# Privacy Compliance Review of the U.S. Secret Service (USSS)

*July 21, 2017*

**Contact Point**

Randolph D. Alles
Director
U.S. Secret Service
U.S. Department of Homeland Security

**Reviewing Official**

Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

## I. Background

On October 7, 2016, the DHS Office of Inspector General (OIG) issued report OIG-17-01, "USSS Faces Challenges Protecting Sensitive Case Management Systems and Data"[1] that included a recommendation that the DHS Privacy Office "conduct a systemic review with recommendations for ensuring USSS compliance with DHS privacy requirements." The DHS Privacy Office (PRIV) launched a Privacy Compliance Review (PCR) on December 2, 2016, based on the OIG recommendation that focused on USSS privacy compliance and privacy practices dating from September 1, 2015.

The primary focus for this PCR was on USSS's adherence to and implementation of privacy requirements set forth in:

1. *Privacy Policy Directive 140-06/DHS Privacy Policy Guidance Memorandum 2008-01*, The Fair Information Practice Principles[2],
2. *DHS Privacy Policy and Compliance Directive 047-01*[3] and *Instruction Number: 047-01-001*[4], and
3. Former Deputy Secretary Jane Lute's 2009 memo designating Component privacy officers[5].

The DHS Privacy Office recognizes USSS Privacy Office staffing shortages and significant changes in information technology systems that were underway during our review. We recognize the resources needed to implement the OIG's recommendations and support USSS Privacy Office efforts to implement those that improve their privacy posture. This report attempts to discuss the situation at the time of review, while adhering to the roles and responsibilities of a well-functioning component privacy office that understands and plans for strategic information management and technology changes. USSS senior leadership should consider the findings in this report as a call to take seriously the needs of the USSS Privacy Office, including the correct and prompt staffing, resourcing, and empowerment of it.

---

[1] *See:* OIG-17-01, "USSS Faces Challenges Protecting Sensitive Case Management Systems and Data" October 7, 2016 *available at*: https://www.oig.dhs.gov/assets/Mgmt/2017/OIG-17-01-Oct16.pdf.
[2] *See:* Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security", *available at*: https://www.dhs. gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[3] *See:* Privacy Policy and Compliance Directive 047-01, July 2011, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf.
[4] *See:* Privacy Policy and Compliance Instruction 047-01-001, July 2011, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.
[5] *See:* OIG-17-01, page 17; Recommendation 5.

## II. Scope and Methodology

*Scope*

The scope of this PCR focused on privacy practices and the overall privacy culture at USSS. More specifically, the PCR assessed USSS's implementation of the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation.

The USSS safeguards the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events. USSS employs over 6,000 special agents, Uniformed Division officers, and other technical, professional, and administrative support personnel.

The 2009 Deputy Secretary's memo designating Component privacy officers was formalized in February 2017 via *DHS Privacy Policy Instruction 047-01-005* for Component Privacy Officers.[6] Pursuant to this Instruction, the USSS Privacy Officer is responsible for overseeing privacy compliance, policy, and oversight activities in coordination with the DHS Chief Privacy Officer. At the time of our review, the USSS Privacy Office was located within the Liaison Division (LIA) of the Office of Government and Public Affairs, which reports to the USSS Deputy Director.[7] LIA staff administer the Freedom of Information Act (FOIA) and Privacy Act (PA) Program for USSS, which is responsible for ensuring USSS compliance with presidential and congressional mandates and directives.

According to OIG-17-01, USSS "system owners and Information System Security Officers (ISSO) … were unaware of the requirements for documenting privacy controls on information systems nor had they received guidance from the DHS Chief Privacy Officer or the USSS Privacy Officer on how these requirements should be documented."[8] This lack of awareness was but one privacy-related criticism in the OIG report that prompted this PCR.

*Methodology*

The DHS Privacy office conducted this PCR in coordination with the USSS Privacy Office, as well as other program offices at the Secret Service, and would like to thank the USSS personnel that facilitated this effort. The findings detailed in this PCR report reflect conclusions reached by the DHS Privacy Office based on our historical interactions with the USSS Privacy Office as

---

[6] *See*: DHS Privacy Policy Instruction Number: 047-01-005, *available at*: https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf, was published on February 2, 2017; the responsibilities listed therein reflect responsibilities previously assigned to USSS by the former DHS Deputy Secretary in June 2009.

[7] *See*: USSS Organizational Chart *available at:* https://www.dhs.gov/sites/default/files/publications/Public%20Org%20Charts%202017.04.12.pdf.

[8] OIG-17-01, Page 18.

well as our analysis of documents, responses, discussions, and other information received and facilitated by the USSS Privacy Office since the PCR was initiated in December 2016.

The PCR is a collaborative process that ensures programs operate in compliance with federal privacy laws, departmental policies, and assurances made in Privacy Impact Assessments (PIA), System of Records Notices (SORN), and other privacy compliance documentation. This PCR was conducted in coordination with the USSS Privacy Officer and focused on implementation of DHS privacy policy as noted above. This PCR did not assess USSS compliance with published PIAs or SORNs given that the OIG had already made recommendations to that effect. Given the expansive scope of this PCR, this report will organize our review of these issue areas according to the DHS FIPPs framework.

In conducting this PCR, the DHS Privacy Office:

- Reviewed relevant USSS operational documents, including policies, Standard Operating Procedures, Information Technology Strategic Plan, Table of Penalties, and Inspection Division Checklist;
- Met with the USSS Chief Operating Officer, as well as officials from the Office of Government and Public Affairs and the Privacy Office on several occasions;
- Developed and distributed an initial questionnaire (December 2016);
- Reviewed initial USSS responses and supporting documentation;
- Developed follow-up questionnaires (February 2017 and May 2017);
- Met with USSS Inspection Division (May 2017);
- Reviewed follow-up USSS responses and supporting documentation;
- Met with USSS Chief Information Security Office (CISO) (June 2017);
- Drafted an initial PCR Report for USSS comments (June 2017);
- Mitigated USSS comments (July 2017);
- Drafted and published final PCR Report (July 2017).

## III. Findings

### A. Summary of Recommendations

Based on our findings, this PCR makes the following 12 recommendations:

1. USSS should promptly reorganize and fully fund the Privacy Office with separate divisions for Privacy and FOIA and appropriately staff and resource each. Additionally, the USSS Privacy Officer should be a senior level federal employee with significant experience and background in privacy and have direct access to the USSS Director.
2. USSS should formalize and empower the USSS Personally Identifiable Information (PII) Working Group to address privacy shortcomings and implement privacy best practices.
3. USSS should formalize the Privacy Officer's authority within decision making fora, such as the Enterprise Governance Council and the Information Technology Review Committee, where privacy equities can be fully addressed before USSS makes operational decisions.

4. USSS should add privacy compliance equities to its Inspection Division, Headquarters/Protection Checklist when it conducts quadrennial compliance inspections of USSS offices.
5. The USSS Privacy Office should attend regularly scheduled monthly compliance meetings hosted by the DHS Privacy Office, as well as maintain a regular interaction/meeting schedule with the analysts assigned as its liaison.
6. As a best practice, USSS should focus on understanding and implementing standing DHS Privacy Policies, Directives, and Instructions, unless said privacy policies/instructions need to be tailored to USSS. USSS should, however, use appropriate means to raise awareness and oversee implementation and compliance with DHS privacy policies/instructions.
7. USSS should promote privacy Standard Operating Procedures (SOP) among system users and imbed SOPs within privacy sensitive systems.
8. USSS Privacy Office should improve processes and increase oversight of USSS compliance with federal privacy laws and regulations and DHS privacy policies. This improvement includes timely submission of privacy compliance documents on all privacy sensitive systems/programs/operations.
9. As a best practice, USSS should continue annual records reviews to ensure any permanent records that are eligible for transfer to the National Archives and Records Administration (NARA) are transferred and that all records are appropriately stored or deleted according to approved records retention schedules.
10. USSS Privacy Office should ensure it supports USSS implementation of DHS Directive Number: 262-05 regarding Information Sharing and Safeguarding by proactively applying appropriate governance mechanisms in the development of information sharing arrangements and ensuring all agreements have been reviewed by the USSS Privacy Office and include all required privacy compliance documents. USSS should ensure the DHS Privacy Office reviews and approves all information sharing and access agreements, as appropriate, to determine if they comply with applicable privacy law and adequately protect individuals' privacy.
11. USSS Privacy Office should work with USSS CIO and system and program managers to develop and conduct regularly scheduled user access audits on all privacy sensitive systems to determine if a user has a continued need to know and remove access for those that do not. Users should be required to complete annual privacy training and affirm knowledge of relevant privacy SOPs for each system to retain access.
12. USSS should overhaul the oversight of mandatory privacy training, to include organizational awareness for the handling and safeguarding of personally identifiable information; privacy incident handling, reporting, and mitigation practices; and compliance documentation requirements.

