



U.S. Department of Justice

Office of the Deputy Attorney General

Associate Deputy Attorney General

Washington, D.C. 20530

December 3, 2015

The Honorable Carolyn N. Lerner
Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW – Suite 300
Washington, DC 20036-4505

Re: OSC File No. DI-15-4560

Dear Ms. Lerner,

This is in response to your letter of July 16, 2015, regarding a whistleblower disclosure alleging that employees of the U.S. Marshals Service (USMS), Tactical Operations Division (TOD), engaged in conduct that may constitute a violation of law, rule, or regulation; gross mismanagement; and an abuse of authority. Specifically, the whistleblower, who chose to remain anonymous, alleged that TOD employees failed to follow appropriate procedures for safeguarding and disposing of Personally Identifiable Information (PII) in violation of the Privacy Act of 1974, and Department of Justice (DOJ) policies and procedures.

At the direction of the Attorney General, USMS Acting Director L. David Harlow appointed the USMS Office of Professional Responsibility (USMS OPR) to lead an investigation into the allegations made by the whistleblower. The investigative report (Report), dated November 30, 2015, is attached. It should be noted that the Attorney General has delegated me the authority to review and sign the report in accordance with 5 U.S.C. § 1213(d).

Sincerely,

A handwritten signature in blue ink, appearing to read "R. A. Prober".

Raphael A. Prober
Associate Deputy Attorney General

Enclosure

AGENCY REPORT SUMMARY
5 U.S.C. 1213(c) & (d)

1. Summary of Information with Respect to which the Investigation was Initiated

By letter dated July 16, 2015, the Office of Special Counsel (OSC) notified the Department of Justice (DOJ) of a whistleblower disclosure allegation under 5 U.S.C § 1213(a), evidencing a violation of law, rule, or regulation. The allegation was made by a whistleblower who chose to remain anonymous.

The allegation made by the whistleblower was that the United States Marshals Service (USMS) Tactical Operations Division (TOD) shared drive on the USMS computer network system contained thousands of unsecured documents containing personally identifiable information (PII), and was improperly accessible by current and former USMS employees and contractors. In addition, OSC stated that unsecured PII was an agency wide issue based on the corrective actions recommended in the previous USMS investigative response (OSC File No. DI-14-1514) to the whistleblower allegations concerning unsecured PII on the USMS Investigative Operation Division's (IOD) shared drive.

The following information in this report substantiates the claim that PII was not appropriately safeguarded on TOD shared drives, identifies the investigation conducted by the USMS Office of Professional Responsibility (USMS OPR), and outlines remediation measures taken by TOD, as well as agency-wide measures taken by Information Technology Division (ITD), Training Division (TD), and Office of General Counsel (OGC) to prevent similar failures in the future.

2. Description of the Conduct of the Investigation

Pursuant to the delegation from the Attorney General, USMS Acting Director David L. Harlow directed the USMS OPR to conduct an independent investigation regarding the allegation that the parent directory for the TOD shared drive \\dfs-share-v01 was widely available to nearly all USMS employees and that access was not limited to authorized TOD employees. USMS OPR was granted full access to the USMS computer network system and had full authority to complete the investigation. USMS OPR's investigative report dated November 30, 2015 is attached.

USMS OPR conducted a search of every folder and subfolder within the parent directory of the TOD shared drive with the intent to locate PII. Upon determination of unsecured PII found within specific folders on TOD's shared drive, ITD was contacted and immediately restricted access. In coordination with ITD, USMS OPR confirmed that these folders were no longer accessible and also attempted to discover who may have accessed the individual files containing PII or sensitive information. Though most of the files have metadata, the data is limited to a time of access and does not identify the individual user accessing the file. There was no available system data for who may have mapped to the drives or opened files. Without the identity of a person who may have accessed the files, further examination is not possible.

3. Summary of Evidence Obtained During the Investigation

The TOD Office of Security Programs initiated an internal review to determine if TOD employees failed to follow appropriate procedures to safeguard and dispose of PII. The Chief of the TOD Office of Security Programs, determined that the claims of non-secure data and PII information were credible and specifically he found:

1. Non-secure access to names, dates of birth, Social Security Numbers (SSN) of current and former USMS operational personnel, contractors, and staff from other USMS districts and divisions;
2. Non-secure access to employee leave request forms and travel vouchers including SSNs;
3. Non-secure access to employee banking information for direct deposit purposes;
4. Non-secure access to resumes, merit promotion career board data, and awards;
5. Non-secure access to fitness tests of operational employees;
6. Non-secure access to Equal Employment Opportunity (EEO) case information; and
7. Non-secure access to Attorney General and Deputy Attorney General briefing materials.

