# Privacy Compliance Review of the Science and Technology Directorate (S&T)

June 24, 2019


**Contact Point**

William M. Bryan
Senior Official Performing the Duties of the Under Secretary for Science and Technology
Science and Technology Directorate
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

The Department of Homeland Security (DHS) Privacy Office (PRIV) launched a Privacy Compliance Review (PCR) on July 27, 2018, under the Chief Privacy Officer's authority in accordance with Section 222 of the Homeland Security Act of 2002, and as a result of growing concerns that the DHS Science and Technology Directorate's (S&T) privacy compliance process, particularly for those programs involving social media and volunteers, did not meet requirements under DHS policies. The PCR reviewed DHS S&T's privacy compliance and privacy practices from October 1, 2016, through July 28, 2018.

The primary focus for this PCR was on DHS S&T's adherence to and implementation of privacy requirements set forth in DHS policy, including, but not limited to:

1. *Privacy Policy Directive 140-06, The Fair Information Practice Principles (FIPPs): Framework for Privacy Policy at the Department of Homeland Security;*[1]
2. *Privacy Policy Directive 140-09, DHS Policy Regarding Privacy Impact Assessments;*[2]
3. *Privacy Policy and Compliance Directive 047-01,*[3] *Privacy Policy and Compliance Instruction 047-01-001,*[4] *and DHS Instruction 047-01-005 for Component Privacy Officers;*[5]
4. *DHS Directive 140-06, Privacy Policy for Research Programs and Projects,*[6] *and Instruction 140-06-001, Privacy Policy for Research Programs and Projects Instruction;*[7] *and*
5. *DHS Directive 026-04: Protection of Human Subjects.*[8]

As a threshold matter, PRIV recognizes the S&T Privacy Office's staffing shortages that existed during this review and that continue to be a factor in the appropriate operation of the S&T Privacy Office. We support S&T Privacy Office efforts to address issues and make changes during the PCR that would quickly improve its privacy posture. However, this PCR makes additional recommendations that will require more in-depth improvements in the DHS S&T privacy program to ensure sustainability. This report attempts to discuss the situation at the time of review, while adhering to the roles and responsibilities of a well-functioning Component

---

[1] *Available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

[2] *Available at*: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-02-dhs-policy-regarding-privacy-impact.

[3] *Available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf.

[4] *Available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.

[5] *Available at*: https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf.

[6] *Available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-for-research-programs-and-projects-directive-140-06_0.pdf,

[7] *Available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-for-research-programs-and-projects-instruction-140-06-001_0.pdf,

[8] *Available at*: https://www.dhs.gov/xlibrary/assets/foia/mgmt-directive-026-04-protection-of-human-subjects.pdf.

privacy office that understands and plans for strategic information management and technology changes. We believe that DHS S&T senior leadership should seriously consider the findings in this report and use PRIV's recommendations to empower the S&T Privacy Office through prompt and correct staffing, resourcing, and other appropriate programmatic changes identified through this review.

## II. Scope and Methodology

*Scope*

The scope of this PCR focused on DHS S&T's implementation of departmental privacy policy, its privacy practices in general, and the overall privacy culture at DHS S&T. The PCR was also designed to review the privacy compliance of programs using social media and volunteers. However, once the review started, and PRIV was made aware of the imminent departure of the former S&T Privacy Officer, coupled with the lack of privacy documentation and historical analysis of projects, the scope shifted to promote privacy best practices in DHS S&T's newly staffed Privacy Office.

The 2009 Deputy Secretary's memo designating Component privacy officers was formalized in February 2017 via *DHS Instruction 047-01-005 for Component Privacy Officers*.[9] Pursuant to the direction of the Deputy Secretary, and continuing under this instruction, DHS S&T created the position of Privacy Officer in 2010. The S&T Privacy Officer is responsible for overseeing privacy compliance, policy, and oversight activities in coordination with the DHS Chief Privacy Officer.

*Methodology*

While PRIV launched this PCR in July 2018, the former S&T Privacy Officer left his position shortly thereafter, which quickly limited PRIV's access to certain information. PRIV compliments DHS S&T leadership and newly hired S&T Privacy Office staff and contractors for their responsiveness despite this limitation. The findings detailed in this PCR report reflect conclusions reached based on PRIV's historical interactions with the S&T Privacy Office, as well as an analysis of documents, responses, discussions, and other information received from the S&T Privacy Office over the course of our review. The recommendations herein promote best practices of well-functioning privacy program.

The PCR[10] 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 DHS S&T leadership and its Privacy Office and focused on implementation of DHS privacy policy as noted above.

---

[9] *See*: DHS Instruction: 047-01-005, *available at*: https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf, published February 2, 2017.

[10] *See*: DHS Instruction 047-01-004, *available at*: https://www.dhs.gov/publication/dhs-privacy-policy-instruction-047-01-004-privacy-compliance-reviews.

