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
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

Privacy Data Loss Prevention (DLP) Working Group Recommendations

December 17, 2014

Byron C
Stephen E
Jun Kim, D
Ida Mix, BI
Carolyn Sc
Solanki Sh
Eric Willia

Commerce Interagency
Privacy Data Loss Prevention Working Group
Recommendations

Table of Contents

Commerce Interagency
Privacy Data Loss Prevention Working Group
Recommendations

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 Privacy 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

Commerce Interagency
Privacy Data Loss Prevention Working Group
Recommendations

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 SNN 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 strong 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 of 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

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.

Table 2

DLP Solutions by DOC Operating Unit

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

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

Commerce Interagency
Privacy Data Loss Prevention Working Group
Recommendations

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

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 gas 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.

Commerce Interagency
Privacy Data Loss Prevention Working Group
Recommendations

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 lost 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.