In September 2015, the USMS OPR was directed to conduct an investigation regarding the allegation that the parent directory for the TOD shared drive \\dfs-share-v01 was widely available to nearly all USMS employees and that access was not just limited to TOD employees. USMS OPR's investigation substantiated that 15 of 58 folders within the parent folder of the TOD shared drive contained PII and other sensitive data and were accessible to USMS "authenticated users." An "authenticated user" is anyone with a Personal Identity Verification (PIV) card who uses it to access the USMS network. This means that virtually all USMS employees and contractors had access to PII within these folders even if they were unaware of this capability.

USMS OPR was not able to independently substantiate the primary allegation of who may have improperly accessed the TOD shared drive. The secondary allegation that the parent folder of the TOD shared drive, \\dfs-share-v01, was accessible to nearly all USMS employees was substantiated in that 15 of the 58 shared drives at that network location granted access to "authenticated users." At least two of the shared drives, AK-Shared and DIRStaff had security properties that allowed anyone with a PIV card to access these drives. These two drives were found to contain unsecured PII and other sensitive information.

4. Listing of Any Violation or Apparent Violation of Law, Rule, or Regulation

Inappropriate maintenance of PII is a violation of the Privacy Act, which limits access to records contained in a system of records (such as PII) to only the agency employees "who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). To constitute criminal conduct, the Act requires "knowing" violations and "willful" disclosure to another. Id. § 552a(i). For civil liability, the Act requires an "intentional or willful" violation and only awards "actual damages." Id. § 552a(g)(4).

As detailed in its Report, USMS OPR did not find evidence of a knowing, willful, or intentional violation of the Privacy Act; nor did it discover any instances of actual inappropriate access to, or disclosure of, PII from the TOD shared drive.

5. Description of Any Action Taken or Planned as a Result of the Investigation

A. Change in Agency Rules, Regulations or Practices

As detailed in the Report, TOD took immediate steps to archive or remove PII from their shared drives, limit or restrict access to PII, and actively engaged with ITD to implement training and protocols for managing PII.

As an agency, the USMS actively took steps to respond to issues with PII being inappropriately exposed on USMS shared drives. The USMS ITD and the Privacy Office within the USMS OGC developed a plan to protect PII within the agency. In general, this plan creates a folder for PII that is managed by each

USMS district and division. Access to this folder and the subfolders within it will be strictly controlled by Secure Custodians identified by the districts and divisions.

ITD has purchased a scanning tool that will search for PII that is not located within the PII folder. This tool will run on a regular basis to quickly identify PII that was not properly stored. In addition, ITD has changed folder permissions from "Full Control" to "Modify" to prevent users from using the "Authenticated Users" group in any action taken. In the past, folder Custodians/Owners had "Full Control" within their district/division shared folder and had the ability to add permissions to the folders. This change will allow the folder custodian permissions to "Modify" which will prevent unintentional misuse of the "Authenticated Users" group.

In regards to providing recurring training to all USMS employees, PII specific training has been limited. Currently, the two courses that include training on PII are Computer Security Awareness Training (CSAT), a DOJ annual training requirement, and Operations Security (OPSEC) training. Both courses have been reviewed to determine the depth of PII training currently provided. The USMS TD, in conjunction with USMS OGC, is currently developing enhanced PII training to include as part of the CSAT and OPSEC.

B. Restoration of an Aggrieved Employee

Not applicable.

C. Disciplinary Action Against any Agency Employee

Inasmuch as the Investigative Report did not find individual culpability, the matter was not referred for disciplinary procedures. Nonetheless, corrective action in TOD and Agency-wide was taken.

D. Referral to the Attorney General of any Evidence of Criminal Violation

As stated, USMS OPR did not find evidence of a knowing, willful, or intentional violation of the Privacy Act; nor did it discover any instances of actual inappropriate access to, or disclosure of, PII from the TOD shared drive. Accordingly, no referrals for possible criminal action were made.

¹ While the HIP AA is also cited, the federal government is not a "covered entity" under HIP AA privacy rules. P.L. 104-191, Sec. 264; 45 C.F.R. §160.103.

