Privacy Impact Assessment
for the

DHS Data Framework – Interim Process to Address an Emergent Threat

DHS/ALL/PIA-051

April 15, 2015

Contact Point
Paul Reynolds
Data Framework Program Management Office
Department of Homeland Security
(202) 447-3000

David Hong
Cerberus Program Manager
Department of Homeland Security
(202) 282-9632

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202)343-1717

Abstract

The Department of Homeland Security (DHS) is publishing this Privacy Impact Assessment (PIA) to explain its plan to expedite DHS's ability to meet a critical mission need through the use of an interim manual data transfer process. Specifically, DHS has a critical mission need to perform classified queries on its unclassified data in order to identify individuals supporting the terrorist activities of: (1) the Islamic State of Iraq and the Levant (ISIL), (2) al-Qa'ida in the Arabian Peninsula (AQAP), (3) al-Nusrah Front, (4) affiliated offshoots of these groups, or (5) individuals seeking to join the Syria-Iraq conflict. (These individuals are often referred to as "foreign fighters" by the media and in public discourse.) The ability to perform classified searches of unclassified data for this uniquely time sensitive purpose will allow DHS to better identify and track foreign fighters who may seek to travel from, to, or through the United States. This type of comparison is a long-standing mission need; however, the specific threat has shortened the timeframe in which DHS must meet the need.

To meet this critical mission need, DHS will adopt an interim process that foregoes many of the automated protections of the DHS Data Framework, such as the tagging of necessary data sets in the unclassified data lake. By foregoing these automated protections, DHS will be able to expedite transfers of information from the Electronic System for Travel Authorization (ESTA), the Advance Passenger Information System (APIS), Form I-94 records, and Passenger Name Records (PNR) directly from the unclassified DHS domain to the classified DHS domain through a manual process.

Although the interim process deviates from the standard model of the Data Framework, DHS is pursuing this process under the auspices of the Data Framework in order to utilize aspects of the Framework's policies, governance, and transparency. Moreover, the interim solution will only continue until the standard model is capable of meeting the mission need. DHS remains committed to the standard model of the Data Framework for meeting DHS's mission needs in the long-term, and the Department will revert to the standard model once the technical capabilities are available. Consequently, regular development on the Framework will continue and will not be affected by the use of the interim process.

Introduction

Data Framework: An Iterative Program

The DHS Data Framework ("Data Framework" or "Framework") is DHS's "big data"[1]

[1] In its report on "big data," the White House noted that most definitions generally "reflect the growing

solution to incorporate privacy protections while enabling more controlled, effective, and efficient use of DHS data within DHS and with other U.S. Government partners, as appropriate. In PIAs published on November 6, 2013,[2] April 29, 2014,[3] and February 27, 2015,[4] DHS described the iterative development of the Data Framework. DHS is pursuing an iterative development process for a variety of reasons, including:

1. The technical, fiscal, and policy complexity of deploying an innovative, large-scale information technology (IT) program;
2. The need to ensure the program effectively meets DHS mission needs;
3. The need to test that policy-based technical controls function appropriately;
4. The need to establish an effective governance process to ensure the long-term success of the program; and
5. DHS's desire to provide robust transparency about the Data Framework.

Although the iterative process is still the most responsible path to ensuring the long-term success of the program, the Department is facing a discrete critical mission need that cannot be fulfilled by the capabilities of the current iteration of the Data Framework. Specifically, the Department has a critical mission need to perform classified searches of unclassified DHS data sets that are not yet fully available in the Data Framework. In the long-term, the Framework will be the most effective, efficient, and responsible mechanism for meeting the Department's critical mission need. In fact, as noted in the first Framework PIAs, the need to perform classified searches on unclassified data is one of the primary reasons DHS

---

technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data." While volume, velocity, and variety are important defining markers of "big data," the power of big data is in how it is used. The White House noted that:

> Unprecedented computational power and sophistication make possible unexpected discoveries, innovations, and advancements in our quality of life. But these capabilities, most of which are not visible or available to the average consumer, also create an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it.

See "Big Data: Seizing Opportunities, Preserving Values," Executive Office of the President, May 1, 2014. Available at: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

[2] *See* DHS/ALL/PIA-046 DHS Data Framework, dated November 6, 2013, for a description of the Data Framework's Pilot/Prototype Phase. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.