## B. Organization/Structure/Authority

*Finding: The Secret Service organizational structure does not elevate the visibility, access, and authority required of the USSS Privacy Office and Officer. The structure of, and support to, the*

*Privacy Office itself fails to sufficiently provide the resources necessary to address information privacy issues.*

The DHS Privacy Office concludes that the current organization of the USSS Privacy Office, as well as its location within the greater Secret Service structure is insufficient to provide the level of oversight and direction necessary to sufficiently oversee the organization's privacy compliance, policy, and oversight activities. The PCR finds that the Office is understaffed, under resourced, and lacks the privacy-specific experience needed to effectively address systematic and programmatic privacy issues and concerns.

Office of Management and Budget (OMB) Circular No. A-130[9] identifies the Senior Agency Official for Privacy (SAOP) as the senior official, designated by the head of an agency, who has overall agency-wide responsibility for information privacy. Under the OMB Memorandum for the Heads of Executive Departments and Agencies, M-16-24,[10] the SAOP will have a principal role in overseeing, coordinating, and facilitating an agency's privacy compliance efforts. As the DHS SAOP, the DHS Chief Privacy Officer formalized DHS privacy policy requiring DHS Components to appoint a Privacy Officer within their Component to oversee privacy compliance, policy, and oversight activities in coordination with the DHS Chief Privacy Officer. Through this directive, the Component Privacy Officer serves as an extension of the DHS Chief Privacy Officer in order to facilitate the successful accomplishment of OMB Circular No. A-130 requirements at the Component level. To facilitate the effective function of Component Privacy Officers,[11] the Department has issued instructions that outline Privacy Officer responsibilities, as well as requirements for the collection, use, maintenance, disclosure, deletion, and destruction of Personally Identifiable Information (PII).[12]

In order to efficiently and effectively identify, mitigate, and reconcile privacy issues related to Secret Service information technology systems and programs, the USSS Privacy Office/Officer must be strategically positioned in a location within the Component's hierarchy that affords it both the authority required, as well as the ability to coordinate with senior leadership as needed. Through the issuance of *DHS Instruction No. 047-01-005*, the Component Privacy Officer, who reports directly to the Component Head, must be a senior level federal employee with significant privacy experience, and be provided the appropriate levels of staff support and resources.

---

[9] *See:* OMB Circular No. A-130: Managing Information as a Strategic Resource (July 2016), *available at:* https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.

[10] *See:* OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (September 2016), *available at:* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_24_0.pdf.

[11] *See*: DHS Privacy Policy Instruction Number: 047-01-005, *available at*: https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf.

[12] *See:* Privacy Policy and Compliance Instruction 047-01-001, July 2011, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.

At this time, the USSS Privacy Office is not advantageously situated to provide the Secret Service Privacy Officer with the level of visibility, access, or influence necessary to fulfill its mission. During the course of this PCR, the Secret Service Privacy Office was located under the Freedom of Information and Privacy Acts (FOIA/PA) Branch, and reported to the Liaison Division, which reported to the Assistant Director of the Office of Governmental and Public Affairs. In Director Clancy's August 22, 2016 response to OIG-17-01, he concurred with the OIG recommendation to "appoint a full-time, senior-level Privacy Officer reporting directly to the USSS Director" and noted an expected completion date of this reorganization by December 31, 2016. On December 2, 2016, the USSS Chief Operating Officer proposed an organizational realignment that would move the Secret Service Privacy Office directly under the Office of Governmental and Public Affairs. The Assistant Director of the Office of Government and Public Affairs reports to the Director of the Secret Service. This alignment also provides a means for the USSS Privacy Office to elevate issues directly to the USSS Director as needed. While this move does reduce some of the management layers and obstructions present under the previous construct and is commensurate with some other DHS Component privacy offices, based on the results of this PCR, the DHS Acting Chief Privacy Officer does not support this proposed realignment. The USSS Privacy Office currently is not adequately staffed with experienced privacy professionals that do not also have other non-privacy related responsibilities. Any realignment will need to demonstrate its effectiveness and efficiency based on how the Secret Service prioritizes privacy and whether the Privacy Officer can implement DHS privacy policies within the Component and freely report directly to the USSS Director, as required.

As part of its repositioning proposal, USSS reported it plans to increase staffing and support levels within its Privacy Office. In response to the PCR Questionnaire, USSS Privacy Office stated there are twenty employees supporting the USSS FOIA/PA Branch. Three employees are designated for privacy issues: the Privacy Officer, an Assistant Privacy Officer, and a full-time privacy professional. During the course of the PCR, the Secret Service Privacy Officer split her time between privacy and disclosure responsibilities, the Assistant Privacy Officer position was vacant from August 2015 through February 2017, and the privacy professional recently transitioned from FOIA. In this configuration, the Privacy Officer served in both a privacy capacity, as well as performing FOIA responsibilities. This runs contrary to *DHS Instruction No. 047-01-005*, which requires the designation of a full-time Privacy Officer with significant privacy experience. USSS proposed plans to transition the Disclosure and Privacy Officer (GS-301-15) position to a Senior Executive Service (SES)-level position, overseeing two division leads, one each for Privacy and FOIA. While no timeline was provided for when this transition will happen, it is imperative for USSS leadership to comply with the terms of the *Instruction*, and appoint a senior-level federal employee with the requisite level of experience and background in privacy to manage the entire privacy process at the USSS. Simply designating the position as an SES is inadequate and will not fix the issues outlined in this PCR. The Secret Service needs to conduct a Workforce Planning Analysis based on applicable federal legal and policy

requirements needed to effectively manage a federal privacy program to determine the proper employment level for its Privacy Office personnel.[13]

OIG-17-01 identified a lack of "privacy leadership," which remains a problem. In February, the USSS Privacy Office noted it began training two additional employees that are currently providing support to FOIA efforts, in order to provide part-time privacy support, and stated it had plans to hire two more full-time privacy professionals. In January 2017, the DHS Privacy Office shared position descriptions with the USSS Privacy Office from other well-staffed DHS Component Privacy Offices to help craft new vacancy announcements, which were expected to be posted in February 2017. The USSS Privacy Office also confirmed that funding for these positions was approved. While the vacancies required position reclassification to focus on privacy responsibilities, as of the date of this report, no vacancy announcements or position descriptions have yet been publically posted despite the OIG raising the staffing issue in 2016. A draft of the reclassified Government Information Specialist (Privacy Analyst), GS-0306/13 position description was shared with the DHS Privacy Office in July, which better reflects the privacy specific skills needed to appropriately staff the USSS Privacy Office.[14] We understand work is underway with the USSS Human Capital Office and recommend that the Secret Service Privacy Office confirm these positions reflect the office's needs stemming from a robust Workforce Planning Analysis[15] and Job Analysis[16] of all its positions – current and new to include the SES, if one is designated.

In February, the Secret Service Privacy Office also indicated that it planned to bring contractors on board as needed, but did not define how it would determine when or if such support was needed. While the proposal to supplement the USSS Privacy Office with additional contract support is a positive step, with no solid timeline for implementation, this does not address the shortcomings facing the USSS Privacy Office. The DHS Privacy Office stands ready to assist the USSS Privacy Office with this effort by sharing the resources required to get a contract vehicle in place or identifying creative detail opportunities to augment current staffing shortfalls.

---

[13] *See:* OMB Memorandum M-16-24: Role and Designation of Senior Agency Officials for Privacy (September 2016), *available at*, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_24_0.pdf.

[14] The Federal Privacy Council (FPC) has a number of resources to help agencies recruit experienced federal privacy professionals; *available at*: www.fpc.gov.