In conducting this PCR, the DHS Privacy Office:

- Reviewed relevant DHS S&T operational documents,[11] such as policies, draft Standard Operating Procedures, Notice and Consent documents, and social media documents;
- Met with S&T Compliance Division leadership and Privacy Office personnel on several occasions;
- Developed and distributed an initial questionnaire (July 2018);
- Reviewed initial DHS S&T responses and supporting documentation;
- Developed follow-up questions and received responses via email exchanges;
- Reviewed DHS S&T follow-up responses and supporting documentation;
- Drafted an initial PCR Report for DHS S&T comments (May 2019);
- Mitigated DHS S&T comments (June 2019); and
- Drafted and published final PCR Report (June 2019).

## III. Findings

### A. Summary of Recommendations

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

1. DHS S&T should promptly reorganize the S&T Privacy Office and fully comply with DHS Instruction 047-01-005.
2. DHS S&T should hire a Privacy Officer who is a senior level federal employee with significant experience and background in privacy.
3. DHS S&T should promptly fund and appropriately staff and resource the Privacy Office.
4. DHS S&T should better leverage and utilize the privacy compliance process to fully comply with departmental policies regarding the use of social media and human subjects as well as when undertaking privacy-sensitive research programs and projects.
5. The S&T Privacy Office should develop a thorough programmatic approach to privacy by incorporating and developing all aspects of a healthy privacy program, including policy, oversight, compliance, awareness, information sharing, incident management, training, and outreach.
6. As a best practice, the S&T Privacy Office should review and adopt DHS guidelines associated with records management.

[11] PRIV notes that our document review was hindered during the PCR due to a lack of transparent record keeping and document organization of the prior S&T Privacy Officer. While DHS S&T leadership were supportive and assisted with efforts at retrieval, the challenges associated with locating and retrieving documents in a less than acceptable records retention system and the departure of the S&T Privacy Officer within a month of the PCR's launch resulted in a piecemeal document production that yielded a minimal number of documents as well as documents lacking historical background and official status. Due to the challenges associated with accessing and reviewing eight years of unorganized, inaccessible, or non-existing documentation, PRIV decided to review the small universe of available documents and move forward with a best practices review of the S&T privacy program. This approach prevented pulling the small S&T Privacy Office staff away from addressing existing privacy issues and requirements.

## B. Explanation of Recommendations

*Finding: The DHS S&T organizational structure as well as the Privacy Office's location within the greater DHS S&T structure does not comply with DHS Instruction Number 047-01-005.*

### 1. DHS S&T should promptly reorganize the S&T Privacy Office and fully comply with DHS Instruction Number 047-01-005.

The current organizational position of the S&T Privacy Office does not comply with DHS Instruction 047-01-005. Office of Management and Budget (OMB) Circular No. A-130[12] 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,[13] 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 through the appropriate formal DHS process 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 instruction, 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,[14] the Department 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).[15]

In order to efficiently and effectively identify, mitigate, and reconcile privacy issues related to DHS S&T projects and programs, the S&T 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. DHS Instruction 047-01-005 states that the Component Privacy Officer reports directly to the Component Head. When the S&T Privacy Office was created in 2010, the Privacy Officer reported to the Chief of Staff, who reported to the Under Secretary for S&T. During the course of the PCR, S&T underwent a Component-wide revitalization that resulted in a reporting structure for the Privacy Officer that did not comply with DHS Instruction 047-01-005.

---

[12] *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.

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

[15] *See:* DHS Directive 047-01-001, July 2011, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.

In October 2018, the Privacy Office was moved from the Office of the Chief of Staff to the Compliance Division in the Office of Enterprise Services. Following the revitalization, the Privacy Officer now reports to the Director of the Compliance Division, who in turn reports to the Principal Director for the Office of Enterprise Services, who reports to the Executive Director for the Office of Enterprise Services. This organization then reports through the Office of the Chief of Staff to the Deputy Under Secretary for Science and Technology, who then reports to the Under Secretary for Science and Technology.

During discussions with DHS S&T leadership, they explained that moving the Privacy Office to the Compliance Division was meant to give the Privacy Office team greater access to and oversight of the programs that are most commonly impacted by privacy requirements. While the factual presentation is not without merit, there was no documentation at that point formalizing the Privacy Officer's placement that ensures the official is still able to execute the responsibilities required by DHS Instruction 047-01-005. To further explain this reporting structure, DHS S&T subsequently provided a memorandum and organizational chart to PRIV that documents and formalizes DHS S&T leadership support and confirms the Privacy Officer's authority and unobstructed access to the Under Secretary for major privacy issues[16]. PRIV considers this memorandum a move in the right direction, however, also notes that the S&T Privacy Office is not listed on the new organizational chart. This lack of visibility is problematic and does not indicate DHS S&T leadership's commitment to building a healthy privacy program. Therefore, PRIV retains the original finding that DHS S&T does not comply with DHS Instruction 047-01-005.

**2. DHS S&T should hire a Privacy Officer who is a senior level federal employee with significant experience and background in privacy.**

*DHS Instruction 047-01-005 for Component Privacy Officers*, outlines requirements for, and responsibilities of the Component Privacy Officer. Not only does the instruction require the Component Privacy Officer report directly to the Component Head, but it also requires that the Component Privacy Officer be a senior level federal employee with significant privacy experience, and be provided the appropriate levels of staff support and resources.