[3] *See* DHS/ALL/PIA-046(a) DHS Data Framework, dated August 29, 2014, for a description of the Data Framework's Limited Production Capability Phase. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-pia-046-a-dhs-data-framework-08292014.pdf.

[4] *See* DHS/ALL/PIA-046(b) DHS Data Framework, dated February 27, 2015, for a description of the Initial Operational Capability Phase. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-046b-dhs-data-framework-20150227.pdf.

is pursuing the Data Framework.[5]

DHS is publishing this PIA to explain its plan to expedite DHS's ability to meet the critical mission need (described below) through the use of interim manual data transfers. Although the interim process deviates from the standard model of the Framework, DHS is pursuing the process under the auspices of the Data Framework in order to utilize aspects of the Framework's policies, governance, and transparency. Eventually, the interim process will also utilize the Data Framework's technical capabilities. Consequently, the interim solution will only continue until the standard model is capable of meeting the mission need. DHS remains committed to the standard model of the Data Framework for meeting DHS's mission need in the long-term, and the Department will revert to the standard model once the technical capabilities are available. Consequently, regular development on the Framework will continue and will not be affected by the use of the interim process.

Critical Mission Need: Discrete Counterterrorism Analysis and Risk Assessments

DHS has an immediate critical mission need to perform classified queries on its unclassified data. This type of comparison is a long-standing mission need; however, the specific threat posed by Foreign Terrorist Organizations, such as the Islamic State of Iraq and the Levant (ISIL), al-Qa'ida in the Arabian Peninsula (AQAP), and al-Nusrah Front, has shortened the timeframe in which DHS must meet the need.[6] (Individuals supporting these groups are often referred to as "foreign fighters" by the media and in public discourse.) Specifically, the Department needs to be able to perform classified searches of its unclassified data to better identify and track foreign fighters supporting these groups. These foreign fighters may transit from or through the United States, or they may seek to travel to the United States to participate in or support an attack on the United States or its allies. Secretary Johnson summarized the threat, explaining that:

> The reality is that there are more than 12,000 foreign fighters [who] have traveled to Syria over the last three years, including more than a thousand Europeans. We estimate that more than 100 Americans have traveled or attempted to travel to Syria to join the fight there one way or another. We are concerned that not only may these foreign fighters join ISIL or other extremist groups in Syria, [but] they may also be

[5] *See* DHS/ALL/PIA-046 DHS Data Framework, dated November 6, 2013, available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf, and DHS/ALL-PIA-046-3 Cerberus Pilot, dated November 22, 2013, available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-cerberus-nov2013.pdf.

[6] ISIL, AQAP, and al-Nusrah Front are designated by the Secretary of State as Foreign Terrorist Organizations (FTO) in accordance with 8 U.S.C. § 1189 (Section 219 of the Immigration and Nationality Act, as amended). More information on the designation process is available from the U.S. Department of State at: http://www.state.gov/j/ct/rls/other/des/123085.htm.

> recruited by these extremist groups to leave Syria and conduct external attacks. The [Federal Bureau of Investigation (FBI)] has arrested a number of individuals who have tried to travel from the U.S. to Syria to support terrorist activities there.[7]

Recent testimony by Francis Taylor, Under Secretary for Intelligence and Analysis, highlights the evolution of the threat and DHS's increasing concern:

> For some time, the U.S. Government, including [DHS], has been concerned that terrorist groups operating in permissive environments present a significant security threat to the United States and to our allies. Events in Australia, Canada and, most recently, in France and Belgium underscore that the foreign fighter threat is no longer a problem restricted to foreign conflict zones such as those in northern Syria or western Iraq. [ISIL] and other like-minded terrorist organizations have been effective in recruiting fighters from Western countries, as well as recruiting individuals for violent action at home for those who cannot travel to conflict zones. The threat is real, it continues to evolve, and it is a present danger to everyone across the globe. It includes people radicalized to violence overseas, or potentially here in the United States. At present, we are unaware of any specific, credible, imminent threat to the Homeland; however, recent events have demonstrated the need for increased vigilance both at home and abroad.[8]