November 30, 2015

United States Marshals Service Investigative Report Office of Special Counsel (OSC) File No. DI-15-4560

Background

By letter dated April 23, 2014, the Office of Special Counsel (OSC) (OSC File No. DI-14-1514) notified the Department of Justice (DOJ) of a whistleblower disclosure allegation that the United States Marshals Service (USMS) Investigative Operations Division (IOD) failed to follow appropriate procedures to safeguard and dispose of personally identifiable information (PII) and protected health information. The allegations made by the whistleblower were that unsecured documents containing PII were stored on IOD's shared network drive and improperly accessible to current and former USMS operational and administrative employees and contractors. In addition, it was alleged that IOD management failed to adhere to legal requirements and other required provisions for the proper storage of PII and other sensitive information. As a result, the maintenance of PII in the shared drive, and access to the PII by these persons, were alleged to be a violation of the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and DOJ security policies and procedures.

In June 2014, USMS Director Stacia A. Hylton appointed U.S. Marshal (USM) James A. Thompson from the District of Utah to lead an investigation into the allegations made by the whistleblower. USM Thompson concluded his investigation in July 2014. Please refer to letter dated August 22, 2014 from Associate Deputy Attorney General Armando Bonilla to the Honorable Carolyn N. Lerner regarding the response to OSC File No. DI-14-1514.

As a result of the 2014 investigation, specific remediation efforts were coordinated with the USMS Information Technology Division (ITD) which included the following:

1. Created a new IOD shared drive and folders with the proper access controls for authorized IOD users so they could add documents to the appropriate folders.
 - Authorized IOD personnel to transfer files from unsecured folders into protected folders.
 - Old PII that was no longer needed and did not need to be archived was eliminated.
 - Any user who was not authorized to access a particular folder would receive an error message saying they did not have access to that folder.
2. Established two entities (one in IOD and one in ITD) to handle access changes so when employees were hired, transferred, or separated, access controls would be updated accordingly using standard User Access Request (UAR) forms. The UAR provides a

November 30, 2015

record of each modification and is consistent with DOJ Order 2640.2F and USMS Policy 12.7 for information technology security.

3. Increased training to IOD employees regarding the need and requirement to protect PII data and how individuals and managers can protect PII in a secure manner. Previous training had not provided enough information to employees on *how* to protect PII.

USM Thompson found no evidence of a knowing, willful, or intentional violation of the Privacy Act; nor did he discover any instances of actual inappropriate access to, or disclosure of, PII from the IOD shared drive. USM Thompson concluded that the readily accessible PII on the IOD shared drive was the result of administrative error and required administrative correction. While administrative correction was taken for IOD shared drives, agency wide administrative correction did not occur at that time.

Current Summary of OSC Request for USMS Investigation re: OSC File No. DI-15-4560

By letter dated July 16, 2015, the OSC notified DOJ of a whistleblower allegation that the USMS Tactical Operations Division (TOD) failed to follow appropriate procedures for safeguarding and disposing of PII and other sensitive data (OSC File No. DI-15-4560). The allegation made by the whistleblower was that the TOD shared network drive, containing thousands of unsecured documents containing PII, was improperly accessible by current and former USMS employees and contractors.

In addition, OSC stated that unsecured PII was an agency wide issue based on the corrective actions recommended in the previous USMS investigative response to the whistleblower allegations concerning unsecured PII on IOD's shared drive. The following information in this report substantiates the claim that PII was not appropriately safeguarded on TOD shared drives, identifies the investigation conducted by the USMS Office of Professional Responsibility (OPR), and outlines remediation measures taken by TOD, ITD, Training Division (TD), and Office of General Counsel (OGC), as well as agency-wide measures taken to prevent similar failures in the future.

TOD and OPR Findings and Remediation

In August 2015, the TOD Office of Security Programs initiated an internal review to determine if TOD employees failed to follow appropriate procedures to safeguard and dispose of PII. In September 2015, Christopher Edwards, Chief of the TOD Office of Security Programs, determined that the claims of non-secure data and PII information were credible. Specifically he found:

November 30, 2015

1. Non-secure access to names, dates of birth, Social Security Numbers (SSN) of current and former USMS operational personnel, contractors, and staff from other USMS districts and divisions;
2. Non-secure access to employee leave request forms and travel vouchers including SSNs;
3. Non-secure access to employee banking information for direct deposit purposes;
4. Non-secure access to resumes, merit promotion career board data, and awards;
5. Non-secure access to fitness tests of operational employees;
6. Non-secure access to Equal Employment Opportunity (EEO) case information; and
7. Non-secure access to Attorney General and Deputy Attorney General briefing materials.