DHS S&T should hire a permanent, full-time, experienced, federal Component Privacy Officer. This PCR finds that DHS S&T maintained a misplaced confidence in the former Privacy Officer's leadership and competence. Thus, the formulation, development, implementation, and oversight of privacy matters within DHS S&T was inadequate to the point that a PCR was required. DHS S&T should carefully consider the requirements for a Component Privacy Officer set forth in DHS Instruction 047-01-005 to ensure that the final selection is an individual who is equipped with the requisite skillset to oversee a successful privacy program.

The former S&T Privacy Officer left his position on September 14, 2018. A newly hired Deputy Privacy Officer began in October 2018 and immediately assumed the duties of the S&T Privacy

[16] May 31, 2019 DHS S&T Memorandum to the DHS Acting Chief Privacy Officer.

Officer with support from two newly hired contractors. The Acting S&T Privacy Officer is responsible for the duties of both the Deputy and S&T Privacy Officers. Having one person handle the duties of two positions places the agency at a disadvantage and creates risk points in the execution of the privacy program.

As DHS S&T moves forward with hiring a dedicated Component Privacy Officer, DHS Instruction 047-01-005 should inform the selection process. The Component Privacy Officer position should be filled permanently with a *senior level federal employee* with *significant experience and background in privacy* [emphasis added]. In describing the duties of such officers, the instruction highlights the need for such individuals to possess expertise and experience with federal privacy laws and regulations as the foundation for their ability to advise Components and to interact with Component leadership to ensure compliance with privacy law and policy.

The position descriptions of Privacy Officers for the other Components named in the Deputy Secretary's memorandum reflect requirements for technical expertise and experience with federal statutes, regulations, and policies as well as the FIPPs. These individuals are required to collaborate with and advise Component leadership, including the Component Heads, Chief Information Officers, and other program managers to ensure the overall compliance and oversight of privacy within the Component and its programs and systems. These individuals are required to lead on all matters regarding privacy and the FIPPs, ranging from serving as the technical authority on the legal mandates to the formulation, development, implementation, and oversight of privacy initiatives with the Component.

On March 1, 2019, DHS S&T posted an agency-internal vacancy announcement for the open Privacy Officer position.[17] DHS S&T leadership requested PRIV involvement in the interview and selection process of the next S&T Privacy Officer. PRIV compliments DHS S&T on this collaboration, which demonstrates DHS S&T leadership's renewed focus on privacy compliance, and sees this as a step in the right direction towards developing a healthy privacy program at DHS S&T.

### 3. DHS S&T should promptly fund and appropriately staff and resource the Privacy Office.

This PCR finds that the historical and current S&T Privacy Office staffing has been and continues to be woefully insufficient to meet the Directorate's needs and cannot support the long term development and sustainability of a healthy privacy program throughout DHS S&T. The S&T Privacy Office currently has federal positions for a Privacy Officer and Deputy Privacy Officer, and two Privacy contractors. Given the S&T Privacy Office's historic shortcomings, need to redirect its privacy culture, and current workload for its unique mission,[18] its staffing

[17] *Available at*: https://www.usajobs.gov/GetJob/ViewDetails/525983600.

[18] DHS S&T should generate a significant amount of Privacy Threshold Analyses (PTA) annually for each of its pilots, research initiatives, projects involving social media or human subjects, etc., which historically have not been

levels are insufficient to meet existing privacy demands and DHS Instruction 047-01-005 requirements, let alone any new privacy requirements.

For the majority of the 10 years the S&T Privacy Office has been in place, it has had one permanent, full-time federal employee with support positions being held by contractors. There was a brief period (September 2013 through March 2015) when there was a second full time federal employee assisting with the DHS S&T privacy program. When the subordinate federal employee left, the position was not backfilled with another full-time federal employee.

Since the PCR started, DHS S&T has pledged to surge the number of contractors working within the S&T Privacy Office. PRIV acknowledges the immediate benefits of supplementing full-time federal employee staffing with additional contractors. Using contract staff can in some cases be more timely or cost efficient than hiring permanent federal employees. There are drawbacks, however, to using contract staff, including turnover and institutional knowledge. When the S&T Privacy Officer left in September 2018, the two contractors left behind were fairly new to the S&T Privacy Office and lacked the requisite institutional knowledge and authority to sustain, let alone move the program forward. With the creation and staffing of the Deputy Privacy Officer position, DHS S&T is starting to address this issue.

This PCR recommends a closer look at providing additional federal employees to support the S&T Privacy Officer and help the Privacy Officer meet the responsibilities outlined in DHS Instruction 047-01-005. A strong privacy office is an integral part of a modern information-focused organization,[19] especially one focused on activities that raise novel questions on the use of data and technology. Every aspect of DHS S&T's research, development, testing, and evaluation mission is replete with privacy risks, and a strong privacy office can help the Directorate think through a smart investment strategy, ensuring resources are not expended that will raise concerns at DHS partners when deployed for operational purposes. DHS S&T relationships also have novel risks, and a strong privacy office can help ensure that DHS equities are protected.

Due to current staffing shortages, the S&T Privacy Office is only able to focus on the most pressing aspects of the program, such as basic compliance documentation, Appendix G[20]

---

completed in a timely matter, if at all. While the S&T Privacy Office completes on average 35 PTAs per year, most PTAs PRIV has on record are still in draft and not sufficiently mitigated. Additionally, the S&T Privacy Office needs to dedicate an individual to handle privacy incidents related to DHS S&T equities.