[15] A Workforce Planning Analysis will serve as the foundation for managing the USSS Privacy Office's human capital needs and requirements. It will also enable the USSS Privacy Office to strategically meet current and future workforce needs to prevent unnecessary disruptions as experienced while the Assistant Privacy Officer position was vacant.

[16] A Job Analysis (JA) is the process of gathering, examining, and interpreting data about privacy tasks and responsibilities. The JA provides a thorough understanding of the essential functions of your privacy positions; lists the duties and responsibilities of the positions; assigns a percentage of time spent for each task; annotates the position's relative importance in comparison with other jobs; and outlines the knowledges, skills, and abilities needed to perform the job and the conditions under which the work is completed.

In order to address current systemic and programmatic privacy gaps, risks, and other issues, USSS leadership should promptly implement a reorganization of its reporting structure, resulting in a direct line of reporting from the Privacy Officer to the Director of the Secret Service. To implement resource and financial provisions of *DHS Privacy Policy and Compliance Directive 047-01*,[17] USSS should also provide the level of material support necessary to appropriately staff the Privacy Office in a way that will allow it to properly attend to information privacy concerns and the development of necessary compliance documentation.

*Finding: The Secret Service Personally Identifiable Information Working Group has made significant recommendations to improve the USSS privacy culture and should be granted additional authority to identify and address privacy concerns and shortcomings with USSS systems.*

According to *Instruction No. 047-01-005*, Component Privacy Officers are responsible for applying appropriate privacy policies and federal privacy laws to its Component's operations and monitoring the Component's compliance with all applicable federal privacy laws and regulations. In his August 22, 2016 response to OIG-17-01: "USSS Faces Challenges Protecting Sensitive Case Management Systems and Data,"[18] the Director of the Secret Service noted the establishment of a PII Working Group designed to "examine the agency's policies and practices regarding the collection and use of PII throughout the Secret Service operations" and to make recommendations to "minimize the use of PII". The Working Group, which reports to the Secret Service Executive Review Board (ERB), consists of USSS personnel from the Office of Investigation, Office of Chief Counsel, Office of Training, Security Clearance Division, Privacy Office, Office of Protective Operations, Office of Strategic Intelligence and Information, Office of Human Resources, Office of Chief Information Officer, and Management and Organization Division. The ERB has final authority over all USSS project proposals, and considers the PII Working Group's recommendations during its decision making process.

To demonstrate its effectiveness, the USSS Privacy Office provided instances of PII Working Group recommendations that have been implemented by USSS. For example, the Working Group recommended technology safeguards to protect PII from inappropriate and/or unintended disclosure when sent via email, recommended minimizing distribution and use of PII being reported in official messages, and recommended minimizing the collection of Social Security numbers when operationally possible. The DHS Privacy Office supports the Working Group's undertakings and supports its continued operations. While this Working Group could attend to part of the *Instruction*-mandated responsibilities, the DHS Privacy Office finds that the USSS Privacy Office staff could further capitalize on this as a resource if the PII Working Group had a formal charter that provided it the authority to identify or, more importantly, rectify violations of USSS or DHS privacy policy, and enforce its recommendations. Without the ability to mandate

---

[17] *See:* IV.B.5 at https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf.

[18] *See:* DHS Office of Inspector General's Report: OIG-17-01.

action, the provision of recommendations by the group that do not have to be addressed is seemingly ineffective.

The Secret Service should formally charter the PII Working Group and provide it with the structure and authority necessary to implement meaningful changes in the way that PII is collected, maintained, and used by the USSS. The working group should meet regularly and be led by the Secret Service Privacy Office. The group should be provided with access to programs and, when necessary, the systems needed to identify privacy gaps and vulnerabilities. The group should be briefed on ongoing efforts to mitigate known risks and remedy systemic compliance issues. In order to best effect change, the working group should be staffed by personnel from all levels of each of the member directorates.

*Finding: The USSS Privacy Office does not have equal standing in decision making fora to be an effective proponent for privacy protections and risk mitigations during the development of USSS investment initiatives.*

According to *Instruction No. 047-01-005*, Component Privacy Officers are responsible for identifying privacy issues related to Component programs and the application of appropriate privacy policies and federal privacy laws to Component operations. Additionally, *Instruction No. 047-01-001* tasks Component Privacy Officers with maintaining an "ongoing review of all Component IT systems, technologies, rulemakings, programs, pilot projects, information sharing, and other activities to identify collections and uses of PII, and to identify any other attendant privacy impacts." Based on responses to this PCR and review of historical privacy compliance documentation received by the DHS Privacy Office, this PCR found that the USSS Privacy Office does not proactively exercise the necessary authority within the Secret Service's decision making forums to ensure that privacy equities are fully addressed before making operational decisions.

For example, the USSS Privacy Officer currently serves as an advisory member in the Enterprise Governance Council (EGC), which is responsible for the review of Unfunded Requirements Requests for Fiscal Year 2017 and Program Decision Options for inclusion in the Fiscal Year 2019 Resource Allocation Plan. Established by the Director of the USSS, and chartered to develop a transparent prioritization process for streamlining the Secret Service's investment initiatives, the EGC is responsible for providing business-level reviews of significant USSS investment initiatives in information technology, science and technology, human resources, and other capital and controlled assets. To ensure the efficient and effective operation of the USSS investment governance process, the EGC has oversight of the Information Technology Review Committee, the Science and Technology Review Committee, the Operations and Support Review Committee, and other purpose-specific committees.

The EGC is composed of Deputy Assistant Director-level personnel from each Directorate, the Office of Chief Counsel, and advisory officials representing various subject matter areas. Advisory members are expected to provide compliance and accountability mechanisms that can

inform, pre-empt, or modify EGC voting activities. In its advisory capacity, the Privacy Officer participates in EGC meetings to assess privacy implications related to newly proposed and developmental systems. As a non-voting member, however, the Privacy Officer does not have the leverage envisioned in *Instruction Nos. 047-01-001* or *047-01-005* to address privacy concerns present in proposed and developmental systems, or to be in a position within the decision making body to meet the overall objective of evaluating USSS programs, systems, and initiatives for potential privacy implications in order to provide mitigation strategies to reduce the privacy impact. As currently organized, the Privacy Office would lend its advice and/or inform the Office of Government and Public Affairs (as a voting member) of its recommendations, but operational decisions could be made without regard to the guidance, much less approval of the Privacy Officer. The USSS Privacy Officer is also limited in her ability to immediately escalate potential privacy issues to the USSS Director without going through other USSS management.

As the primary official within the Secret Service responsible for providing guidance to USSS leadership, program managers, business owners, and project developers on privacy-related matters, the Privacy Officer should be positioned in a way that allows collaboration and equal representation with the leadership of the Office of the Chief Information Officer (OCIO) and the Office of the Chief Counsel (OCC). Without inclusion as a decision-making member in the EGC, for example, the USSS Privacy Officer is not being afforded a level of status equivalent to other Deputy Assistant Director-level personnel representing the directorates involved, and necessary to resolve privacy issues within programs and systems at the outset. The Privacy Officer should be seen as an equal partner and should have the authority to engage in such fora.

The Secret Service contends that the involvement of the Privacy Officer at the production-level of system and program development or change, as currently employed, sufficiently addresses privacy concerns. This involvement helps to effectively incorporate privacy protections and mitigate the risks associated with privacy-sensitive systems early in the process, to ensure it is part of the initiative's foundation. However, privacy compliance documentation provided the DHS Privacy Office does not support this claim. For example, in 2015 the Secret Service retired its Mainframe system, which supported a number of USSS applications. Had the USSS Privacy Office been substantially intertwined in the management of the service's IT systems, the privacy compliance documentation needs that arose from the retirement of this system would have been identified before the Mainframe was disbanded, resulting in a more efficient means of addressing compliance requirements for the applications housed within it. Instead, after the system was shut down, the USSS Privacy Office reactively generated, and had to have the DHS Privacy Office expedite review and clearance of a number of compliance documents to ensure that coverage was in place.

