Data Privacy and Integrity Advisory Committee

April 26, 2022

AGENDA

I. Call to Order & Roll Call

II. Opening Remarks

III. Policy Subcommittee Report and Discussion

IV. Emerging Subcommittee Report and Discussion

V. Public Comment

VI. Meeting Adjourned

Call to Order & Roll Call:

Bill Bice, Deputy Designated Federal Official

Opening Remarks:

Lisa Sotto, Chairperson, Data Privacy and Integrity Advisory Committee (DPIAC)

Brief Remarks to the Committee

Chief Privacy Officer Lynn Parker Dupree

Dennis Dayman
DPIAC Policy Subcommittee Chair

Policy Subcommittee Recommendations

- Fact findings:
  - The Data Privacy and Integrity Advisory Committee ("DPIAC" or "Committee") was tasked with providing recommendations on how the Privacy Office could better oversee information sharing across the Department of Homeland Security ("DHS") offices and components.
  - DPIAC sub-committee focused its review specifically on information sharing involving PII and/or sensitive PII pertaining to U.S. persons or special protected classes of individuals.
  - The sub-committee further narrowed its focus to external information sharing only (i.e., DHS sharing PII with other federal agencies, foreign partners, or the private sector).
  - To understand existing information sharing practices at DHS and provide written guidance on best practices, sub-committee members reviewed both public and non-public DHS materials stated in the report relevant to the Tasking.
  - Sub-committee members also met with DHS personnel over the course of several months.
    - Use of governance structures, including leveraging governance bodies or oversight technologies to track information sharing activities;
    - Supplementing existing processes, such as privacy compliance documentation (i.e., Privacy Impact Assessments) or other Departmental processes that could be leveraged; and
    - Establishing or updating privacy policies.

Policy Subcommittee Recommendations

- Privacy Office Authority :
  - The Privacy Office has a framework of policies, procedures, and guidance to administer its privacy program and has statutory authority to ensure that all DHS information sharing agreements comply with Privacy Act and E-Government Act requirements as well as DHS's privacy policy.
  - The Privacy Office policy for reviewing Information Sharing Access Agreements (ISAAs) is rooted in the Homeland Security Act of 2002, which calls for the Privacy Office to ensure that use of technology sustains and does not erode privacy protections.
  - Instruction calls for Component Privacy Officers and Privacy Points of Contact (PPOCs), and other DHS employees as appropriate, to submit all proposed ISAAs involving PII to the DHS CPO for review and approval prior to finalizing them. The DHS Privacy Office has developed a specialized PTA template components it should use to conduct privacy compliance assessments of ISAAs.
  - Information sharing arrangements do not always originate within the DHS Privacy Office and may not be subject to Privacy Office review or approval, there is no current mechanism in place for the Privacy Office to track and monitor all information sharing programs, or for the Privacy Office to identify pending or executed ISAAs across DHS and its component agencies (e.g., the Federal Emergency Management Agency).

Policy Subcommittee Recommendations

- Overview:
  - ISAAs may inherently require sharing of PII to achieve DHS initiatives and objectives. However, any improper use or disclosure of such information may impact national security or other important interests of the United States; harm the individuals the PII relates to; violate laws, regulations, and/or contracts; and otherwise cause damage to impacted organizations or individuals.
  - ISSA's should adopt a specified set of *consistent baseline* controls and procedures the necessary security and privacy controls and handling procedures to protect PII from unauthorized use or disclosure and call for enhanced or supplemental safeguards to be included within the ISAA i.e. notice to privacy office, tracking, and automated management of them.
  - The sub-committee recommendations are based on three central and interrelated objectives to address the privacy of PII in ISAAs:
    - Greater consistency across ISAAs;
    - Greater oversight and accountability of information sharing access agreements; and
    - Greater engagement across DHS offices and components.
  - These following objectives are derived from the Tasking, OIG Report, materials and information reviewed by the DPIAC, evolving privacy laws, and privacy best practices as understood by members of the DPIAC.

Policy Subcommittee Recommendations

- Consistency: Adopt and Promulgate an ISAA Privacy Addendum.
  - An ISAA Privacy Addendum ("IPA") could be circulated in template form and be attached to a contemplated ISAA with minimal effort to provide significant privacy controls and oversight to ISAAs.
    - Alerting the DHS Privacy Office (i) before entering into an ISAA, (ii) in the event of a security incident involving PII, (iii) upon renewal or material modification of an ISAA, or else every 5 years, (iv) upon termination or expiration of an ISAA, or (v) in the event of adverse changes impacting PII;
    - Baseline requirement to comply with applicable laws and federal standards concerning the privacy and security of PII;
    - Impose basic controls on the use and disclosure of PII; and
    - Ensure cooperation with the DHS Privacy Office if necessary.