[19] *See* OMB Circular A-130: Managing Information as a Strategic Resource (July 2016), Appendix 1, at pp. A-1 – A-2.

[20] *See* the DHS Homeland Security Acquisition Manual (HSAM), *available at*: https://www.dhs.gov/sites/default/files/publications/HSAM%20Conformed%20through%20Notice%202019-03.pdf. For acquisitions that do not require a written acquisition plan, the requirements official shall complete Appendix G - Checklist for Sensitive Information. If the requiring official determines that a contractor will have access to sensitive information and/or information systems will be used to input, store, process, output, and/or transmit sensitive information, the requiring official shall ensure the Statement of Work, Statement of Objective, Performance Work Statement, or specification is reviewed by the organizations identified at HSAM 3004-470(b) and obtain signatures, as applicable, on this checklist. The sheer volume of DHS S&T contracts for its numerous projects and pilots, and

reviews, and minimal outreach/training. Appendix G reviews occur for all contracts or awards of $150,000 or more. Appendix G requires the S&T Chief Information Officer, Security Officer, and Privacy Officer to review each Statement of Work (SOW) to determine if sensitive information such as PII, will be collected, used, or shared during the acquisition lifecycle. The S&T Privacy Officer completed 1,245 Appendix G reviews for FY 2018. This translates into 1,867.50 man hours or 233.5 days spent on Appendix G reviews for Fiscal Year 2018. From January 1-March 6, 2019 the S&T Privacy Officer conducted 106 Appendix G reviews, which translates into 159 man hours or approximately 20 work days. With the Privacy Officer devoting such a large portion of time to Appendix G reviews, other parts of the privacy program become neglected and are placed at risk.

To further implement responsibilities in DHS Instruction 047-01-005, the S&T Privacy Office should dedicate a staff member to lead investigations and remediation activities on DHS S&T PII incidents. While historically DHS S&T has reported relatively few PII incidents, PRIV considers that this could be due to lack of employee awareness of what constitutes a PII breach, lack of awareness on how to report a PII breach, or simple indifference. With dedicated staff, awareness and training would increase and the Privacy Office would be able to spot trends in incidents to improve employee response. This will require DHS S&T obtaining access to the Department's Enterprise Cyber Operations Portal (ECOP) to have the ability to directly assess and mitigate reported suspected or confirmed incidents.[21]

Additionally, as a best practice, the S&T Privacy Office, in conjunction with the Office of the Chief Human Capital Officer, should conduct a robust Workforce Planning Analysis[22] to improve the chance for sustainability once these initial staffing concerns are addressed. As DHS S&T works with the Office of the Chief Human Capital Officer, it should take into consideration a staffing model the melds a talent base familiar with the underlying programs of DHS S&T's unique mission with experienced privacy personnel.[23]

---

the fact that Privacy Office contractors are forbidden from conducting such reviews, consumes the majority of the Privacy Officer's attention.

[21] During this transition, the S&T Privacy Office will receive full support from the DHS Privacy Office Director of Incidents.

[22] A Workforce Planning Analysis will serve as the foundation for managing the S&T Privacy Office's human capital needs and requirements. It will also enable the S&T Privacy Office to strategically meet current and future workforce needs to prevent unnecessary disruptions as experienced while the Privacy Officer and Deputy Privacy Officer positions were vacant.

[23] For example, the U.S. Immigration and Customs Enforcement (ICE) Privacy Office focuses on hiring individuals with a privacy background and familiarity with law enforcement programs and requirements. The Cybersecurity and Infrastructure Protection Agency (CISA) Privacy Office focuses on hiring individuals with privacy experience and cyber and technology knowledge. DHS S&T should also focus on developing a privacy staff with a depth of privacy knowledge and backgrounds in the areas handled by DHS S&T, particularly research, testing, development, and evaluation methodologies.

*Finding: S&T Privacy Office's limited resources combined with DHS S&T's unique mission within the Department, lead to ineffective privacy compliance with departmental policies and instructions.*

4. **DHS S&T should better leverage and utilize the privacy compliance process to fully comply with departmental policies regarding the use of social media and human subjects as well as when undertaking privacy-sensitive research programs and projects.**

One of the underlying reasons for this PCR was the timeliness of, and unmitigated privacy concerns within, DHS S&T's privacy compliance documentation for social media exercises involving volunteers.[24] During the course of this PCR, the S&T Privacy Office provided minimal documentation of how the Directorate complies with departmental policies regarding social media[25] or human subjects.[26] PRIV acknowledges that due to the departure of the previous S&T Privacy Officer, access to historical and complete documentation was a challenge for the current Privacy Office staff. However, based on PRIV's compliance holdings for DHS S&T pilots and projects involving social media and volunteers, this PCR makes this recommendation to reiterate the importance of the Department's privacy compliance process to ensure DHS S&T sustains and does not erode privacy protections when it undertakes privacy-sensitive research programs and projects.[27]

The Department's privacy compliance process begins with a Privacy Threshold Analysis (PTA). A fully-mitigated PTA is a required document that serves as PRIV's official determination as to whether a DHS program or system (including pilots) has privacy implications, and if additional privacy compliance documentation is required (such as a PIA and SORN). For DHS S&T's use of social media in its testing or research, for example, a completed PTA in advance of testing is required. A completed PTA also satisfies DHS Directive 026-04's requirement that the Chief Privacy Officer ensures that privacy-sensitive research programs and projects follow DHS privacy policy and standards.[28] The purpose of a PTA is to identify programs and systems that are privacy-sensitive, demonstrate the inclusion of privacy considerations during the review of a

---

[24] *See*: https://www.dhs.gov/science-and-technology/news/2017/10/31/news-release-ny-first-responders-train-critical-incident.