*Finding: The USSS Privacy Office should be more substantially involved in the development and review of Secret Service systems to proactively mitigate potential privacy compliance issues and information privacy/safeguarding risks.*

The Secret Service conducts regular reviews of its systems to ensure compliance with standing USSS policies and protocols. For example, the Inspection Division conducts compliance reviews of all offices and programs on a quadrennial basis, in order to verify that all operations are in accordance with established USSS requirements. Additional Program Management Reviews (PMR) are conducted quarterly by the USSS OCIO. During our review, the DHS Privacy Office found more could be done to review privacy equities during the Secret Service's inspection processes to address potential gaps between privacy policy and practice and avoid potential privacy compliance shortfalls.

As outlined in OMB Circular No. A-108,[19] agencies are required to establish a comprehensive approach to improve the management of their information resources, specifically with regard to privacy enhancements. OMB Circular A-130[20] outlines the need to conduct continuous monitoring, or an ongoing awareness of privacy risks and the assessing of privacy safeguards at a frequency sufficient to ensure compliance with applicable requirements and to adequately protect personally identifiable information. The DHS CISO issued DHS 4300A: Sensitive Systems Handbook,[21] that instructs organizations to develop a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Additionally, 4300A outlines, as a best practice, the coordination of security audit functions with other organizational entities that require audit-related information in order to enhance mutual support.

As currently structured, the Inspection Division's quadrennial review does not specifically include privacy aspects in the review process. Despite the substantive effort to review all aspects that comprise each Secret Service system during the quadrennial review, assessments of privacy protections and compliance documentation are absent from this process. While the USSS CIO has made significant changes to its oversight of USSS IT systems as a result of OIG-17-01 and states that privacy is considered throughout the system management lifecycle, this is not always reflected in privacy compliance documentation received by the DHS Privacy Office. While the USSS Privacy Office is invited to participate in the PMR process, there does not seem to be sufficient prioritization to incorporate or compel the Privacy Office to provide any proactive assistance or assessment. While this PCR found that both the quadrennial review and PMR processes satisfy the need outlined in OMB Circular A-130 to conduct continuous monitoring and maintain an ongoing awareness of Secret Service systems, more substantive involvement,

---

[19] *See:* OMB Circular No. A-108: Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act (December, 2016), *available at:* https://www.federalregister.gov/documents/2016/12/23/2016-30901/reissuance-of-omb-circular-no-a-108-federal-agency-responsibilities-for-review-reporting-and.

[20] *See:* OMB Circular No. A-130: Managing Information as a Strategic Resource (July 2016), *available at:* https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.

[21] *See:* DHS 4300A: Sensitive Systems Handbook – Attachment S: Compliance Framework NIST Special Publication 800-53: Controls for Privacy Sensitive Systems (August, 2014), *available at:* https://www.dhs.gov/sites/default/files/publications/4300A-Handbook-Attachment-S-Compliance-Framework-for-Privacy-Systems.pdf.

including careful attention to looming expiration dates, by the USSS Privacy Office would mitigate risks for the adequate protection of sensitive and personally identifiable information.

In order to enhance the ability of the Secret Service to assess all aspects of its systems and programs, USSS should more rigidly and proactively add privacy equities to all review processes. Not only should they include Privacy Office personnel in review activities, but also specifically add privacy review requirements to their assessments. USSS Inspection Division was open to this idea during our Review, and we encourage the USSS Privacy Office to craft the assessment's scope and compliance metrics. Each assessment should include a comprehensive review of the system's Privacy Threshold Assessment (PTA), as well as any other related documentation, including Privacy Impact Assessments (PIA) and System of Record Notices (SORN). This review will aid in determining if updates to compliance documentation, which must be completed any time there is a change to the system or the information that is being collected, maintained, or used, is needed. Adding privacy aspects to regular compliance reviews will also help to increase the understanding of privacy-related issues and concerns among program and system management personnel, inherently increasing privacy knowledge and fostering a privacy-protective culture at the Secret Service.

*Recommendations*

1. USSS should promptly reorganize and fully fund the Privacy Office with separate divisions for Privacy and FOIA and appropriately staff and resource each. Additionally, the USSS Privacy Officer should be a senior level federal employee with significant experience and background in privacy and have direct access to the USSS Director.
2. USSS should formalize and empower the USSS PII Working Group to address privacy shortcomings and implement privacy best practices.
3. USSS should formalize the Privacy Officer's authority within decision making fora, such as the Enterprise Governance Council and the Information Technology Review Committee, where privacy equities can be fully addressed before USSS makes operational decisions.
4. USSS should add privacy compliance equities to its Inspection Division, Headquarters/Protection Checklist when it conducts quadrennial compliance inspections of USSS offices.

## C. Involvement

*Finding: The USSS Privacy Office is not sufficiently involved in key departmental privacy meetings, resulting in a lack of awareness of trending privacy issues, policy changes, and evolving practices.*

Collaboration amongst members of the DHS Privacy Community ensures that all members are aware of developments in privacy law, policy, and issues, in addition to providing personnel from varying component privacy offices the opportunity to discuss department priorities and initiatives. Participants work through cutting edge issues together, addressing major changes to

privacy compliance, such as those from OMB or from Executive Orders. Based on the DHS Privacy Office's historical experience, the USSS Privacy Office does not engage in a consistent or meaningful manner with other members of the DHS Privacy Community, including the DHS Privacy Office.

According to the DHS Privacy Office Guide to Implementing Privacy,[22] Privacy Office staff are required to maintain a high level of awareness of developments in privacy law, policy, and issues. As such, staff is encouraged to reach out to other federal agencies, privacy advocates, and stakeholders. The DHS Privacy Office coordinates regular meetings with component Privacy Officers and Privacy Points of Contact (PPOCs), including a monthly compliance meeting and regularly scheduled coordination meetings, in order to facilitate outreach efforts.

Accordingly, component privacy office personnel are expected to take part in these meetings so as to stay abreast of privacy-related developments. The Secret Service Privacy Officer indicated that the responsibility to attend these meetings was delegated to subordinate personnel; however, according to the DHS Privacy Office Compliance team, Secret Service Privacy Office personnel failed to attend the majority of the regularly scheduled monthly compliance meetings. These meetings have proven to be a valuable forum to pass along information related to recent policy changes as well as occasions for Component privacy personnel to seek assistance related to programmatic or system issues within their organization. These meetings also provide Component privacy personnel with an opportunity to identify their priorities, and allow the DHS Privacy Office to prioritize review schedules and confirm compliance documentation production timelines/deadlines. The failure of the Secret Service Privacy Office to consistently participate in these meetings has undoubtedly had a negative impact on their ability to work in an open, cooperative, and efficient manner with the DHS Privacy Office regarding the review and adjudication of their compliance documentation (PTAs, PIAs, and SORNs).

The Secret Service Privacy Office should attend monthly privacy meetings organized by the DHS Privacy Office Senior Director for Compliance and maintain regular interaction with the DHS Privacy Office analyst(s) assigned as their liaison to facilitate better communication on issues, organization on tasks, and timely completion of required compliance documentation. As the principal interagency forum to improve the privacy practices of agencies, the Federal Privacy Council is another excellent resource for the USSS to use. More than just training, the Federal Privacy Council offers resources to support interagency efforts to protect privacy and provide expertise and assistance to agencies and improve the management of agency privacy programs by identifying and sharing lessons learned and best practices.

*Finding: The Secret Service Privacy Office should conduct a gap analysis to determine if established department-wide policies meet the component's needs.*

---

[22] *See:* The DHS Privacy Office Guide to Implementing Privacy (June 2010), *available at:* https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf.

In response to OIG-17-01, the Secret Service Privacy Office developed a *Privacy Policy and Compliance Directive* that provides direction on the collection, use, maintenance, disclosure, deletion, and destruction of PII. Upon review, however, it is almost verbatim to *DHS Instruction No. 047-01-001: Privacy Policy and Compliance*[23] without addressing Secret Service-specific issues, nor placing any additional substantive requirements on USSS personnel.

Per DHS *Directive No. 047-01: Privacy Policy and Compliance*,[24] Component Heads are responsible for implementing DHS privacy policy and procedures as established by the DHS Chief Privacy Officer. Under *Instruction No. 047-01-001*, Component Privacy Officers and PPOCs are responsible for overseeing the implementation of DHS privacy policies, including all guidance documents and memoranda, at the Component level. If the USSS Privacy Office determines that *DHS Instruction No. 047-01-001* is specific enough to meet the needs of the Component, then efforts should be focused on implementing said policy, and raising awareness and compliance among USSS personnel. If, however, the USSS Privacy Office found any gaps after analyzing existing DHS policies, steps should be taken to fill those gaps by creating customized policies as other Component Privacy Offices have done.