In September 2015, the USMS OPR was directed to conduct an investigation regarding the allegation that the parent directory for the TOD shared drive \\dfs-share-v01 was widely available to nearly all USMS employees and that access was not just limited to TOD employees. USMS OPR’s investigation substantiated that 15 of 58 folders within the parent folder of the TOD shared drive contained PII and other sensitive data and were accessible to USMS “authenticated users.” An “authenticated user” is anyone with a Personal Identity Verification (PIV) card who uses it to access the USMS network. This means that virtually all USMS employees and contractors had access to PII within these folders even if they were unaware of this capability.

Table One below lists the 15 shared drives that were accessible and also summarizes the TOD shared drives located on \\dfs-share-v01 . The table reflects the status of the shared drives as of September 11, 2015.

November 30, 2015

Table One: Accessible Folders on TOD's Shared Drive \\dfs-share-v01

Network Location	Folder	Can I access the folder contents?	Can I Read individual files?	Do Authenticated Users have access at some level?	Was I able to capture Properties - Security Screenshot?	PII Accessible / Found
\\dfs-share-v01	AK-Shared	Yes	Yes	Yes	Yes	Yes ²
\\dfs-share-v01	ALN-Shared	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	ALS-Shared	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	ARW-Shared	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	DIRStaff	Yes	Yes	Yes	Yes	Yes ²
\\dfs-share-v01	District	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	FLM	Yes	Yes	Yes	Yes	Yes ¹
\\dfs-share-v01	GAM-Shared	Yes	Yes	Yes	Yes	Yes ¹
\\dfs-share-v01	GAN-Shared	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	GAS-Shared	Yes	yes	Yes	Yes	No
\\dfs-share-v01	HI-Shared	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	pcc18	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	pcc19	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	PCC21	Yes	No	Yes	Yes	No
\\dfs-share-v01	pcc22	Yes	Yes	Yes	Yes	No
\\dfs-share-v01	PersonalSecurity	Yes	No	Yes (File names only)	Yes	No
\\dfs-share-v01	SOG-Migration	No	N/A	N/A	Yes	N/A
\\dfs-share-v01	SOG-NAS	No	N/A	N/A	Yes	N/A
\\dfs-share-v01	SOG-NAS-Shared	No	N/A	N/A	Yes	N/A
\\dfs-share-v01	SOG-NAS-Software	No	N/A	N/A	Yes	N/A
\\dfs-share-v01	SOG-NAS-Users	No	N/A	N/A	Yes	N/A
\\dfs-share-v01	TOD	No	N/A	N/A	Yes	N/A
\\dfs-share-v01	TODGroupShares	No	N/A	N/A	Yes	N/A
\\dfs-share-v01	TODShares	No	N/A	N/A	Yes	N/A

¹ Remedial measures taken to ensure these drives were no longer accessible as of October 19, 2015.

² Remedial measures taken to ensure these drives were no longer accessible as of November 13, 2015.

USMS OPR conducted a search of every folder and subfolder of AK-Shared by mapping to the drive and opening every folder with the intent to locate PII. *Table Two* provides a summary of the PII found within AK-Shared (the District of Alaska's shared drive).

November 30, 2015

Table Two: Summary of PII Found within the AK-Shared Drive

File Location (AK-Shared)	PII or Sensitive Data Found
Admin2-> ao-> Vicki stuff	Five files containing SSNs of 5 individuals, 1 file contained Civil Process with name and home address of one individual
Admin2->Training->FY2010	One file (SF-182) with SSN of 1 employee
AK-Task_Force->af task force	Felony warrant listing 84 individuals with SSNs
Criminal->Criminal Clerk Files	Two items with the name and DOB of two USMS prisoners
Criminal->Criminal Desk Misc	One item with name and DOB of a USMS prisoner, one resume with SSN
Criminal->Detainers->Probation Detainer	One USM-16D with SSN and DOB of USMS prisoner
Criminal	Three letters to the FBI requesting rap sheet correction, three SSN of three USMS prisoners
CSO->Porter BI	Three files containing PII w/SSN for one individual
District_Info->DSO(Guards) ->Guard Files	One listing of 33 individuals with SSNs. Two files containing copy of passport and driver's license for one individual.
Fairbanks->DSO Guard folder	USM-601 with SSN for three individuals
Fairbanks->HEARD	Subject report and wanted poster with PII/SSN for one individual
Fairbanks->Monthly Warrants	Three listings of warrants from 2008 with DOB and SSN of between 112-191 individuals each
Fairbanks->HUFF->	Subject report and warrant worksheet with PII/SSN for one individual
Project Reunion-Batch Results from NSOTC->ALASKA	Nine folders containing USM-129s with SSN and other PII concerning 9 sex offenders
Project Reunion-Batch Results from NSOTC->SPECIAL CASES	Seven folders containing USM-129s with SSN and other PII concerning 7 sex offenders
Project Reunion-Batch Results from NSOTC->UNKOWN	Fifteen folders containing USM-129s with SSN and other PII concerning 15 sex offenders
Project Reunion-Batch Results from NSOTC->NON-ALASKA	Eighteen folders containing USM-129s with SSN and other PII concerning 18 sex offenders

