DRAFT REPORT

Report [_____] of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with Information Sharing

As approved in Public Session on [_____]

I. Summary

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.

This report reflects detailed review by the Committee of the current status of information sharing practices, and provides specific recommendations that may help promote *consistency* in baseline privacy controls for information sharing, facilitate *oversight* by the Privacy Office across all information sharing activities, and achieve better *engagement* across DHS offices and components.

Specifically, the recommendations propose adopting a template ISAA Privacy Addendum that can be included in both existing and future sharing arrangements involving personally identifiable information ("PII"), with contractually-required reporting to the Privacy Office at both the inception of new sharing agreements as well as upon certain events (e.g., incident or renewal), with such reports funneled into a Patent Office tracking system that can serve as an inventory of sharing arrangements involving personal information. With these core capabilities in place, the Privacy Office could engage with appropriate stakeholders across DHS offices and components to provide training and awareness, leading to increased adoption and compliance.

II. Tasking

On October 27, 2020, the DHS Chief Privacy Officer ("CPO") requested that DPIAC provide guidance on information sharing. Specifically, the tasking ("Tasking") asked the following:

> Provide written guidance on best practices to ensure the effective implementation of privacy requirements for information sharing across the DHS enterprise. Specifically, I ask that the Committee address the following:
>
> a. How can the DHS Privacy Office better engage offices and Components to improve consistency in meeting information sharing requirements related to privacy?
>
> b. How can the DHS Privacy Office provide better oversight of the privacy protections included in information sharing agreements? Are there specific metrics that can be utilized and written into these agreements?

> c. Are there other considerations necessary to effectively implement privacy requirements into DHS information sharing activities?[1]

The Tasking was assigned to DPIAC's Policy Subcommittee, which later presented its findings to the full committee for review. This report represents the results of that review and addresses several recommendations related to the DHS Privacy Office's request, particularly with respect to Information Sharing Access Agreements ("ISAAs").

The scope of the tasking concerned oversight of DHS Offices and Components with respect to sharing agreements involving PII, and specifically with regard to external information sharing (i.e., DHS sharing with other federal agencies, foreign partners, or the private sector).

III. Background and Fact Finding

A. Background

"Congress enacted the Privacy Act of 1974 (Privacy Act) and the E-Government Act of 2002 (E-Government Act) to balance the Government's access and collection of PII with the protection of individuals from unwarranted invasions of privacy. The Acts impose specific requirements on agencies when collecting PII. The E-Government Act requires agencies to address privacy risks when developing or procuring new or modified technologies to collect, maintain, use, or disseminate PII. Additionally, agencies must fully protect individual privacy and comply with the Privacy Act and all other applicable privacy laws, regulations, and policies when sharing data."[2]

"In its mission to secure the homeland, the Department of Homeland Security collects PII from U.S. citizens, lawful permanent residents, and foreign nationals visiting the United States. DHS employees and contractors may share that information with its partners, including other Federal agencies and state and local governments, to carry out day-to-day mission duties. For example, the Federal Emergency Management Agency (FEMA) collects PII from disaster survivors and may share limited PII with its partners with disaster mission responsibility. U.S. Customs and Border Protection (CBP) collects PII from foreign nationals when processing passengers at ports of entry to target high-risk travelers and facilitate legitimate travelers. All DHS information technology (IT) systems, programs, and initiatives that collect PII or have privacy impact are subject to the requirements of U.S. data privacy and disclosure laws."[3]

"The DHS Privacy Office's mission is to protect individuals by embedding and enforcing privacy protections and transparency in all DHS activities."[4] The DHS Privacy Office includes

---

[1] *See* DPIAC Meeting October 27, 2020 (https://www.dhs.gov/publication/dpiac-meeting-october-27-2020).

[2] Office Of Inspector General, Department of Homeland Security, *DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives*, OIG-21-06 (Nov. 4, 2020), at 1 (https://www.oig.dhs.gov/sites/default/files/assets/2020-12/OIG-21-06-Nov20.pdf).