[25] *DHS Directive 110-01: Privacy Policy for Operational Use of Social Media* applies to "any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual." Note that DHS S&T is required to do a PTA for any social media tools even if they are not operationalizing the use of social media. DHS S&T may choose to do a joint PTA with the operational Component if there is a pilot and the operational Component would also be required to complete and provide PRIV with the Social Media Operational Use Template, *available at*: http://dhsconnect.dhs.gov/org/comp/nppd/privacy/Pages/Privacy-and-Social-Media.aspx.

[26] *DHS Directive Number 026-04: Protection of Human Subjects* requires DHS S&T to "closely coordinate all programmatic procedures and policies with [PRIV…]" and to "work with [PRIV] to develop procedures associated with human subjects research to ensure that individual privacy interests are fully respected."

[27] 6 U.S.C. § 142.

[28] *See:* DHS Directive 026-04, Attachment, Principles for Implementing Privacy Protections in DHS Research Projects.

program or system, provide a record of the program or system and its privacy requirements, and demonstrate compliance with privacy laws and regulations.

The S&T Privacy Office should review the historical compliance documentation that has been shared with PRIV. These draft compliance documents will provide insight into the issues that need to be addressed moving forward. The S&T Privacy Office should also develop Standard Operating Procedures (SOP), DHS S&T specific policy guidance, and an outreach/training program to ensure that privacy principles are embedded in all programs involving social media and the public.

*Finding: DHS S&T lacks a thorough programmatic approach to privacy.*

5. **The S&T Privacy Office should incorporate and develop all aspects of a healthy privacy program, including, compliance, policy, information sharing,[29] incident management, oversight, training, and outreach.**

DHS Instruction 047-01-001 states that the Component Privacy Officer is responsible for "maintaining an ongoing review of all Component information technology (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." These responsibilities serve as the core functions for a healthy privacy program.

A healthy privacy program addresses all aspects of privacy, compliance review and documentation, policy development, incident handling and response, information sharing review, program oversight, outreach awareness, and training. A well-developed privacy program ensures that privacy is included throughout the lifecycle of every project and program. DHS S&T needs to build a compliant and healthy privacy program.

Compliance

DHS Instruction 047-01-005 states that the Component Privacy Officer is responsible for preparing "Privacy Threshold Analyses, Privacy Impact Assessments, and System of Records Notices, as well as any associated privacy compliance documentation, as directed by the DHS Privacy Office policy or required by law." This requirement creates the basis for the Component compliance program.

Compliance documentation is an important part of a thriving privacy program. The PTA, PIA, and SORN are the tools through which DHS assesses privacy in departmental IT systems and programs and is able to track PII inventories. They provide necessary transparency to the public into DHS operations, and ensure that the Department is mitigating risks to privacy. As part of the privacy compliance process, the DHS Privacy Office works with Component Privacy Officers, Privacy Points of Contact (PPOC), program managers, system owners, and IT security personnel

[29] While PRIV could not adequately review the S&T Privacy Office's oversight of DHS S&T information sharing activities, this is part of a healthy privacy program.

at Headquarters and DHS Components to ensure that sound privacy practices and controls are integrated into the Department's operations. To assist those responsible for completing privacy compliance documentation, the DHS Privacy Office published official Department guidance[30] regarding the requirements and content for PTAs, PIAs, SORNs, and Privacy Act (e)(3) Statements.[31]

Based on PRIV's historical interactions with the S&T Privacy Office, and confirmed over the course of this PCR, the S&T Privacy Office produces minimal privacy compliance documentation, despite its research and development projects that include PII, and does not follow the prescribed PTA process. DHS S&T's privacy compliance documentation also historically lacks timeliness and completeness. These processes are not optional.

During the course of this PCR, the S&T Privacy Office noted that, together with the program manager, it may draft and sign a "memorandum for the record" describing the project and stating that the project does not collect any PII and that the project is not privacy sensitive. This practice erodes the principles set out in *Privacy Policy Directive 140-09, DHS Policy Regarding Privacy Impact Assessments*[32] that requires DHS's Chief Privacy Officer to conduct PIAs in accordance with its statutory authorities. The PTA process, discussed above, was established to assist the Chief Privacy Officer with making a determination as to whether or not a system/project is privacy sensitive and if other privacy compliance documentation is required. The Component Privacy Office is charged with providing its expert analysis to PRIV, but is not independently authorized to make this determination, even on systems/projects that the program manager deems to not impact privacy.