USMS OPR conducted a search of DIRstaff by mapping to the drive and opening every folder with the intent to locate PII. *Table Three* provides a summary of the PII and representative samples of the sensitive data found within the DIRStaff shared drive.

Table Three: Summary of PII Found within the DIRStaff Shared Drive

File Location (DIRStaff)	PII or Sensitive Data Found
1.AGreport	Five hundred and seventy reports to the AG from 10/09/01 - 12/02/08
3.Director>Columbian Incident	Three files with medical info on 3 employees
4.Deputy Director>PWP for SES Reporting to DD	One Performance Work Plan for an SES employee
7.COS>D.O'Hearn>Personnel Issues>Grievances	Two files regarding two employees grievances
7.COS>Shooting Incidents	Five files containing LES information

November 30, 2015

File Location (DIRStaff)	PII or Sensitive Data Found
Deputy Director's Itineraries	Contains subfolders with various Deputy Director itineraries from 2007-2013
Director's Itineraries	Contains Director itineraries from 2007-2015
Director's Travel Authorizations	Five files with home address and last four of a SSN for a former Director
Director Harlow Travel Itineraries	Contains travel itineraries of Acting Director Harlow
SES Resumes Jan 2011	Contains resumes and ECQs for current and former USMS SES
District	Ninety-six subfolders with SF-71s and USM-356s (990) for 123 employees

In coordination with ITD, USMS OPR confirmed the FLM, GAM-Shared, AK-Shared and DIRStaff folders were no longer accessible and also attempted to discover who may have accessed the individual files containing PII or sensitive information. Though most of the files have metadata, the data is limited to a time of access and does not identify the individual user accessing the file. There was no available system data for who may have mapped the drives or opened files. Without the identity of a person who may have accessed the files, further examination is not possible.

Upon determination of unsecured PII found within TOD's shared drive, ITD was contacted and restricted all access to the TOD shared drive. Before making any changes to the shared drive, ITD preserved the drive in accordance with preservation orders not associated with this investigation. Although information related to the Critical Incident Response Team (CIRT) members was accessible, there was no PII associated with the Employee Assistance Program (EAP) or CIRT counseling that was accessible or protected under HIPAA. Chief Edwards is currently working with ITD on a protocol to store PII and ensure that controls are put in place to ensure proper access and storage.

In summary, TOD worked with ITD to identify and protect PII on the TOD shared drive. Specific actions were immediately initiated when TOD was first notified of the allegations. Remediation efforts that were completed in September 2015 included:

1. Restricted access to the TOD shared drive, allowing only program Chiefs and the administrative officer to have access;
2. Created a new TOD shared drive with folders to better organize and retain necessary PII data;
3. Initiated a division-wide review of all items stored on the TOD shared drive to determine what was necessary for retention, archiving, or elimination;
4. Created an ad hoc internal working group within TOD to establish a standardized filing structure, naming conventions, and access control standard operating procedures;
5. Reauthorized user access on a limited basis; and,

November 30, 2015

6. Initiated UAR procedures to grant access on a case-by-case basis if approved by TOD and ITD.

TOD took immediate steps to remove PII from their shared drives, limit access, and have actively engaged ITD to increase training, restrict access to PII, archive or remove PII that is no longer needed, and terminate access to those who no longer have a need to access PII.