[3] *Id*.

[4] *Id*. at 2.

three teams: (1) the Privacy Policy and Oversight Team is responsible for developing DHS privacy policy; (2) the Privacy Compliance Team oversees privacy compliance activities; and—*most relevant to this report*—(3) "[t]he Information Sharing, Safeguarding, and Security Team provides specialized privacy expertise to support DHS information-sharing initiatives with its partners. The team also evaluates information sharing requests to assess and mitigate privacy risks and ensure compliance with privacy terms and conditions."[5]

The DHS Office Of Inspector General ("OIG") is legislatively mandated to periodically assess DHS's implementation of the Privacy Act.[6] On November 4, 2020, the OIG issued an audit report entitled DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives (the "OIG Report").[7] The audit objective was to determine whether the DHS Privacy Office has effective oversight of department-wide privacy activities, programs, and initiatives.[8] The OIG Audit "made three recommendations to the DHS Privacy Office to improve oversight of privacy compliance, information sharing access agreements, and privacy training."[9] DHS concurred with all three recommendations.[10] With respect to information sharing, DHS responded that "the DHS Privacy Office will develop standards for which types of ISAAs the CPO needs to review, and which may be delegated to Component Privacy Officers or [Privacy Points of Contact]."[11]

Since issuance of the OIG Report, the DHS Privacy Office has undertaken several initiatives in response to the OIG Audit findings and recommendations. Specifically in connection with information sharing, one of the steps taken by the DHS Privacy Office was to issue the present Tasking to the Committee.

B. Fact Finding

DPIAC focused its review specifically on information sharing involving PII and/or sensitive PII pertaining to U.S. persons or special protected classes of individuals, such as refugees, asylees, or others. DPIAC 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, DPIAC members reviewed both public and non-public DHS materials relevant to the Tasking. DPIAC members also met with DHS personnel over the course of several months.

---

[5] *Id*. at 3.

[6] *Id*. at cover page.

[7] *Id*.

[8] *Id*.

[9] *Id*.

[10] *Id*.

[11] *Id*. at 18.

Some of the key public documents included the following:

- The OIG Report;
- Management Directive 262-05, *Information Sharing and Safeguarding* (Sept. 4, 2014);[12]
- Management Directive 047-01, *Privacy Policy and Compliance* (July 25, 2011);[13]
- Policy Directive 262-15, *Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy* (June 5, 2009);[14]
- OMB Memorandum M-11-02, *Sharing Data While Protecting Privacy* (Nov. 3, 2010);[15]
- DHS Directive 047-01, *Privacy Policy and Compliance* (July 7, 2011);[16]
- DHS Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (April 25, 2017).[17]
- Sample Privacy Impact Assessments ("PIAs");[18] and
- Sample Systems of Records Notices ("SORNs").[19]

Some of the key non-public documents included:

- Information Sharing Access Agreements (ISAAs) with external agencies and parties; and
- Privacy Threshold Analysis ("PTA") and Privacy Impact Assessment ("PIA") forms.

DPIAC members also discussed topics relating to the Tasking with the DHS CPO, the Committee's designated federal officer ("DFO") and the DHS Privacy Office compliance team.

---

[12] https://www.dhs.gov/sites/default/files/publications/mgmt/information-and-technology-management/mgmt-dir_262-05-information-sharing-and-safeguarding.pdf.

[13] https://www.dhs.gov/sites/default/files/publications/mgmt/information-and-technology-management/mgmt-dir_047-01-privacy-policy-and-compliance_revision-00.pdf.

[14] https://www.dhs.gov/sites/default/files/publications/mgmt/information-and-technology-management/mgmt-dir_262-15-dhs-fed-info-share-enviro-privacy-civ-lib-protection-pol.pdf.

[15] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-02.pdf.

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

[17] https://www.dhs.gov/sites/default/files/publications/Privacy%20Policy%20Guidance%20Memo%202017-01%20-%20FINAL.pdf.

