	+R	+R	+R	+R
IA-2(6)		+GR	+GR	
IA-2(7)		+GR	+GR	
IA-2(11)		+GR	+GR	
IA-3				+R
IA-4	+ER	+ER	+ER	+GR
IA-4(3)		+GR	+GR	
IA-5		+R	+R	+GR
IA-6				+GR
IA-7	+GR	+GR	+GR	+GR
IA-8		+R	+R	+R
IR-1	+GVR	+GVR	+GVR	+GR
IR-2	+GR	+GR	+GR	+GR

	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
CONTROL	LOW	MODERATE	HIGH	PHI
IR-4	+GR	+GR	+GR	+GR
IR-4(3)				+EVR
IR-5	+GR	+GR	+GR	+R
IR-6	+GVR	+GVR	+GVR	+R
IR-7	+GR	+GR	+GR	+R
IR-8	+GR	+GR	+GR	+GR
IR-10	+GR	+GR	+GR	
MA-1		+ER	+ER	+GR
MA-2				+GR
MA-4(6)	+R	+R	+R	+R
MA-5	+GR	+GR	+GR	+GR
MP-1	+VR	+VR	+VR	+VR
MP-2	+VR	+VR	+VR	+VR
MP-3	+GR	+GR	+GR	+GR
MP-4	+VR	+VR	+VR	+R
MP-5	+VR	+VR	+VR	+VR
MP-5(4)	+R	+R	+R	+GR
MP-6		+GVR	+GVR	+VR
MP-6(1)	+GR	+GR	+GR	+GR
MP-6(8)		+GR	+GR	
MP-7		+GVR	+GVR	
MP-7(1)		+R	+R	
MP-8(3)		+VR	+VR	+GVR
PE-1				+R
PE-2	+R	+R	+R	+GR
PE-2(1)				+GR
PE-3	+R	+R	+R	+R
PE-4				+GR
PE-5	+GR	+GR	+GR	+GR
PE-6				+GR
PE-8				+GR
PE-17	+GR	+GR	+GR	
PE-18			+GR	+GR
PL-1				+ER
PL-2	+EGR	+EGR	+EGR	+R

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			PHI
	LOW	MODERATE	HIGH	
PL-4	+ EGR	+EGR	+EGR	
PL-8	+GR	+GR	+GR	
PS-1	+ER	+ER	+ER	+R
PS-2	+ER	+ER	+ER	+GR
PS-3	+ER	+ER	+ER	+GR
PS-3(3)	+GVR	+GVR	+GVR	+GR
PS-4	+GR	+GR	+GR	+GR
PS-5	+ER	+ER	+ER	+GR
PS-6	+GR	+GR	+GR	+R
PS-7	+GR	+GR	+GR	+R
PS-8	+EGR	+EGR	+EGR	+R
RA-1	+EGR	+EGR	+EGR	+R
RA-2	+ER	+ER	+ER	+R
RA-3	+EGVR	+EGVR	+EGVR	+GVR
SA-2	+ER	+ER	+ER	
SA-3	+GR	+GR	+GR	
SA-4	+EGR	+EGR	+EGR	+ER
SA-8	+GR	+GR	+GR	
SA-9				+ER
SA-9(5)	+EGR	+EGR	+EGR	
SA-11		+EGR	+EGR	
SA-11(5)			+ER	
SA-15(9)		+EGR	+EGR	
SA-17	+EGR	+EGR	+EGR	
SA-21	+GVR	+GVR	+GVR	+GR
SC-2		+ER	+ER	+ER
SC-4	+GR	+GR	+GR	+R
SC-7(14)				+GVR
SC-8	+GVR	+GVR	+GVR	+VR
SC-8(1)	+EVR	+EVR	+EVR	+GR
SC-8(2)		+GVR	+GVR	
SC-12	+VR	+VR	+VR	+GR
SC-13	+VR	+VR	+VR	+GR
SC-28	+GVR	+GVR	+GVR	+R
SC-28(1)	+EGR	+EGR	+EGR	+GR

	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
CONTROL	LOW	MODERATE	HIGH	PHI
SI-1	+R	+R	+R	+R
SI-3				+GR
SI-4	+GR	+GR	+GR	+R
SI-5				+GR
SI-7	+VR	+VR	+VR	+VR
SI-7(6)	+ER	+ ER	+ ER	+ GR
SI-8				+ GR
SI-10		+VR	+ VR	
SI-11	+VR	+ VR	+ VR	+ VR
SI-12	+EGR	+EGR	+EGR	+EGR
PM-1	+GR	+GR	+GR	+R
PM-2	GR	GR	GR	+ER
PM-3	+R	+R	+R	
PM-5	+GR	+GR	+GR	+GR
PM-7	+GR	+GR	+GR	+R
PM-9	+ER	+ER	+ER	+ER
PM-10	+EGR	+EGR	+EGR	+ER
PM-11	+EGR	+EGR	+EGR	+R
PM-12	+ER	+ER	+ER	
PM-13	GR	GR	GR	R
PM-14	+EGR	+EGR	+EGR	
PM-15	+EGR	+EGR	+EGR	
AP-1	+GR	+GR	+GR	
AP-2	+GR	+GR	+GR	
AR-1	+EGR	+EGR	+EGR	+GR
AR-2	+GR	+GR	+GR	+R
AR-3	+ER	+ER	+ER	+ER
AR-4	+GVR	+GVR	+GVR	+R
AR-5	+EGR	+EGR	+EGR	+R
AR-6	+R	+R	+R	+GR
AR-7	+GR	+GR	+GR	+R
AR-8	+R	+R	+R	+GR
DI-1	+GR	+GR	+GR	
DI-1(1)		+GR	+GR	
DI-1(2)		+VR	+VR	

	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
CONTROL	LOW	MODERATE	HIGH	PHI
DI-2	GR	GR	GR	
DI-2(1)	GR	GR	GR	
DM-1	+GR	+GR	+GR	+R
DM-2	+VR	+VR	+VR	+VR
DM-2(1)				+R
DM-3	+GR	+GR	+GR	+GR
DM-3(1)	GR	GR	GR	+GR
IP-1	+GR	+GR	+GR	+GR
IP-1(1)				+R
IP-2	+GR	+GR	+GR	+ER
IP-3	+GR	+GR	+GR	+R
IP-4	+R	+R	+R	+R
IP-4(1)	GR	GR	GR	+R
SE-1	+GR	+GR	+GR	+ R
SE-2	+GR	+GR	+GR	+R
TR-1	+GR	+GR	+GR	+GR
TR-1(1)	G	G	G	GR
TR-2	+GR	+GR	+GR	
TR-2(1)	+GR	+GR	+GR	
TR-3	+R	+R	+R	
UL-1	+EGR	+ EGR	+ EGR	+R
UL-2	+ EGR	+ EGR	+ EGR	+ GR