The primary allegation contained in the OSC letter of July 16, 2015, that the TOD shared drive was accessible by a large number of current and former employees, was substantiated by TOD Chief Clay Edwards. USMS OPR was not able to independently substantiate the primary allegation of who may have improperly accessed the TOD shared drive. The secondary allegation that the parent folder of the TOD shared drive, \\dfs-share-v01, was accessible to almost all USMS employees was substantiated in that 15 of the 58 shared drives at that network location granted access to “authenticated users.” At least two of the shared drives, AK-Shared and DIRStaff had security properties that allowed anyone with a PIV card to access these drives. These two drives were found to contain unsecured PII and other sensitive information.

Agency Wide Current and Planned Corrective Actions

As an agency, the USMS has actively taken steps to respond to issues with PII being inappropriately exposed on USMS shared drives. The USMS ITD and the Privacy Office within the USMS OGC developed a plan to protect PII within the agency. In general, this plan creates a folder for PII that is managed by each USMS district and division. Access to this folder and the sub-folders within it will be strictly controlled by Secure Custodians identified by the districts and divisions.

In November 2015, ITD purchased a scanning tool that will search for PII that is not located within the PII folder. This tool will run on a regular basis to quickly identify PII that was not properly stored. In addition, ITD has changed folder permissions from “Full Control” to “Modify” to prevent users from using the “Authenticated Users” group in any action taken. In the past, folder Custodians/Owners had “Full Control” within their district/division shared folder and had the ability to add permissions to the folders. This change will allow the folder custodian permissions to “Modify” which will prevent unintentional misuse of the “Authenticated Users” group.

These proactive measures will address the issues found with PII being accessible by users who do not have a need-to-know.

Table Four provides a general timeline for implementation of the USMS plan to protect PII and the expected task completion dates. Please refer to *Attachment One* for a detailed implementation plan identified by phase, specific tasks, and status of completion.

Table Four: General Expected Timeline for USMS PII Implementation Plan

USMS Investigative Response to OSC File No. DI-15-4560

November 30, 2015

Expected Task	Expected Completion Date
Send notice to USMS Senior Leadership notifying them of the ITD's implementation plan to secure PII information and directing them to designate primary and alternate Secure Custodians responsible for PII access control. <ul style="list-style-type: none"> • Per memo dated September 28, 2015 from Acting Director David Harlow to USMS Leadership (U.S. Marshals, Chiefs, Assistant Directors, and Deputy Assistant Directors). 	COMPLETED September 28, 2015
Send notice to all users regarding the proper protection of PII information and Law Enforcement Sensitive (LES) information, including instructions on how to ensure files containing PII or LES are properly protected with restricted access. <ul style="list-style-type: none"> • Per memo dated September 28, 2015 from Assistant Director/Chief Information Officer Karl Mathias to all USMS employees. 	COMPLETED September 28, 2015
Create protected PII folders for each division/district.	COMPLETED October 2, 2015
Create training material for Secure Custodians.	COMPLETED October 30, 2015
Train Secure Custodians.	December 8, 2015
Inspect and identify PII content to be moved into the Protected PII folder.	January 18, 2016
Move PII content into the protected PII folder.	February 29, 2016
Begin periodic scanning of all USMS content to ensure PII data does not exist outside of the PII folder.	March 31, 2016
Develop and implement enhanced training as part of Computer Security Awareness Training (CSAT). <ul style="list-style-type: none"> ○ DOJ annual training requirement. 	June 1, 2016

Please note that due to the large volume of USMS data, it is expected that a significant amount of effort will be involved to decide how to organize PII folders and then to move PII data into them. Moving the information is a manual process that will take time. ITD anticipates this process will take several months to complete. The result, however, will be a much more secure and maintainable method of securing PII.

In regards to providing recurring training to all USMS employees, PII specific training has been limited. Currently, the two courses that include training on PII are Computer Security Awareness Training (CSAT), a DOJ annual training requirement, and Operations Security (OPSEC) training. Both courses have been reviewed to determine the depth of PII training currently provided:

- CSAT currently provides limited training on PII. Specifically, there are only four slides dedicated to the topic and provides an overview in the following areas:
 - Slide 1: Definition of PII

November 30, 2015

- Slide 2: Examples of common PII
 - Slide 3: Regulations related to PII (e.g. Privacy Act, Office of Management and Budget, etc.)
 - Slide 4: DOJ PII reporting requirements
- OPSEC provides training on PII as it relates to identifying critical information for the agency.
 - This course is focused on providing employees with a 5-step OPSEC process and training on how to integrate this process into their personal and professional lives.
 - This training was not intended to provide information on the statutory and regulatory requirements of protecting PII.
 - This training is not required under the Executive Order.