[18] *See* https://www.dhs.gov/privacy-impact-assessments.

[19] *See* https://www.dhs.gov/system-records-notices-sorns.

At the DPIAC public meeting on May 14, 2021, the Policy Subcommittee Chair reported on the subcommittee's progress and proposed next steps. Some of the recommendations contemplated at that time included:

- 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.[20]

Following that meeting the Policy Subcommittee completed its work, after which its findings and recommendations were presented to the full Committee for review and feedback prior to finalizing this report.

C. Privacy Office Authority

By DHS Directive and Delegation, the Office of Strategy, Policy and Plans leads information sharing in policies and negotiation of enterprise information sharing agreements.

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 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.

"DHS formally documents information sharing activities in an ISAA. ISAAs are defined as any memorandum of understanding, memorandum of agreement, or any form of agreement used to facilitate the exchange of information between two or more parties. ISAAs contain specific requirements relating to privacy, including:

- the appropriate authorities providing the information to the recipient and the recipient collecting the information;
- compliance with provider and recipient privacy documentation requirements; and
- acknowledgement that collection, use, maintenance, and dissemination of PII under the agreement is consistent."[21]

"According to a 2011 DHS privacy policy, the CPO is responsible for ensuring all DHS ISAAs comply with DHS privacy compliance documentation requirements and DHS policy.

---

[20] *See* DPIAC Meeting May 14, 2021 (https://www.dhs.gov/publication/dpiac-meeting-may-14-2021).

[21] OIG Report (referenced above) at 12-13.

Additionally, the accompanying instruction calls for Component Privacy Officers and 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."[22]

Because information sharing arrangements do not 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).

There is a particular need for the Privacy Office to address information sharing in a manner that is pragmatic and practical both for the Privacy Office, as well as across DHS and its component agencies. There are already significant privacy compliance measures (e.g., PIAs, SORNs) that could overlap with any further assessments proposed for information sharing arrangements, risking duplicative efforts, and potentially holding up important initiatives. In addition, significant privacy provisions appear in many ISAAs, although the specific terms and requirements can vary significantly. Finally, many DHS components are large agencies operating semi-autonomously and rely primarily on their own privacy office for day-to-day operations, rather than engaging with the DHS Privacy Office on all matters involving PII or information sharing.

IV. Recommendations

A. Overview

As noted above, many ISAAs may inherently require sharing of PII[23] to achieve DHS initiatives and objectives.[24] However, the improper use or disclosure of such information may impact

---

[22] *Id*. at 13 (citing DHS Directive 047-01, *Privacy Policy and Compliance*, July 7, 2011 (referenced above); DHS Instruction 047-01-001, *Privacy Policy and Compliance*, July 25, 2011 (https://www.dhs.gov/publication/privacy-policy-and-compliance-instruction-047-01-001)).

[23] PII means "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf). "[T]he definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual." OMB Memorandum 10-22, *Guidance for Online Use of Web Measurement and Customization Technology*, June 25, 2010 (https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf).

[24] The DHS Fair Information Practice Principles ("FIPPs") form the basis of DHS privacy and other civil liberties compliance policies and procedures governing the use of PII. *See* Policy Directive 262-15 (referenced above) at 3-4. "Consistent with the Privacy Act and DHS SORN guidance … any sharing of such information outside the agency

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.

ISAAs should therefore adopt the necessary security and privacy controls and handling procedures to protect PII from unauthorized use or disclosure. ISAAs reviewed by DPIAC members certainly went to great lengths to address security and privacy needs, but a specified set of *consistent baseline* controls and procedures could simplify the task in many instances as well as provide uniformity and reliability to the process. At the same time, specific circumstances could certainly call for enhanced or supplemental safeguards to be included within the ISAA.[25] Baseline requirements could mandate notice to the Privacy Office both prior to executing an ISAA, as well as upon renewal and in the event of a security incident impacting PII. These ISAA-related notices to the Privacy Office could be tracked—and at least partially automated—driving better *oversight and accountability*. Once the Privacy Office has implemented baseline requirements and systems to store and track ISAA materials, it can engage with appropriate stakeholders across DHS and its component agencies to drive adoption on a go-forward basis. Engagement efforts can also facilitate compilation of existing ISAAs.