For PTAs that have been provided to PRIV, DHS S&T's submissions have historically been late and incomplete. For several major projects conducted by DHS S&T, the privacy compliance documentation was not submitted until the project was ready to start. Often, there was no time to fully adjudicate privacy concerns, much less bake privacy best practices into the project. The historic lack of timeliness points to a privacy program that is not embedded into the everyday processes of DHS S&T.[33] DHS S&T leadership should fully implement *DHS Instruction 047-01-005 for Component Privacy Officers* to ensure its Privacy Office provides effective privacy compliance oversight from the very beginning.

---

[30] *See*: DHS Privacy Office Guide to Implementing Privacy, *available at*: https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf.

[31] Disclosures required by Section (e)(3) of the Privacy Act appear on documents used by the Department to collect PII from individuals to be maintained in a Privacy Act System of Records. 5 U.S.C. § 552a(e)(3).

[32] *Available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-02.pdf.

[33] During the course of this PCR, the S&T Privacy Office noted that it was included in very specific meetings relating to the proposal and development of certain projects. It was also noted that Appendix G reviews provided insight into DHS S&T activities. PRIV notes these meetings and reviews are a worthy starting point, but are minimally beneficial if the Privacy Office does not increase engagement with its clients. Ongoing collaboration with the program managers is necessary to address privacy compliance and policy requirements.

It is worth noting that with the recent addition of the Deputy Privacy Officer and two contractors during the course of the PCR, PRIV notes that the overall quality and timeliness of privacy compliance documentation has improved. Changing the compliance expectations within DHS S&T program offices will take time, however, to meet PRIV's expectations for an effective S&T Privacy Office. The S&T Privacy Office should continue to develop timely, high quality, comprehensive compliance documents and work with the PRIV Compliance team to continue to address privacy compliance issues. However, compliance is just one part of a healthy privacy program.

Policy

Policy implementation and development are important elements of an effective privacy program, as well. *The DHS Privacy Office Guide to Implementing Privacy*[34] establishes the need for policy development at the Chief Privacy Officer level and the Component Privacy Officer level, as appropriate. PRIV implements the policies outlined in its Directive, as well as other federal laws and regulations, by issuing policies and procedures, policy guidance, and memoranda across the Department. These documents explain the criteria for collecting and using PII in a manner that furthers the Department's mission, yet minimizes the impact on individual privacy.

Component Privacy Officers and PPOCs develop Component-level privacy policies as needed to reflect and further the mission of the Component, ensuring that such privacy policies are consistent with DHS Privacy Office policies and the FIPPs. Such policies often address specific mission roles or programs. They can also inform development of DHS-wide policies. PRIV reviews privacy policies and guidance developed by Component Privacy Officers and PPOCs to ensure consistency in privacy policy across the Department.

Currently, DHS S&T lacks policy development in its privacy program and should develop a Component specific privacy policy program due to its unique mission and unique projects. For example, the S&T Privacy Office should promptly focus on pilots and other research projects that collect and use social media, and develop policy that reflects the operational needs of DHS S&T and its customers while implementing DHS privacy policy for social media. During the PCR, the S&T Privacy Office provided two draft policy documents to PRIV, one finalized policy document, and referenced DHS privacy policy documents in response to the remaining PCR policy questions.[35] DHS-wide privacy policy is the minimum requirement that should be promoted and implemented within the Component, but tailored privacy policy can better meet the Component's needs. The S&T Privacy Office's lack of policy development does not contribute to building a robust privacy program, so it should develop a privacy policy program to address the unique privacy issues that arise in its distinctive mission within DHS.

[34] *Available at*: https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf.
[35] The S&T Privacy Office provided a finalized Standard Operating Procedure regarding privacy incidents, a draft Privacy SOP dating back to 2013, and a draft social media guidance document that DHS S&T was writing on behalf of PRIV, but had not contacted PRIV to advise that the document was being created.

Incident Management

Privacy incidents, whether accidental or malicious, can pose specific risks to individuals, because there is an increasing recognition that personal information, such as Social Security numbers, financial account information, health information, and biometric data, is valuable and can be reverse engineered with a potential for great public harm. Therefore, it is crucial that DHS personnel be able to identify and report a suspected or confirmed privacy incident.[36] This is a difficult task if employees do not receive training and guidance on properly handling PII and identifying privacy incidents.

This PCR found that the S&T Privacy Office provides minimal outreach and training on what constitutes a privacy incident and what should be done when a privacy incident occurs. During the course of the PCR, the PRIV Director of Incidents reviewed the types of incidents occurring at DHS S&T and the degree of assistance provided by the S&T Privacy Office to resolve reported incidents. The total number of reported incidents was low during the time frame covered by the PCR. However, without additional insight from the S&T Privacy Office, it is difficult to know whether the incident numbers are low due to careful handling of PII or due to a lack of understanding and ability to identify privacy incidents. Additionally, of the incidents that were reported, minimal support was provided to the PRIV Director of Incidents to mitigate the incident.