The USMS TD, in conjunction with USMS OGC, is currently developing enhanced PII training to include as part of the CSAT and will include additional PII related information in the following areas:

- In the office, while traveling or teleworking;
- On a portable electronic device (BlackBerry, iPhone, laptop, or USB flash drive);
- Emailing, faxing, or by other electronic transfer;
- Storing on a network shared drive or SharePoint;
- Encrypting PII;
- Securing PII when not in use; and
- Disposing of PII.

It was determined that enhancing PII training as part of CSAT benefits the agency because this training is required by DOJ and the completion of this course is enforceable via computer access. Therefore, if training is not completed, computer access will be turned off. In addition, since CSAT already includes PII training, enhancing this course will allow the new PII training material to be implemented sooner.

November 30, 2015

Attachment One:

USMS Implementation Plan for Protected PII Review, Validation, Clean-up and Verification Plan and Timeline (*as of November 27, 2015*)

Item No.	Phase	Task	USMS Responsible Office	Expected Completion Date	Status
1	PREPARE	Notify ALL USMS users about the protected PII situation, the proposed timeline to correct the situation and the need to ensure we protect and properly handle protected PII.	USMS Director	25-Sep-15	COMPLETED
2	PREPARE	Identify Primary and Alternate Secure PII Custodian to USMS/ Senior Component Official for Privacy (SCOP).	ALL Districts and Divisions	1-Oct-15	COMPLETED
3	PREPARE	Direct users within the District or Division to perform a complete review and validation of all files and folders assigned to them.	ALL District and Division Senior Leaders	2-Oct-15	COMPLETED
4	PREPARE	Create a separate protected PII shared drive with folders for each Division and District.	ITD/Investment Management Branch (IMB)	2-Oct-15	COMPLETED
5	PREPARE	Generate Excel folder and file listings for each Account Manager to help Secure Custodians define and setup their protected PII folders.	ITD/IMB	2-Oct-15	COMPLETED
6	PREPARE	Generate HTML files of Security Group Permissions for each Division and District Security Groups. Account Managers will be able to use the HTML file to verify who is assigned group permissions within a folder and assist Secure Custodians to identify level of permissions to folders and subfolders.	ITD/IMB	2-Oct-15	COMPLETED
7	PREPARE	Create a SharePoint site in ITD to load the Excel folder and file listings.	ITD/Program Management Office (PMO)	2-Oct-15	COMPLETED
8	PREPARE	Load the HTML files of Security Group Permissions for each Division and District Security Groups on the SharePoint site. This will allow the Secure Custodians to access this file to view who has permissions for the various groups who have access to the folders and files within their purview.	ITD/PMO	2-Oct-15	COMPLETED

November 30, 2015

Item No.	Phase	Task	USMS Responsible Office	Expected Completion Date	Status
9	PREPARE	Create a link to the SharePoint site where the Excel folder and file listings are located for Account Managers to access pertinent information and instructions to help Secure Custodians.	ITD/PMO	2-Oct-15	COMPLETED
10	PREPARE	Provide each Secure Custodian a list of what constitutes protected PII. Also provide the list to all users to help identify the presence of protected PII in their folders.	USMS/SCOP	5-Oct-15	COMPLETED
11	PREPARE	Send the complete list of Primary and Alternate Secure Custodians to ITD via email to: USMS-ITD-IMB-ServerOperations@usms.doj.gov	USMS/SCOP	22-Oct-15	COMPLETED
12	PREPARE	Create training material that SMB will use to teach Secure Custodians how to assign permissions and how to MOVE (NOT COPY) files.	ITD/Service Management Branch (SMB)	30-Oct-15	COMPLETED
13	PREPARE	Assign and grant SharePoint permissions to ITD/SMB and ITD/IMB	ITD/PMO	30-Oct-15	COMPLETED
14	PREPARE	Send link of SharePoint site to ITD/SMB and ITD/IMB.	ITD/PMO	30-Oct-15	COMPLETED
15	PREPARE	Submit a completed USM Form 169 to the Help Desk requesting ROOT permissions to the current folder(s) assigned and to the newly created protected PII subfolder. The USM Form 169 also needs to specify the need for permissions to structure and control new protected PII subfolder.	Each Secure Custodian	30-Nov-15	IN PROGRESS
16	ENABLE	Process ALL submitted DISTRICT Secure Custodians' USM Form 169s. Grant DISTRICT Secure Custodians the proper permissions to the current folder(s) assigned and the newly created protected PII folder.	ITD/SMB	4-Dec-15	IN PROGRESS