The recommendations below are based on three central and interrelated objectives to address the privacy of PII in ISAAs:

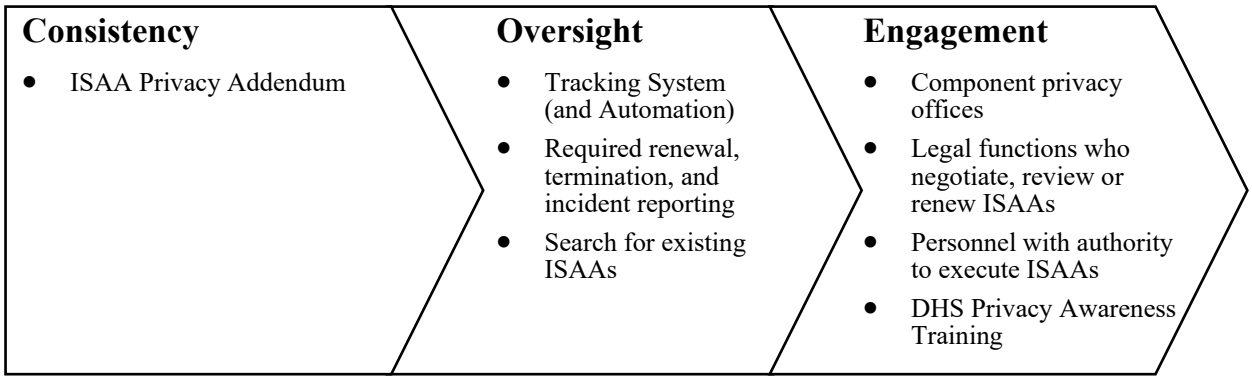
- Greater *consistency* across ISAAs;
- Greater *oversight* and accountability of information sharing access agreements; and
- Greater *engagement* across DHS offices and components.

These 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.

must be compatible with the purpose(s) for which the information was originally collected. … As a part of the DHS PIA process and addressed in PIA guidance, components must articulate the purpose and authorities for the collection of information as well as identify the internal and external recipients with whom they share PII." *Id*. at 4.

[25] Some of the recommendations here are based on important guidance and best practices developed in other contexts but nevertheless useful here as well, for example, the guidance published by NIST for cyber threat information sharing. *See, e.g.,* NIST Special Publication 800-150, *Guide to Cyber Threat Information Sharing*, October 2016 (http://dx.doi.org/10.6028/NIST.SP.800-150).

Proposed elements of achieving each objective are illustrated below and addressed in detail in the following sections.



Where automation and standard protocols can be used, they are eminently preferred over manual efforts. This can simplify enhanced measures such as those suggested here, help expedite adoption, and drive long term efficiencies at overseeing ISAA activities while minimizing to the extent possible any additional overhead both within the Privacy Office as well as at DHS offices and components who are directed to adopt the new measures.

B. Consistency

1. Adopt and Promulgate an ISAA Privacy Addendum

An ISAA Privacy Addendum ("IPA") could be circulated in template form and simply be attached to a contemplated ISAA with minimal effort to provide significant privacy controls and oversight to ISAAs.[26] Importantly, the IPA could easily be executed with respect to existing

[26] Template privacy addendums are increasingly required for agreements that involve data sharing to address both privacy laws and organizational privacy risks (in most instances, data is shared with a service provider for contracted services). Many organizations develop their own form, adopt an industry form, or use a form issued by a regulatory authority for such purposes.

For example, protected health information ("PHI") governed by the Health Insurance Portability and Accountability Act ("HIPAA") and/or Health Information Technology for Economic and Clinical Health Act ("HITECH") may only be shared with a service provider pursuant to a Business Associate Agreement ("BAA") with very specific baseline contractual terms. *See* Department of Health & Human Services, *Business Associate Contracts* (https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html). Many organizations effectively use form BAAs that can be attached to services agreements.