Rather than generating duplicative policies and instructions, USSS should focus its efforts on understanding and implementing standing DHS privacy policies, directives, and instructions. This will ensure that all USSS personnel, programs, and systems are handling personally identifiable information in a manner consistent with departmental standards. If the Secret Service does not believe that current Department-wide policies are adequately addressing its needs, a thorough and thoughtful analysis could be conducted to identify gaps or issues, as well as ways in which they might be addressed through the development of more specific component level policy.

*Finding: The Secret Service does not adequately describe privacy requirements within the Standard Operating Procedures (SOP) for privacy-sensitive systems, potentially reducing the focus of program personnel on privacy implications.*

Based on responses and an example provided to the DHS Privacy Office during this PCR, the Secret Service does not identify privacy-specific needs and requirements within the SOPs developed for privacy-sensitive systems. An assessment of the PMR SOPs resulted in the discovery that other than a tertiary listing, no real attention is paid to privacy issues or compliance within the SOPs. The document identifies a need to ensure that privacy documentation is in place, but does not require a substantive review and analysis of the validity, timeliness, or applicability of the documentation. The PMR SOPs fails to provide an outline of how to properly assess compliance with applicable privacy laws, departmental policies, and Secret Service procedures.

---

[23] *See:* Privacy Policy and Compliance Instruction 047-01-001, July 2011, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.
[24] *See:* Privacy Policy and Compliance Directive 047-01, July 2011, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf.

The lack of privacy-specific language and requirements within system-specific SOPs reduces the awareness of privacy issues and implications for Secret Service personnel operating USSS systems. At this time, USSS largely depends on the issuance of official messages advising employees of privacy requirements. These official messages provide information on general privacy requirements and protocols, as well as direction on where employees can find additional DHS and USSS privacy related directives. However, the general nature of these messages fails to provide a link to the system-specific privacy issues that could better be addressed within the system's SOPs.

The USSS Privacy Office should advocate for the inclusion of privacy-specific language, notices, and instructions within program and system SOPs in order to better engrain privacy concepts within Secret Service operations. The drafting of system and program-specific privacy language within the SOPs will also more clearly identify the privacy implications presented through the operation of a system. To ensure that this is done, USSS Privacy Office might consider reviewing program and system SOPs during the PTA, PIA, and SORN development processes. If not already occurring, system owners and ISSOs should work with Privacy Office personnel during the development of these documents, to collaborate on the development and review of the SOPs without creating an additional burden. This would also afford the Secret Service Privacy Office with the opportunity to develop a privacy section within the SOPs during the initial system development phase, as well as provide for a clearly defined review cycle aligned with other compliance documentation timelines. This would not only ensure that the SOPs itself contained updated information, but also that it properly reflects the current privacy environment and system managers were aware of means to properly navigate privacy risks.

*Recommendations*

5. The USSS Privacy Office should attend regularly scheduled monthly compliance meetings hosted by the DHS Privacy Office, as well as maintain a regular interaction/meeting schedule with the analysts assigned as its liaison.
6. As a best practice, USSS should focus on understanding and implementing standing DHS Privacy Policies, Directives, and Instructions, unless said privacy policies/instructions need to be tailored to USSS. USSS should, however, use appropriate means to raise awareness and oversee implementation and compliance with DHS privacy policies/instructions.
7. USSS should promote privacy SOPs among system users and imbed SOPs within privacy sensitive systems.

## D. Oversight

*Finding: USSS Privacy Office does not currently employ a sufficient level of oversight to ensure that the development and operation of systems and programs occurs in a privacy-compliant manner.*

The successful management of a Privacy Compliance program requires a high degree of planning, coordination, and review. While recognizing USSS Privacy Office staff shortages, at this time, the level of oversight by the USSS Privacy Office is not sufficient to facilitate successful, privacy-compliant operations.

The DHS Chief Privacy Officer, via the Privacy Office, is responsible for the evaluation of all new or proposed DHS information systems and programs in order to determine their impact on privacy, and to ensure that those systems do not erode protections relating to the use, collection, and disclosure of personal information.[25] As outlined in the DHS Privacy Office Guide to Implementing Privacy,[26] DHS Privacy Office personnel conduct regular meetings with DHS Chief Information Office (CIO) staff, DHS Chief Information Security Office (CISO) staff, and Component program or system owners, to discuss new initiatives and how privacy can be addressed during both development, as well as through the system's lifecycle. This includes the OMB requirement that the SAOP within each agency review the administration of the agency's privacy program and report compliance data to OMB.[27] Accordingly, DHS components are responsible for reviewing, and if necessary updating, system and program PIAs every three years, SORNs every two years, and PTAs every three years.[28] In order to meet the Department's compliance oversight requirements, the same level of involvement is expected of the component Privacy Office with regard to its programs and systems.[29] The DHS Privacy Office depends on each Component to successfully manage its own compliance programs, insuring that all DHS systems and programs are operating in a compliant manner.

In order to track each Component's adherence to the comprehensive framework required under the Federal Information Security Modernization Act (FISMA),[30] which is designed to protect government information, operations, and assets, the Department employs a scoring system. USSS has increased its Privacy Compliance score from 56 percent for PIAs and 91 percent for SORNs in 2015, to 100 percent for each as of July 2017. It must also be noted however, that while biennial reviews for SORNs are required under existing OMB policy, there have been no updates to USSS-specific SORNs submitted to the DHS Privacy Office since 2011. Therefore,

---

[25] 6 U.S.C. § 222.
[26] *See:* The DHS Privacy Office Guide to Implementing Privacy (June 2010), *available at:* https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf.
[27] *See:* OMB Circular No. A-108: Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act (December 2016), *available at:* https://www.federalregister.gov/documents/2016/12/23/2016-30901/reissuance-of-omb-circular-no-a-108-federal-agency-responsibilities-for-review-reporting-and.
[28] *See:* The DHS Privacy Office Guide to Implementing Privacy (June 2010), *available at:* https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf.
[29] One of the responsibilities of the Component Privacy Officer, as outlined in *DHS Privacy Policy Instruction 047-01-005*, is the monitoring of the Component's compliance with all applicable federal privacy laws and regulations; implementing corrective, remedial, and preventive actions, including those identified in any DHS Privacy Compliance Reviews; and notifying the DHS Privacy Office of privacy issues or any non-compliance, when necessary.
[30] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014).

the 100 percent score is a misleading representation of the Secret Service's adherence to standing OMB requirements.

The 100 percent score for PIAs is also not the appropriate measure, in that it only accounts for FISMA systems operated by the Secret Service. All Components at DHS actively operate non-FISMA systems and privacy-sensitive programs that deal with PII and require appropriate compliance documentation, including PIAs. While Secret Service has focused its efforts on completing documentation for each of its identified FISMA systems, it has not yet submitted any PIAs or SORNs for non-FISMA systems or sensitive technologies or programs that do not trigger the E-Government Act, but still require PIAs as directed by the Chief Privacy Officer under section 222 of the Homeland Security Act.

Based on historical interactions with the DHS Privacy Office, the USSS Privacy Office demonstrates a lack of proactive management and oversight of the generation, review, and submission of privacy compliance documentation that matches the level of detail, analysis, and general readability of that submitted by its component counterparts. The Department uses PTAs, PIAs, and SORNs as the mechanisms by which privacy in Departmental IT systems and programs is assessed.[31] This absence of privacy compliance documentation points to USSS Privacy Office's inability to forge a privacy-focused culture within the organization that ensures the inclusion of privacy personnel during program and system development.

Though the USSS Privacy Office contends that it is deeply embedded in the planning, development, and change processes of Secret Service systems, the decommissioning of the USSS Mainframe in 2015 provides evidence to the contrary. Planning for the system's retirement began at least as early as 2009,[32] and if the Secret Service Privacy Office were as involved in the management of IT systems as required, the privacy implications associated with this type of effort should have been identified and addressed well before the system was actually shuttered. In this case, the Privacy Office was forced, after the fact, to identify, develop, and submit for approval the necessary privacy documentation to bring the new systems that resulted from the Mainframe's decommissioning into compliance. Though the Mainframe was disbanded in 2015, compliance documentation for the multiple systems associated with this effort was not completed until July 2017. All of the PTAs and PIAs submitted by the USSS Privacy Office to the DHS Privacy Office between March 2016 and the time of this report were related to the inventory of systems associated with the shuttering of the Mainframe.