November 30, 2015

Item No.	Phase	Task	USMS Responsible Office	Expected Completion Date	Status
17	ENABLE	Process ALL submitted DIVISION Secure Custodians' USM Form 169s. Grant DIVISION Secure Custodians the proper permissions to the current folder(s) assigned and the newly created protected PII folder.	ITD/SMB	4-Dec-15	<i>IN PROGRESS</i>
18	PREPARE	Identify and implement a process to structure, manage, and document how Secure Custodians will control access to their assigned protected PII folder. Secure Custodians may use a USM Form 169 to document permissions inside the Protected PII folder. NOTE: The process to manage the access to the respective PII folder includes the SCOP to provide guidance and ensure the processes are instituting IAW established privacy guidance.	Each Secure Custodian	4-Dec-15	<i>IN PROGRESS</i>
19	ENABLE	Schedule ONLINE training sessions for all Secure Custodians. Training will cover how to assign permissions to the protected PII folder and also how to move protected PII data from their current folder structure into the new protected PII folder. PII Custodian Training Schedule: 30 Nov - 8 Dec 2015 at 1000 and 1600 daily (1 hour) sessions via online training. PII Custodians MUST attend a training session. Attendance will be documented.	ITD/SMB	8-Dec-15	
20	INSPECT	Work with Division or District key personnel to validate each folder and file assigned.	ITD/SMB Account Managers & Secure Custodians	14-Dec-15	
21	INSPECT	Inspect folders and files to identify if there is protected PII content. Identify to designated District or Division Secure Custodians what folders and files contain	Each User	18-Jan-16	

USMS Investigative Response to OSC File No. DI-15-4560

November 30, 2015

Item No.	Phase	Task	USMS Responsible Office	Expected Completion Date	Status
		protected PII.			
22	CERTIFY	Validate all folders and files and send a letter/form to Secure Custodian certifying that folders/files containing protected PII are properly identified.	Each User	25-Jan-16	
23	MOVE	Move (NOT COPY) each identified file containing protected PII data to the newly created protected PII folder.	Each Secure Custodian	1-Feb-16	
24	CLEAN	Verify folders and files identified as containing protected PII data have been MOVED from the current folder(s) assigned to the newly created protected PII folder.	Each Secure Custodian	15-Feb-16	
25	CERTIFY	Return validated PII Excel folder and files listing to USMS/OGC. Certify to USMS/OGC via letter that all folders and files identified as containing protected PII data have been moved and there is no presence of PII in each folder.	Each Secure Custodian	29-Feb-16	
26	SCAN	Perform an initial scan of all USMS content to ensure protected PII is not present outside of the designated protected PII shared drive.	ITD/IMB	31-Mar-16	
27	VERIFY	Review the initial scan to ensure protected PII is NOT present outside of the designated protected PII Shared Drive.	ITD/ Security and Enterprise Architecture Branch (SEAB)	8-Apr-16	
28	ALERT	Notify Secure Custodians of protected PII outside of the designated shared drive.	ITD/SEAB	12-Apr-16	
29	CLEAN	MOVE protected PII from unsecured shared drives to the designated protected PII shared drive and folder.	Each Secure Custodian	18-Apr-16	
30	CERTIFY	Certify that Protected PII is cleared and removed from unsecured Shared Drives.	Each Secure Custodian	21-Apr-16	

November 30, 2015

Item No.	Phase	Task	USMS Responsible Office	Expected Completion Date	Status
31	PREVENT	Perform quarterly check of the list of personnel with permissions to the protected PII shared drive to ensure USM Form 169s are on file documenting appropriate level of permissions.	ITD/IMB	21-Apr-16	
32	PREVENT	Notify Secure Custodians of any permission discrepancies found on the protected PII shared drive.	ITD/IMB	25-Apr-16	
33	PREVENT	Reconcile protected PII shared drive permissions with ITD/SEAB and complete appropriate documentation to include submitting USM Form 169s if needed.	Each Secure Custodian	29-Apr-16	
34	PREVENT	Develop/update and implement enhanced training as part of Computer Security Awareness Training (CSAT)	DOJ & USMS/OGC	1-Jun-16	