Similar approaches can be found outside the United States. For example, the European Commission recently issued updated its Standard Contractual Clauses ("SCCs") which provide a form data protection agreement between parties that may be used to lawfully transfer PII between parties in certain contexts, such as for cross-border transfers (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).

Based on the Committee's experience, a significant number of public and private sector agreements involving PII now rely on a form privacy and/or security addendum as an effective means to ensure privacy safeguards are properly and consistently addressed in view of privacy law requirements and industry best practices.

ISAAs, so those ISAAs can be supplemented with added privacy protections and oversight while remain in effect without interruption or a disruptive contractual overhaul.

Key provisions in the IPA will include the following:

1. 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;

2. Baseline requirement to comply with applicable laws and federal standards concerning the privacy and security of PII;

3. Impose basic controls on the use and disclosure of PII; and

4. Ensure cooperation with the DHS Privacy Office if necessary.

Critically:

- The IPA would ***not*** impose any requirement on the DHS Privacy Office to address every ISAA (which may impose too much demand on available resources); and

- The IPA would ***not*** require pre-approval of the DHS Privacy Office for an ISAA to proceed in any respect (which would create a bottleneck that could inhibit mission-critical activities).

With an IPA, key safeguards can be set with a recognized baseline that can also be leveraged to drive the oversight objectives that follow below. The IPA would ensure that the DHS Privacy Office receives notice of all ISAAs and any material events that occur during their lifespan, providing a central receiving point for collecting and tracking all ISAA activity across the entirety of DHS. As described below, the intake process would optimally be automated to populate a tracking system as ISAA notices are received. This alerting mechanism would also provide the DHS Privacy Office with an easy means to establish metrics around ISAA activities and practices, determine when audits may be appropriate, and leverage available IPA terms to facilitate such audits.

A sample IPA is attached to this report as **Appendix A**. Although it may require material changes to meet DHS needs for ISAAs, the DPIAC takes no pride of authorship. The IPA could be written to not conflict with more stringent provisions in the underlying ISAA, but any ISAA that cannot meet the baseline IPA requirements would require express approval from the DHS Privacy Office.

C. Oversight

1. 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 (i.e., PTAs, PIAs, and SORNs). The DHS Privacy Office began working with the DHS Office of the Chief Information Officer on a Privacy Compliance Artifact Tracking System ("PRIV-CATS"), launched in October 2019.[27]

The DHS Privacy Office should undertake an assessment on further developing PRIV-CATS to track ISAAs. This could be a natural extension of the current function for PRIV-CATS, and reduce duplicative efforts while maintaining more robust insights into organizational data flows because ISAAs are often associated with specific PTAs, PIAs, and/or SORNs.

Alternatively, 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.

Template IPAs could include instructions for providing notice to the Privacy Office, such as uploading the ISAA and accompanying IPA through a website form or via secure (encrypted) email to a designated email address.[28] The receiving system or email box can be configured to store the attachment in an appropriate repository as well as index key details within a Privacy Office system (e.g., PRIV-CATS) for future reference and tracking. A webform would be more optimal as the form could solicit key information (relevant DHS office or component, entity receiving PII, type of notice, etc.) that gets imported into the system while the uploaded ISAA and IPA gets stored in an associated repository. There are a number of commercial Contract Management Systems ("CMSs") on the market—some of these systems may be approved for DHS' use, otherwise, they may provide useful examples of how a suitable CMS can be designed and implemented within DHS.

2. 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.[29] In the case of international ISAAs, the DHS Policy Office is typically responsible for submitting the agreements to the Privacy Office for review and approval.[30] For non-international ISAAs, those officials whose signature appears on the ISAA should submit the proposed sharing of PII to the Privacy Office. While Component Privacy

---

[27] OIG Report (referenced above) at 17-18.