Policy Subcommittee Recommendations

- Oversight:
  - ISAA Tracking Systems (and Automation)
    - The DHS Privacy Office previously identified the need for a new compliance tracking system with automated reporting features to track and schedule timely reviews of privacy compliance documents
      - DHS Privacy Office should undertake an assessment on further developing PRIV-CATS to track ISAAs.
      - The Privacy Office should assess whether a standalone tracking system for ISAAs would be more suitable—either long-term or for an interim period while necessary modifications to PRIV-CATS can be implemented.
  - Ensure and Strengthen Accountability for Notices to the Privacy Office
    - DHS officials responsible for implementing ISAAs, who share PII, should notify the Privacy Office of the proposed sharing of PII (via designated webform or email address) pursuant to existing policy responsibilities
      - When entering into an ISAA;
      - Upon renewal or modification of an ISAA, but in no event less than once every five years for longer-term ISAAs;
      - Upon expiration or termination of an ISAA, to certify that all PII received under the ISAA has been returned or destroyed, and/or the basis for any further retention;
      - Upon discovery of an actual or suspected compromise of PII received under the ISAA; and
      - Upon discovery of an adverse change impacting PII
  - Inventory Existing
    - With the PRIV-CAT tracking system in place, in combination with some of the engagement efforts identified below, the Privacy Office would be in a better position to work with different DHS offices and components to inventory and identify current ISAAs and add them to its system, as well as consider whether any currently-in-effect ISAAs should be supplemented with an IPA

Policy Subcommittee Recommendations

- Engagement:
  - There are evident challenges in achieving effective coordination and cooperation across all DHS offices and components, each of which have limited resources, numerous priorities and practical challenges that can inhibit the necessary coordination with the Privacy Office.
  - While the DPIAC has limited insight into those realities, privacy offices have faced similar challenges in other public and private sector organizations (albeit often not to the same extent).
  - While the DPIAC believes this determination should be made within the Privacy Office, possible targets could be (1) component privacy offices, (2) legal functions who may negotiate, review and renew ISAAs, and (3) personnel with authority to execute ISAAs.
  - The ISAA Privacy Addendum (IPA) can be also included in PTA templates and other ISAA-related materials to promote adoption and use.
  - For broader outreach and education, annual DHS Privacy Awareness Training can perhaps be amended to reference the importance of reporting ISAAs to the Privacy Office and the need to complete IPAs.

Policy Subcommittee Recommendations

- Conclusion:
  - The recommendations presented in the full report are based on privacy practices that have achieved effective results in other organizations involved in data sharing for various purposes.
  - If adopted at DHS, these recommendations may likewise result in more consistency on privacy considerations for ISAAs, with more effective Privacy Office oversight and engagement going forward.

Committee Discussion and Voting

Chris Teitzel
DPIAC Emerging Technologies Subcommittee Chair

Emerging Technologies Subcommittee Recommendations

- Tasking Overview:
  - Emerging Technologies Subcommittee (ETS) was tasked to consider the Department of Homeland Security's (DHS) transition to cloud service technologies and the enhanced capabilities this transition has provided the Department during the COVID-19 telework environment to determine if there are associated privacy risks that would merit a near-term tasking.
  - During the October 27, 2020 DPIAC meeting, then Chief Information Officer Karen S. Evans briefed the DPIAC on the transition her office facilitated to enable teleworking and additional cloud migrations during the COVID-19 pandemic.
    - an average daily load of 10,000 teleworkers suddenly turned into 70,000 as offices throughout the country were closed for in-person work
    - the Homeland Security Information Network (HSIN) saw a 200% increase in traffic and the DHS HQ Virtual Private Network (VPN) increased in usage by 483%.
  - Outside of the cloud productivity tools and teleworking, DHS has an ongoing migration and modernization of data and services that it supports
    - Migration of data, services and computing to the cloud, where possible.
    - Consolidation of datacenter operations
    - Modernization of remaining systems

Emerging Technologies Subcommittee Recommendations

- Fact Finding:
  - ETS met with representatives of the Office of the Chief Information Officer (OCIO) to discuss and understand better the transition that has taken place due to COVID-19 and the ongoing cloud migration initiatives.
    - Each system has undergone evaluations to determine if they can be moved to the cloud
    - Any system deem not able/ready to move has documented justification for staying on-premises
    - Any "legacy system" not migrated to the cloud has plans for rebuilding on modern technology to ensure comparable resilience to their cloud counterparts.
    - Management Directives (and addendums) play a critical role in providing guidance for how systems are managed and migrated.
      - When there is a gap in the Management Directives, DHS works with technology partners to fill the gap and provide best practices

Emerging Technologies Subcommittee Recommendations

- Risks Of Cloud Migration Overview:
  - Data Security
    - Inventory and categorization
    - Maintain permissions and sharing
    - Zero Trust model critical to modern cloud systems
  - Data Integrity
    - Ensure data is not modified or lost en-route to cloud
    - Data retention planning for copies and backups
  - Data Privacy
    - Catalog and identify Personally Identifiable Information (PII)
    - Data minimization by evaluating if PII is necessary to retain
  - User Training

Emerging Technologies Subcommittee Recommendations

- Findings:
  - DHS' ongoing cloud migrations have been conducted with appropriate care and effort to keep data secure, private and available.
  - With this occurring with the backdrop of a global pandemic and shift to remote work, the efforts by DHS are commendable.
  - Policies and Management Directives are being followed as expected
  - In situations where Management Directives do not exist, DHS is working well with software providers to follow industry best practices and standards while simultaneously updating and/or implementing appropriate Management Directives.

Emerging Technologies Subcommittee Recommendations

- Recommended Next Steps:
  - DHS conduct a review and inventory of the Management Directives and addendums currently in place to ensure any new technologies are appropriately covered by internal policies.
  - DHS review its OIG audit process to ensure that after initial migration ongoing audits are conducted in an appropriate cadence, along with ensuring audits includ guidelines for 3rd party contracts
  - DHS proactively include and evaluate both a privacy and security review early in the discussions of any system, tool, or data migration to ensure privacy by design principles can be followed and accounted for early in the process and not afterwards during an audit.

Committee Discussion and Voting

Public Comment

Meeting Adjourned