PRIV recommends the S&T Privacy Office assign a staff member to lead training, awareness, investigations, and remediation activities on future DHS S&T privacy incidents. The DHS S&T staff lead for incidents should be someone other than the S&T Privacy Officer. Given the workload already handled by the S&T Privacy Officer, such a designation will fail to produce the attention and response time needed to mitigate incidents. In order for the S&T Privacy Office to become more fully invested in incident management, the DHS S&T staff lead will need to obtain access to ECOP to have the ability to directly assess reported suspected or confirmed incidents. Additionally, a dedicated incident staff member could provide the requisite outreach and training for DHS S&T personnel.

Oversight

Program oversight is an integral part of all privacy programs. Effective oversight protects the Department, helps ensure compliance with laws and policies, and provides guidance when issues arise. Privacy oversight is difficult if the privacy program is not embedded in the overall structure of the organization and aware of the programs and projects being undertaken by the agency. As the S&T Privacy Office becomes more embedded in the mission of DHS S&T, the front-end oversight function through compliance, policy development, training, outreach, and privacy incident handling should mature and become a natural part of the overall program. Fully

[36] *See*: Privacy Incident Handling Guidance, *available at:* https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf.

implementing the responsibilities of DHS Instruction 047-01-001[37] and DHS Instruction 047-01-005[38] provides ample oversight opportunities for the S&T Privacy Office. The S&T Privacy Office should be accountable for complying with DHS privacy policy, providing training to all employees, contractors, and others working on behalf of DHS S&T who use PII, and auditing the actual use of PII to demonstrate compliance with fair information practice principles and all applicable privacy protection requirements.

Training and Outreach

The provision of privacy-specific training is key to establishing a fundamental understanding among all employees and others working on behalf of DHS S&T of the need to protect and safeguard personally identifiable information. It is not only necessary to provide this training to new employees, contractors, and others working on behalf of DHS S&T, but also as an ongoing effort to account for the changes in policy and legislation that govern the protection of such information and to continually raise awareness. Training is particularly relevant for DHS S&T due to its unique mission within the Department. This PCR finds that the S&T Privacy Office has not built a substantial recurring training regimen that addresses the unique nature of DHS S&T's programs and projects. Additionally, the S&T 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,[39] 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 requirement related to privacy. Under OMB Circular A-130,[40] 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,[41] the DHS Privacy Office developed a training course, *Privacy at DHS: Protecting Personal Information*, which is to be completed annually by all DHS

---

[37] *Available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.

[38] *Available at*: https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf.

[39] *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.

[40] *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.

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

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, should be created and delivered by the S&T Privacy Office given DHS S&T's unique mission and role within DHS. Lastly, in order to facilitate auditing and accountability, the S&T Privacy Office should track the provision and completion of all privacy-related training to employees and contractors.

During the PCR, the S&T Privacy Office provided PRIV with overview privacy training presentations for the years 2011, 2013, 2014, 2015, and 2017 and noted research-specific training material. However, these were broad, overview presentations (not much different from the mandatory DHS-wide privacy training) and there was no record of when the training occurred or who attended. As part of her outreach effort across the Directorate, the new Acting Privacy Officer developed a presentation for S&T Project Managers that addresses the role of the Privacy Office in the DHS S&T organizational structure. The S&T Privacy Office should overhaul the delivery and oversight of mandatory privacy training, to include organizational awareness for handling and safeguarding PII; privacy incident handling, reporting, and mitigation practices; and privacy compliance documentation requirements.

Of particular relevance to DHS S&T given its high number of contractors and others who perform work on behalf of the Directorate, the S&T Privacy Office should also require that all non-employees working on behalf of the Directorate complete and submit completion certificates from DHS sponsored privacy training.[42] PRIV recommends that these individuals take DHS hosted privacy training to ensure that all DHS privacy policy and best practices are conveyed in a timely fashion. DHS S&T should collect, and provide the S&T Privacy Office access upon request, completion certificates from all contractors and others performing work on behalf of DHS S&T and track training compliance for the life of the arrangement. While a more thorough, DHS S&T mission-specific training program is ideal, given the current staffing levels and accompanying time constraints, this is not a project slated for the near future.

The S&T Privacy Office plans to work with PRIV to develop advanced training for its personnel, which PRIV supports. In addition to the training programs offered by the DHS Privacy Office, a number of the Component Privacy Offices, including those at the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), and U.S. Customs and Border Protection (CBP), have constructed their own privacy training and awareness programs tailored to meet the needs of their staff, programs, and systems. As part of their recurring training and

[42] More information on DHS Security and Training Requirements for Contractors, including required privacy training, *available at*: https://edit.dhs.gov/dhs-security-and-training-requirements-contractors; *see:* "Privacy at DHS: Protecting Personal Information".

outreach efforts, some Components hold training supplemental sessions such as All Hands Training and Privacy Awareness Weeks, Privacy Awareness Days, one-hour sessions on protecting privacy, or poster campaigns that promote the protection of PII. The S&T Privacy Office should look to these other privacy training and outreach programs for ideas on developing mission specific training requirements.