[28] For enhanced tracking, each component agency could have its own tailored template IPA and unique webform or email account, which would help with more precise tracking and could potentially direct a copy to that component agency's own privacy office.

[29] DHS Policy Guidance Memorandum 2017-01 (referenced above) states that "[w]ith respect to information sharing activities, Department employees must confirm whether an agreement (e.g., information sharing access agreement, memorandum of understanding, memorandum of agreement), federal statute, or other legal authority permits the sharing and follows the terms of any applicable agreement or arrangement. Also, notwithstanding specific authority permitting the sharing of information, there may exist other policy considerations that would affect DHS's decisions whether to share information. Finally, the Department requires protections on further dissemination of the records beyond the requestor's agency or organization, and coordination with the DHS Office or Component responsible for acquiring the records subject to being shared to avoid operational conflicts.".

[30] DHS Instruction 047-01-001, Privacy Policy and Compliance, July 25, 2011 (referenced above).

Officers or Privacy Points of Contact should make submissions, as a practical matter they are not always made aware of the existence of such agreements.

Notice should be provided:

- 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.

DHS entities that engage in ISAAs should be identified and engaged by the Privacy Office (see Engagement) through targeted training to ensure they firmly understand their reporting obligations.

An existing framework is in place for the reporting obligations by ISAA owners, the Privacy Office may also wish to look for opportunities to strengthen and clarify this obligation by drafting new policies and instructions.

3. Inventory Existing ISAAs

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.

D. 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).

The approaches outlined here can be presented to the DHS Information Sharing Coordination Council and the Information Sharing Governance Board ("ISGB").[31] Upon receiving any

[31] "The DHS Chief Privacy Officer … participate[s] in DHS' Information Sharing Coordination Council, a Department-wide group administered by the Information Sharing and Collaboration (IS&C) Branch, Office of Intelligence and Analysis, and designed to provide coordinated, Department-wide deliberation and input on information sharing policy and related matters to the Information Sharing Governance Board (ISGB). The ISGB is,

necessary approval and support, perhaps focusing engagement efforts on departments and staff most connected to information sharing and ISAAs could result in progress on both implementing better go-forward practices as well as tracking down past ISAAs. 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 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.

V. Conclusion

The recommendations presented in this 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.

VI. Enclosures

Appendix A – Sample ISAA Privacy Addendum

---

the executive steering committee and decision-making body for the Department on information sharing and collaboration issues. The ISGB oversees the planning and development of major information sharing programs and policies, and resolves internal information sharing and access disputes involving two or more DHS Components. [T]he DHS Chief Privacy Officer [] serve[s] as [an] ex officio member[] on the ISGB." (Policy Directive 262-15 (referenced above) at 5-6.)

Appendix A – Sample ISAA Privacy Addendum

Please contact the DHS Privacy Office's Information Sharing, Safeguarding, and Security Team with any questions at [EMAIL/PHONE].

###

ISAA Privacy Addendum

This ISAA Privacy Addendum ("IPA") supplements the accompanying Information Sharing Access Agreement ("ISAA") between the Department of Homeland Security, including its components, agencies, and offices (hereinafter "DHS") and the counterparty identified therein (the "Data Recipient" or "DR") with respect to any Personally Identifiable Information ("PII") that DR may receive or access from or on behalf of DHS under the ISAA.

In addition to all terms and conditions set forth under the ISAA, DR agrees to protect and handle all PII as detailed in this IPA. In the event of any express conflict between this IPA and the ISAA, the more stringent terms will apply.

1. **Privacy Review**. The parties hereto represent that before executing the accompanying ISAA, this IPA and the ISAA was submitted to the DHS Privacy Office for review as directed below, with reference to any associated Privacy Impact Assessment ("PIA").