It is imperative that the USSS Privacy Office continues its efforts to ensure that system and program managers are aware of the need to engage privacy personnel early in the system development or amendment process and that their contributions are timely, meaningful, and

---

[31] Guidance for the applicability and development of Privacy Compliance documentation is available on the DHS Privacy website at https://www.dhs.gov/compliance.

[32] *See:* Secret Service plans IT reboot: Agency plans for a multi-phased IT modernization effort (October 19, 2009), *available at* https://fcw.com/articles/2009/10/19/web-secret-service-it-modernization.aspx.

productive. The USSS Privacy Office depends on ISSOs to inform them of pending compliance deadlines. However, in order to stay ahead of expiring privacy compliance documentation, resulting in the delay of Authority to Operate (ATO) reauthorizations, expiration of compliance documentation, and missed review cycle requirements, the USSS Privacy Office should proactively monitor the lifecycle of USSS IT systems.[33] Missed deadlines are exasperated when the DHS Privacy Office is asked to review PTAs, PIAs, and SORNs expeditiously in order to meet the planned start date of its operations or systems. When compared with other DHS components, USSS has substantially fewer SORNs[34] to manage, and should be able to better control the review process to ensure timely and thorough evaluations are conducted.

The Secret Service Privacy Office must fortify its oversight efforts and implement processes that more deeply engrain privacy into the operations of USSS systems and programs. In order to achieve this goal, the USSS Privacy Office should also develop an outreach program designed to provide system administrators and program managers with a better understanding of the role that the Privacy Office plays in the development and continued authorization of Secret Service systems. Additionally, with the intention of maintaining a greater awareness of the status of privacy compliance documentation, as well as to prevent lapses in coverage, the USSS Privacy Office should develop a document tracking system capable of alerting personnel in advance (3-6 months) of the expiration or mandated review date of compliance documents, including PTAs, PIAs, and SORNs. This would ensure that documents are completed by program offices, as well as provide a reasonable amount of time for review and adjudication by the USSS and DHS Privacy Offices.

To reinforce previously stated findings that the structure of, and support to, the Privacy Office itself does not sufficiently provide the resources necessary to address information privacy issues, it should be noted that toward the end of our review, USSS made a concerted effort to provide for review a number of PIAs for systems that, at the time, were not in line with FISMA requirements. This uptick coincided with the addition of an Assistant Privacy Officer with privacy experience, clearly demonstrating that additional dedicated privacy staff members resulted in an increase in the production of compliance documentation. During the months of April and May 2017, the Secret Service Privacy Office submitted six PIAs for review, of which five have been signed and published to the DHS Privacy website.

*Finding: The Secret Service is conducting regular, annual, reviews of records to ensure that eligible permanent records are transferred to the National Archives and Records Administration (NARA) for appropriate storage or deletion.*

---

[33] *See:* OIG-17-01: USSS Faces Challenges Protecting Sensitive Case Management Systems and Data (October 2016), *available at: https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-01-Oct16_1.pdf.*

[34] The DHS Privacy Website includes a list of all of the SORNs maintained by component organizations, *available at:* https://www.dhs.gov/system-records-notices-sorns.

The Secret Service has an established records review process that involves assessments at multiple levels, and across various timelines. USSS conducts records reviews in accordance with the requirements of the Federal Records Act,[35] which establishes the framework for records management programs in Federal Agencies, including the creation, maintenance, and disposition of records. The Secret Service also conducts reviews in accordance with OMB Exhibit 300[36] guidelines, as required by *OMB Circular No. A-11 Part 7, Section 300: Planning, Budgeting, Acquisitions, and Management of Capital Assets*,[37] as well as DHS Acquisition Management requirements and internal standards.

In accordance with the Secret Service's Office Inspection Program, the management of records, office files, and related materials are reviewed and evaluated for compliance with applicable policies and regulations on a quadrennial basis. Through its current process, USSS personnel identify both temporary and permanent records in order to ensure that storage, maintenance, transfer, and disposition are being completed in line with respective schedules. Ad-hoc assessments are conducted for records identified for disposition scheduling purposes, records inventory management, and office assistance visits. On an annual basis, the Records Management Program Office reviews all Federal Records Center holdings for Secret Service offices to ensure that all eligible permanent records are transferred to NARA promptly. Additional periodic IT PMRs are conducted, at intervals outlined under OMB Exhibit 300 guidelines and DHS Acquisition Management requirements, to assess each system's compliance with the Federal Records Act.[38] Similar to other established reviews, PMR assessments identify whether records are being managed according to appropriate NARA-approved schedules; if temporary records are being purged; if permanent records are being transferred at the end of the life cycle; and if new record types have been created that would require the revision of existing schedules.

In compliance with the Data Minimization Principle,[39] which states that DHS should "only retain PII for as long as is necessary to fulfill the specified purpose(s)," the Secret Service should continue to perform records reviews and compliance assessments across the various management levels and intervals at which they are currently being performed. Both scheduled and ad-hoc assessments ensure that records are being maintained and disposed of in accordance with established federal, departmental, and USSS policies, preventing issues with retention protocols.

---

[35] 44 U.S.C. §§ 3101-3107

[36] *See:* OMB Exhibit 300: Capital Asset Plan and Business Case Summary, *available at:* https://www.dhs.gov/exhibit-300-capital-asset-plan-and-business-case-summaries-fiscal-year-2013.

[37] *See:* OMB Circular No. A-11 Part 7, Section 300: Planning, Budgeting, Acquisitions, and Management of Capital Assets, *available at:* https://www.gsa.gov/graphics/staffoffices/sec300.pdf.

[38] 44 U.S.C. §§ 3101-3107

[39] *See*: Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

*Finding: The Secret Service Privacy Office lacks adequate oversight of, or participation in, the development of Information Sharing and Access Agreements in which the USSS is a partner to affirm that all agreements comply with applicable privacy laws or policies and provide adequate protection for the individuals' information that is being shared.*

At this time, the Secret Service Privacy Office is not sufficiently involved in the development, review, or monitoring of USSS Information Sharing and Access Agreements[40] (ISAA). Based on privacy compliance documents reviewed by the DHS Privacy Office, the USSS Privacy Office's awareness or privacy oversight seems limited to cross checking existing SORNs that may allow for a routine use to share the information. Having the legal authority to share information is not sufficient ISAA governance to ensure that when personally identifiable information is shared, privacy safeguards follow the information to agencies it is being distributed to, and any further dissemination that may occur.

*DHS Directive No. 262-05: Information Sharing and Safeguarding*,[41] establishes the policy and governance framework for information sharing and safeguarding both within the Department, as well as with federal, state, local, tribal, territorial, private sector, and international partners. *Directive No. 262-05* outlines the responsibilities of the DHS Chief Privacy Officer to ensure that departmental information sharing and safeguarding activities comply with applicable laws and provide adequate protections for individuals' privacy. As the main point of contact for the DHS Privacy Office at the USSS, the Secret Service Privacy Officer should be an active participant in the discussion, construction, and implementation of all USSS ISAAs that involve PII. As outlined in the DHS Information Sharing and Safeguarding Strategy,[42] Components should support and sustain the capacity and capability to share and safeguard mission-essential information in support of the DHS mission. As the primary steward of information privacy protection for the Secret Service, this responsibility falls largely on the USSS Privacy Office. Additionally, as directed in *DHS Instruction No. 047-01-005*, each Component Privacy Officer is to provide privacy oversight of information, including PII, as well as communicate privacy initiatives on Component programs with internal and external stakeholders in coordination with the DHS Privacy Office.

The Secret Service Privacy Office claims that it is involved in the generation, review, and completion of all Information Sharing and Access Agreements involving USSS-maintained PII. A sample review of the DHS Privacy Office's records for USSS PTAs identified a number of instances in which systems operated by the Secret Service share information, including PII, outside of the Department. However, the USSS Privacy Office states that there are no

---

[40] DHS May 2017 Lexicon defines ISAA as an "agreement that is used to facilitate the exchange of information between the Department (or any element or entity within the Department) and one or more outside parties."