In addition to recommendations for recurring training, the S&T Privacy Office should have the ability to track the completion of mandatory training through the headquarters Performance and Learning Management System (PALMS) as well as the authority to require completion for all DHS S&T personnel. The involvement of the S&T 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 DHS S&T and creating a culture of privacy awareness within the Directorate. The S&T Privacy Office 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 S&T Privacy Office has historically labored with minimal resources and has been unable to fully embed privacy and build a robust privacy program. Moving forward, DHS S&T leadership should provide the S&T Privacy Office with the requisite resources and staffing levels to ensure the development of a healthy, well rounded privacy program. As DHS S&T implements the PCR recommendations to improve the overall function of its Privacy Office, possible technical or policy changes should be fully considered to allow greater training oversight by the S&T Privacy Office.

**6. As a best practice, the S&T Privacy Office should review and adopt DHS guidelines associated with records management.**

Records are the foundation of open government, supporting the principles of transparency, participation, and collaboration. Well-managed records can be used to assess the impact of programs, to improve business processes, and to share knowledge across the Government.[43] DHS Directive 141-01[44] establishes the DHS Records and Information Management (RIM) Program and sets forth the policies for managing records regardless of medium, lifecycle stage, or environment. DHS S&T should review, adopt, and incorporate DHS records management guidelines into its privacy program.

From the PCR's outset, issues with the S&T Privacy Office's records management program proved problematic. After the prior S&T Privacy Officer's departure, it was discovered that all relevant privacy program documentation existed on the former Privacy Officer's laptop. The majority of the documentation provided by DHS S&T during the review was uncovered in unorganized emails. The PCR was hindered due to a lack of transparent record keeping and document organization of the prior S&T Privacy Officer. The challenges associated with

[43] OMB Managing Government Records Directive M-12-18, *available at*: https://www.archives.gov/files/records-mgmt/m-12-18.pdf.
[44] *Available at*: http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/141-01.pdf#search=records%20and%20information%20directive.

locating and retrieving documents in a less than acceptable records retention system and the departure of the S&T Privacy Officer within a month of the PCR's launch resulted in a piecemeal document production that yielded a minimal number of documents as well as documents lacking historical background and official status. Due to the challenges associated with accessing and reviewing eight years of unorganized email documentation, PRIV decided to review the small universe of available documents and move forward with a best practices review of the S&T privacy program. This approach prevented pulling the small S&T Privacy Office staff away from addressing existing privacy issues and requirements, but hindered aspects of the PCR process.

To its credit, during the course of the PCR, the S&T Privacy Office took the following steps to rectify the records management issue:

1. Developed an S&T Privacy Office Shared Drive, which is a centralized location for privacy documentation.
2. Established a basic file plan for the Shared Drive.
3. Sorted files, folders, and documents received into the Shared Drive from the prior S&T Privacy Officer's laptop while maintaining, under a separate folder, the source materials transferred from the prior Privacy Officer's laptop.
4. Established records on adjudicated PTAs for 2014 through 2018:
    a. Worked with DHS PRIV to obtain missing adjudicated PTAs.
    b. Developed an S&T Privacy Tracker for 2014 to current adjudicated PTAs, including information on PIAs and SORNs, if any, related to each adjudicated PTA (including both S&T PIAs and SORNs; DHS-wide PIAs and SORNs; and DHS Component PIAs and SORNs; expiration dates; post-adjudication action, if any, required for a PTA; etc.).
    c. Working with DHS PRIV to reconcile information on PTAs adjudicated during calendar years 2014-2018 to define follow up, if any required, by DHS PRIV and/or the S&T Privacy Office.
    d. Initiating activities necessary to contact PTA-designated program managers regarding status of initiatives under expired or expiring PTAs to determine required follow up actions.
5. Established centralized records on all active DHS S&T PIAs.
6. Established a central file folder for completed Appendix G reviews starting in 2018, which contains information on each Appendix G review and comments on the SOW and Appendix G documents, including whether a PTA may be or is required with regard to that SOW.
7. Established separate issue-specific folders and subfolders to assure access to current and historical matters.

Since the start of the PCR, DHS S&T has worked to incorporate several records management guidelines into its processes and PRIV encourages those efforts to continue moving forward. PRIV compliments the S&T Privacy Office on the steps outlined above and considers these positive indicators that the S&T Privacy Office is taking its records management obligations seriously. The records management practices described in the PCR ensure that some of the

problems described in the PCR will not arise again in the future. In addition to the steps above, as a best practice, PRIV also recommends additional training and coordination with the S&T Records and Information Management Officer, as well as the development of a Privacy Office Standard Operating Procedure for records management, if appropriate.

## IV. Conclusion

This PCR found that DHS S&T requires significant resources to have an effective privacy program that incorporates robust compliance, oversight, outreach, and collaboration and made six recommendations for areas in which S&T could improve their privacy posture. To that end, the DHS Privacy Office requests that the S&T Privacy Office:

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

The DHS Privacy Office would like to thank DHS S&T for their assistance in conducting this PCR and for being responsive to our inquiries throughout the PCR process. We look forward to working with DHS S&T in the future to provide any and all support needed to assist in implementing this PCR's recommendations.

## V. Privacy Compliance Review Approval

### Responsible Official

William M. Bryan
Senior Official Performing the Duties of the Under Secretary for Science and Technology
Science and Technology Directorate
U.S. Department of Homeland Security

### Approval Signature

[Original signed copy on file with the DHS Privacy Office.]

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