2. **Required Notices to the DHS Privacy Office**. All notices required below should be directed to the DHS Privacy Office via [WEBFORM / EMAIL ADDRESS]. In the event DR does not receive an acknowledgement of receipt from the DHS Privacy Office, alternate notice shall be made via mail to [MAILING ADDRESS] or by contacting the DHS Privacy Office for another means of communication. Upon request of the DHS Privacy Office, DR shall provide a copy of the ISAA and this IPA, and any other reasonably related documentation. A party to the ISAA may provide any of the above-required notices on behalf of the other party (e.g., the relevant DHS office or component may provide notice of renewal on behalf of the DR).

    a. **Notice of pending ISAA**. In advance of executing the ISAA, the relevant DHS office or component shall notify the DHS Privacy Office and provide a copy of the ISAA and attachments thereto.

    b. **Notice of Security Incident**. DR will immediately notify the DHS Privacy Office in the event of a Security Incident, as defined and further described below.

    c. **Notice of Renewal / Material Modification / Five-Year Notice**.

        i. DR will notify the DHS Privacy Office within thirty (30) days of renewing or materially modifying the ISAA, including when such renewal is automatic. Such notice shall include documentation evidencing the renewal or modification.

        ii. In the event the ISAA term exceeds five (5) years, DR will notify the DHS Privacy Office within thirty (30) days of each five-year anniversary of the ISAA effective date.

d. **Notice of Termination or Expiration**. DR will notify the DHS Privacy Office within thirty (30) days of termination or expiration of the ISAA. Such notice shall include a summary of PII (i) returned to DHS, (ii) certified as destroyed following termination or expiration of the ISAA, and (iii) identify whether and to what extent any PII is being retained, and the basis for such retention under the ISAA and applicable laws.

e. **Adverse Changes**. DR will notify the DHS Privacy Office promptly if DR: (i) has reason to believe that it is unable to comply with any of its obligations concerning PII under the ISAA or this IPA and it cannot cure this inability to comply within a reasonable timeframe; or (ii) becomes aware of any circumstances or change in applicable law that is likely to prevent it from fulfilling its obligations concerning PII under the ISAA or this IPA. If the ISAA or this IPA, or any actions to be taken or contemplated to be taken in performance of the ISAA or this IPA, do not or would not satisfy either party's obligations under the laws applicable to each party, the parties will negotiate in good faith upon an appropriate amendment to the ISAA or this IPA.

3. **Compliance with Applicable Laws and Standards**. DR will comply with all laws relating to the protection of PII, including as applicable the Privacy Act of 1974, as amended (Pub. L. 93-579), and other relevant laws, regulations, system of records notices ("SORNs"), PIAs, and departmental policies for the sharing of data, including but not limited to the laws identified in the ISAA.

4. **Limitations on Use**. DR will Process PII only as expressly permitted in the ISAA. The duration of the Processing will be the same as the duration of the ISAA, except as otherwise specified therein. As used in this IPA, "Process" or "Processing" means the collection, recording, organization, structuring, alteration, use, access, disclosure, copying, transfer, storage, deletion, combination, restriction, adaptation, retrieval, consultation, destruction, disposal, or other use of PII.

5. **Confidentiality**. DR will hold PII in strict confidence and impose confidentiality obligations (and as applicable security clearance obligations) on all DR personnel who receive access to, or otherwise Process, PII, in accordance with the requirements of this IPA and the ISAA, including during the term of their employment or engagement and thereafter.

6. **Information Security Program**. DR will implement, maintain, monitor and, where necessary, update a comprehensive written information security program that contains appropriate administrative, technical, and physical safeguards to protect PII against anticipated threats or hazards to its security, accessibility, confidentiality or integrity. As part of its information security program, DR will maintain appropriate access controls, including, but not limited to, limiting access to PII to the minimum number of DR personnel who require such access to fulfil the limited purpose authorized by the ISAA and providing those personnel who have access to PII with appropriate training relating to information security. The foregoing information security program shall comply with all applicable laws and federal standards applicable to the PII.