[41] *See*: DHS Directive No. 262-05: Information Sharing and Safeguarding, *available at:* http://dhsconnect.dhs.gov/policies/Instructions/262-05_Information_Sharing_Safeguarding.pdf.

[42] *See:* DHS Information Sharing and Safeguarding Strategy (January 2013), *available at:* https://www.dhs.gov/sites/default/files/publications/12-4466-dhs-information-sharing-and-safeguarding-strategy-01-30-13--fina%20%20%20_0.pdf.

agreements that warrant their review. The DHS Privacy Office encourages the USSS Privacy Office to audit all of its PTAs, as well as any Component-based information sharing, in an effort to cross check and account for shared information, and to ensure it is in accordance with and covered by official ISAAs. The Secret Service Privacy Officer should regularly advise USSS officials that serve on or directly participate in the Information Sharing Coordinating Council (ISCC), which includes Action Officers from each DHS component and office and provides a monthly working-level forum for addressing all Department-wide information sharing matters. USSS Privacy Officer involvement in the ISCC would ensure that the flow of USSS PII across the Department occurs in a privacy-protective manner. Additionally, the USSS Privacy Office should maintain a physical record of all established agreements involving USSS PII, as well as encourage those responsible to ensure that all agreements are entered into the DHS Enterprise Architecture Information Repository (EAIR).[43]

*Finding: The Secret Service Privacy Office is not adequately involved in the conduct of regular, thorough, assessments of its IT systems to ensure that appropriate security measures and access limitations are in place for systems containing personally identifiable information.*

The USSS Privacy Office lacks an in-depth review and audit process designed to verify that appropriate security and privacy protections are in place. The USSS Privacy Office also has no involvement in, or oversight of, the process governing the provision of individual access for systems that maintain personally identifiable information.[44]

According to OMB Circular No. A-130,[45] agencies are expected to appropriately monitor, audit, and document their organization's compliance with the FIPPs. Additionally, the roles and responsibilities of all employees and contractors who have access to PII should be clearly defined, and appropriate levels of training should be provided. This Circular further requires that agencies implement policies of least privilege that only permit the use of organization networks and data so that users have role-based access to only the information and resources that are necessary to the conduct of their job-related duties. As prescribed in the OMB Circular No. A-108,[46] each SAOP is responsible for reviewing the administration of the agency's privacy

---

[43] *See:* OMB Memorandum M-13-13, Open Data Policy - Managing Data as an Asset (May 2013), *available at:* https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf. In compliance with OMB M-13-13, DHS has developed the Enterprise Architecture Information Repository (EAIR); a centralized repository of Enterprise Architecture assets used by DHS and its Components.

[44] *See: Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53 Revision 4 – Appendix J, Control AR-4: Privacy Monitoring and Auditing), available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf .

[45] *See:* OMB Circular No. A-130: Managing Information as a Strategic Resource (July 2016), *available at:* https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.

[46] *See:* OMB Circular No. A-108: Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act (December, 2016), *available at:* https://www.federalregister.gov/documents/2016/12/23/2016-30901/reissuance-of-omb-circular-no-a-108-federal-agency-responsibilities-for-review-reporting-and.

program as part of the annual FISMA reporting process. This requirement is further reinforced under 44 U.S.C. §§ 3555,[47] which mandates that each agency shall perform an independent evaluation of the effectiveness of information security policies, procedures, and practices.

At the time of this PCR, the USSS Privacy Office did not demonstrate its proactive involvement in the process for granting individuals access to Secret Service IT systems, including those that contain PII. The Secret Service's current practice gives system owners authority and responsibility to determine which individuals will be provided with user and privileged level access to USSS systems. Not only does each system owner determine who will be provided with access, the system owner also establishes system-specific criteria for access on both privileged and unprivileged levels. The only visibility that the USSS Privacy Office demonstrated in this process is the information provided by the system owner during the PTA and PIA processes. The USSS does have in place automated processes that lock or remove access to those accounts considered "inactive". This process is overseen by system ISSOs and the Secret Service IT Cyber Security team. Otherwise, the USSS Privacy Office does not participate in the regular auditing or monitoring of privacy-sensitive systems to ensure that individuals provided with access, still require it.

The Secret Service Privacy Office must establish a regular and thorough review process for all USSS systems, which is designed to identify and mitigate or remediate privacy risks. The authority to regulate access to information in the system also helps reduce the risk of a privacy incident, even by those that may be authorized users.[48] As part of that review, the USSS Privacy Office should establish user access reviews at regularly scheduled intervals to ensure that only individuals with a job-related requirement/need-to-know have access to sensitive systems and information. Those individuals who no longer require access should be purged from the system. The access to USSS systems and sensitive information should be based on policies and procedures that define specifically the necessary roles, responsibilities, and access requirements of individual users. To that end, the Secret Service Privacy Office should also become more involved in the process by which determinations of system access are made, specifically in the development of policies and procedures that definitively outline role-based permissions.

*Recommendations*

8. USSS Privacy Office should improve processes and increase oversight of USSS compliance with federal privacy laws and regulations and DHS privacy policies. This includes timely submission of privacy compliance documents on all privacy sensitive systems/programs/operations.

---

[47] 44 U.S.C. §§ 3551-3558 outlines a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.

[48] The DHS Privacy Incident Handling Guidance notes that a privacy incident 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 have access or potential access to PII in usable form, whether physical or electronic, or where authorized users access PII for an unauthorized purpose.

9. As a best practice, USSS should continue annual records reviews to ensure any permanent records that are eligible for transfer to NARA are transferred and that all records are appropriately stored or deleted according to approved records retention schedules.
10. USSS Privacy Office should ensure it supports USSS implementation of DHS Directive Number: 262-05 regarding Information Sharing and Safeguarding by applying appropriate governance mechanisms in the development of information sharing arrangements and ensuring all agreements have all required privacy compliance documents. USSS should ensure the DHS Privacy Office reviews and approves all information sharing and access agreements to determine if they comply with applicable privacy law and adequately protect individuals' privacy.
11. USSS Privacy Office should work with USSS CIO and system and program managers to develop and conduct regularly scheduled user access audits on all privacy sensitive systems to determine if a user has a continued need to know and remove access for those that do not. Users should be required to complete annual privacy training and affirm knowledge of relevant privacy SOPs for each system to retain access.

## E. Training

*Finding: Improved FOIA/Privacy Act training is provided to new employees and certain USSS divisions, but more could be done to provide USSS personnel with a greater understanding of privacy requirements and best practices on an ongoing basis.*

The provision of privacy-specific training is key to establishing a fundamental understanding among all employees of the need to protect and safeguard personally identifiable information. It is not only necessary to provide this training upon the onboarding of new employees and contractors, but also as an ongoing effort to account for the changes in policy and legislation that govern the protection of sensitive information and raise awareness on a continuing basis. While the Secret Service is providing much improved orientation-based privacy training, it has not built a substantial recurring training regimen. Additionally, the USSS Privacy Office does not currently have the ability to effectively track the completion of mandatory privacy training, or to enforce training requirements.

As outlined in the OMB Circular Number A-108,[49] all federal agencies are required to establish sufficient training mechanisms to provide their personnel with an understanding of the Privacy Act, OMB guidance, the agency's implementing regulations and policies, and any job-specific

[49] *See:* OMB Circular No. A-108: Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act (December 2016), *available a:t* https://www.federalregister.gov/documents/2016/12/23/2016-30901/reissuance-of-omb-circular-no-a-108-federal-agency-responsibilities-for-review-reporting-and.

requirement related to privacy. Under OMB Circular A-130,[50] each SAOP must assess and address the training and professional development needs of his/her agency with respect to privacy. As such, agencies shall develop, maintain, and implement mandatory agency-wide privacy awareness and training programs that are consistent with applicable OMB, National Institute of Standards and Technology (NIST), and Office of Personnel Management (OPM) policies, standards, and guidelines for all personnel. This training should include foundational information, *as well as more advanced, role-based privacy training* (emphasis added) to information system users, managers, senior executives, and contractors. Per the DHS Privacy Office Guide to Implementing Privacy,[51] the DHS Privacy Office developed a training course, *Privacy at DHS: Protecting Personal Information*, which is to be completed annually by all DHS employees and contractors. The course expands on basic privacy concepts in order to build an understanding among DHS personnel of the Privacy Act and E-Government Act, as well as the proper use and protection of PII. Supplemental training offered by the DHS Privacy Office to Component personnel includes instruction on privacy basics, as well as the drafting and development of privacy compliance documents such as PTAs, PIAs, and SORNs. Advanced, role-based privacy training, however, is best created and delivered by the Component Privacy Office given its awareness of the Component's mission and culture. Lastly, in order to facilitate auditing and accountability the USSS Privacy Office should track the provision and completion of all privacy-related training to employees and contractors.