7. **Security Incident**. DR will promptly notify the DHS Privacy Office (and in any event within forty-eight (48) hours or sooner if required by law) if DR knows or suspects that there has

been any accidental or unauthorized access, acquisition, use, modification, disclosure, loss, destruction of, or damage to PII, or any other unauthorized Processing of PII ("Security Incident"). In the event of any Security Incident, DR will reasonably cooperate with the DHS Privacy Office to limit the unauthorized access, disclosure or use of PII, seek the return of any such PII, and assist in providing notice relating to the Security Incident to individuals or third parties as directed by the DHS Privacy Office. This obligation is in addition to any notice obligations that DR may have under the ISAA. The DHS Privacy Office will reasonably endeavor to coordinate with other DHS offices or components involved in any response to a Security Incident.

8. **Data Integrity**. DR will seek to ensure that all PII maintained by DR in connection with the ISAA is accurate and, where appropriate, kept up to date, and will erase or rectify inaccurate or incomplete PII in accordance with DHS instructions.

9. **Cross-Border Transfers**. DR will ensure that PII is not physically transferred to, accessed by, or otherwise Processed in any country other than the United States except, and only to the extent, expressly permitted in the ISAA.

10. **Disclosures and**. DR will not disclose or transfer PII to, or allow access to PII by (each, a "Disclosure") any third party without except, and only to the extent, expressly permitted in the ISAA.

11. **Subcontractors**. DR will, prior to any Disclosure of PII to a subcontractor, (i) obtain express prior approval from DHS, and (ii) enter into an agreement with such subcontractor that is at least as restrictive as this IPA and the ISAA with respect to the protection of PII. DR will be fully responsible for all acts or omissions by its subcontractor(s) with respect to the Disclosure and the terms of this IPA and the ISAA, and DR commits to monitor such subcontractor(s) with respect to the terms of this IPA and the ISAA.

12. **Requests or Complaints from Individuals**. DR will promptly notify the appropriate DHS office in writing if DR receives: (i) any requests from an individual to exercise any rights afforded by applicable law or provided under the relevant terms of use with respect to their PII Processed under the ISAA (e.g., request for access); or (ii) any complaint relating to the Processing of PII, including allegations that the Processing infringes on an individual's rights. DR will not respond to any such request or complaint unless expressly authorized to do so by DHS, will reasonably cooperate with DHS with respect to any action taken relating to such request or complaint, and will seek to implement appropriate processes (including technical and organizational measures) to assist DHS in responding to requests or complaints from individuals where deemed necessary in DHS's discretion. If DR is unsure who to contact in regard to such request or complaint, it shall contact the DHS Privacy Office for instructions.

13. **Disclosure Requests**. If DR receives a lawful demand to produce or disclose PII from any court or governmental authority ("Legal Demand"), DR will immediately notify DHS (except to the extent prohibited by applicable United States law). DR will cooperate with DHS in the event DHS elects to intervene and prevent or limit such disclosure. Notwithstanding the foregoing, DR will exercise all reasonable efforts to prevent and limit any such disclosure

and to otherwise preserve the confidentiality of PII and will cooperate with DHS with respect to any action taken with respect to such Legal Demand, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to PII. If DR is unsure who to contact in regard to a Legal Demand, it shall contact the DHS Privacy Office for instructions.

14. **Information Requests and Cooperation**. DR will provide relevant information and assistance as requested by the DHS Privacy Office to demonstrate DR's compliance with its obligations under the ISAA and this IPA with respect to PII, and reasonably assist DHS in meeting its own policies and obligations regarding PII.

15. **Return or Disposal**. Subject to any express terms of the ISAA to the contrary, upon termination or expiration of the ISAA for any reason or upon DHS's request, (i) DR will immediately cease Processing PII and will return it in a manner and format reasonably requested by DHS, or (ii) if return is not required by DHS, DR will permanently destroy all PII received or Processed under the ISAA. As directed in the notice provision above, DR will provide a written certification to the DHS Privacy Office that all PII has been returned or destroyed consistent with federal standards for destruction, as required under the ISAA or applicable law.

16. **Modifications to this IPA**. DR will cooperate in good faith with DHS to modify the terms of the ISAA and/or this IPA if required due to changes in applicable law governing PII.

###