The USSS Privacy Office provided training slide decks used during Uniformed Division and Special Agent training, which is required of all new officers. This training, led by a certified instructor from USSS's Office of the Chief Counsel, provides a comprehensive overview of the Privacy and Freedom of Information Acts. The instructor includes examples that make the presentation relevant to USSS personnel and explains why these two laws should be important to participants during their course of work. The DHS Privacy Office compliments USSS in developing and delivering this role-based training and encourages the USSS Privacy Office to capitalize on these resources to develop opportunities to provide existing personnel, including system managers, senior executives, and contractors, with refresher training as appropriate.

For other USSS personnel, the USSS Privacy Office provides training during the orientation process for new personnel. While the time allotted here is less than that of the role-based training noted above, the USSS Privacy Office should take advantage of the examples used in the role-based training to make the topic more relevant and engaging for new employees. The USSS Privacy Office should also offer its system administrators and managers customized privacy training that not only raises awareness of privacy best practices, but reinforces the need to ensure privacy compliance when overseeing USSS systems. Due to staffing and resource shortages, the USSS Privacy Office has sought the assistance of the DHS Privacy Office in providing advanced

---

[50] *See:* OMB Circular No. A-130: Managing Information as a Strategic Resource (July 2016), *available at:* https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.

[51] *See:* The DHS Privacy Office Guide to Implementing Privacy (June 2010), *available at:* https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf.

and ongoing training to its personnel. When the USSS Privacy Office is appropriately resourced, the Secret Service Privacy Office should assume this responsibility given its awareness of mission critical elements and USSS culture. In the meantime, a more active, engaging, and robust outreach awareness campaign could occur to keep privacy responsibilities at the forefront of USSS personnel, addressing the OIG's findings that USSS personnel were "unaware" of component specific privacy responsibilities.[52] The Secret Service Privacy Office provided examples of posters and flyers used to spread awareness, which could be more effectively and frequently used until such time as the office is able to offer relevant privacy training for existing staff. The Privacy Office should reach out to specific programs and offices to provide position-related privacy training designed to identify functional privacy issues that employees and contractors might encounter.

In addition to recommendations for recurring training, the USSS Privacy Office should have the ability to track the completion of required privacy training as well as the authority to require completion. In an effort to improve its tracking of training efforts, the Secret Service is moving from its current Learning Management System (LMS), which does not provide a means of accounting for training completed by contractors, to the DHS Performance and Learning Management System (PALMS),[53] which will provide a much more robust and real-time tracking capability for all personnel across the agency. As this occurs, the USSS should address the Privacy Office's inability to effectively enforce training requirements and provide a mechanism to do so. The USSS Privacy Office confirmed with the USSS Office of Training that there is a mechanism in PALMS for the USSS Privacy Office to access reports to identify employees who have not taken required training and requested email notifications to report employees' failure to complete the mandatory privacy training, as well as mandatory social media training for authorized USSS users.

Secret Service reported that in Fiscal Year 2016, 5,347 (82 percent) of the 6,508 individuals employed by the service completed the department-mandated "Privacy at DHS: Protecting Personal Information" training. The USSS Privacy Office cited the deployment of personnel in support of operational objectives, including preparation for the 2016 Presidential Campaign and the Inauguration as the reason for a reduced completion rate. Despite the operational draws on USSS personnel, there is no reason that a 100 percent completion rate for this mandatory training is not achievable. Currently, USSS depends on direct supervisors to review the status of each employee's training assignments and verify completion via LMS. If an employee fails to complete the training, the supervisor notes it in his/her annual or semi-annual performance evaluation and may submit a report to the Office of Integrity (ITG) for review and action. ITG applies a standard set of penalties dependent upon the type of infraction, however, the USSS Table of Offense Codes and Penalty Guidelines does not identify a specific penalty for failing to

---

[52] *See:* DHS Instruction 110-01-001: Privacy Policy for Operational Use of Social Media (June 2012), *available at,* https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf.

[53] *See*: DHS/ALL/PIA-049 Performance and Learning Management System (PALMS) (January 2015), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-palms-01232015.pdf.

complete required training. Additionally, all Secret Service offices are subject to compliance inspections every four years, at which time the Inspection Division would note failures to complete all assigned training in the office's evaluation. While this could be an effective way of oversight, waiting four years between reviews to determine training completion rates is too long.

While there does appear to be a process in place to identify and discipline USSS personnel that fail to complete mandatory privacy training, the disparity between the number of individuals employed by the Secret Service and the number of individuals that completed mandatory privacy training during FY 2016 suggests that this process is not enforced. With the move to PALMS, which is expected in August 2017, and the proposed email notifications, the USSS Privacy Office will have the ability to more proactively monitor training completion rates. However, the Secret Service should also consider implementing a user access restriction capability currently employed by other components and agencies that terminates access to computer systems if required privacy or social media training is not completed.

The involvement of the USSS Privacy Office in the creation, provision, and completion tracking of privacy-specific training is paramount to protecting and safeguarding personally identifiable information collected, maintained, and used by the Secret Service and creating a culture of privacy awareness within the Component. The Secret Service should institute a more substantial recurring training program, including regular outreach efforts, awareness campaigns, and on-site, role-based training for system and program personnel consisting specifically of compliance documentation-related instruction. The move from LMS to PALMS should help to bolster USSS's ability to track the completion of required privacy training assignments. The USSS Privacy Office should also become more involved in the tracking of privacy-related training, rather than relying on the four-year audit cycle of the ITG. This will ensure that the Privacy Office is involved at all levels of the process. However, simply tracking the completion of these tasks will not likely result in an increase in the successful completion of required trainings. To guarantee that employees complete necessary privacy training, USSS could consider revoking access to agency IT systems for individuals that fail to complete required courses.

*Recommendations*

12. USSS should overhaul the oversight of mandatory privacy training, to include organizational awareness for the handling and safeguarding of personally identifiable information; privacy incident handling, reporting, and mitigation practices; and compliance documentation requirements.

## IV. Conclusion

This PCR found that USSS requires significant resources to have an effective privacy program that incorporates robust outreach, collaboration, and oversight and made 12 recommendations for several areas in which USSS could improve their privacy posture. To that end:

- The DHS Privacy Office requests that the USSS Privacy Office monitor the implementation of this PCR's recommendations and update, as needed, relevant USSS privacy documentation to reflect the findings and/or outcomes of this PCR; and
- The DHS Privacy Office requests that the USSS Privacy Office provide a written report on the implementation status with supporting documentation as appropriate of all recommendations within 12 months of this PCR's publication date. For any recommendations, including best practice recommendations, that USSS has not implemented or has chosen not to implement in that timeframe, we request that USSS explain why the recommendations were not implemented.

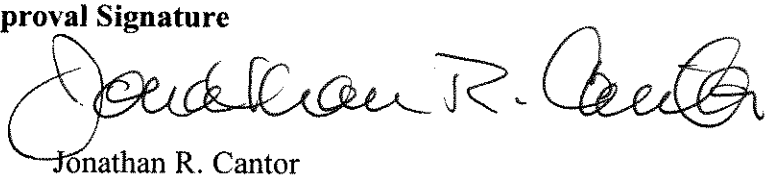
Finally, the DHS Privacy Office thanks USSS for their assistance in conducting this PCR and for being responsive to our inquiries throughout the PCR process. We look forward to working with USSS in the future to provide any and all support needed to assist in implementing the recommendations of this PCR.

## V. Privacy Compliance Review Approval

**Responsible Official**

George D. Mulligan
Chief Operating Officer
U.S. Secret Service
Department of Homeland Security

**Approval Signature**



Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security