In describing the Department's activities to combat groups such as ISIL, Secretary Johnson noted that DHS, the FBI, and the Intelligence Community "…are making enhanced and concerted efforts to track Syrian foreign fighters who come from or seek to enter this country" and are "…enhancing our ability to share information with each other about suspicious individuals."[9]

Expediting the ability to perform classified searches of DHS's unclassified data sets supports DHS's efforts to counter the threat posed by foreign fighters by allowing DHS to use the information it receives from U.S. Government or foreign government partners—much of

---

[7] *See* "Remarks by Secretary of Homeland Security Jeh [Charles] Johnson at the Council on Foreign Relations – As Delivered," dated September 10, 2014. Available from the DHS Press Office at: http://www.dhs.gov/news/2014/09/10/remarks-secretary-homeland-security-jeh-johnson-council-foreign-relations-%E2%80%93.

[8] *See* "Written Testimony of I&A Under Secretary Francis Taylor for a House Committee on Homeland Security Hearing Titled, 'Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror,'" dated February 11, 2015. Available from the DHS Press Office at: http://www.dhs.gov/news/2015/02/11/written-testimony-ia-under-secretary-house-committee-homeland-security-hearing.

[9] *See* "Remarks by Secretary of Homeland Security Jeh [Charles] Johnson at the Council on Foreign Relations – As Delivered," dated September 10, 2014. Available from the DHS Press Office at: http://www.dhs.gov/news/2014/09/10/remarks-secretary-homeland-security-jeh-johnson-council-foreign-relations-%E2%80%93.

which may be classified—to identify high risk individuals traveling to, through, or from the United States. These high risk travelers may be the subject of intelligence analysis at DHS; be the subject of a referral to another agency for appropriate action (e.g., to the Department of State for visa revocation); have an application to the Electronic System for Travel Authorization denied; or may be referred for additional scrutiny (e.g., secondary inspection) when they travel to, through, or from the United States.

Addressing the Mission Need: Interim Manual Data Transfers

The details of the interim manual data transfer process will be outlined in a Concept of Operations signed by U.S. Customs and Border Protection (CBP), the owner of the datasets to be transferred, and the DHS Office of Intelligence and Analysis (I&A), but key aspects of the process are described below for transparency.

As part of the interim solution, DHS will manually transfer the Electronic System for Travel Authorization (ESTA),[10] the Advance Passenger Information System (APIS),[11] Form I-94 records,[12] and Passenger Name Records (PNR)[13] to the DHS classified Top Secret/Sensitive Compartmented Information (TS/SCI) domain. All of these data sets have been previously approved for inclusion in the Data Framework.[14] As with all data incorporated into the Data Framework, the ESTA, APIS, I-94, and PNR information remains covered by the source System of Records Notices (SORN)[15] while it is in the Data Framework.

Unclassified data transferred to the classified domain remains unclassified, but placing

[10] *See* DHS/CBP/PIA-007 *et seq.* Electronic System for Travel Authorization, originally issued June 2, 2008, and updated on July 11, 2011, July 18, 2012, June 5, 2013, and November 3, 2014. Available at: http://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[11] *See* DHS/CBP/PIA-001 *et seq.* Advance Passenger Information System, originally issued March 21, 2005, and updated on August 8, 2007, September 11, 2007, November 18, 2008, June 21, 2011, and June 5, 2013. Available at: http://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[12] *See* DHS/CBP/PIA-016 U.S. Customs and Border Protection Form I-94 Automation, dated February 27, 2013. Available at: https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/pia-cbp-16-I-94-automation-20130227.pdf.
[13] *See* DHS/CBP/PIA-006 *et seq.* Customs and Border Protection Automated Targeting System, originally issued August 3, 2007, and updated on December 2, 2008, June 1, 2012, January 31, 2014, and September 16, 2014. Available at: http://www.dhs.gov/privacy-documents-us-customs-and-border-protection
[14] *See* Appendix A of DHS/ALL/PIA-046(b) DHS Data Framework, dated February 27, 2014, for more information on the data sets included in the Data Framework. Appendix A is available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-046b-appendix-a-dhs-data-framework-20150227.pdf.
[15] *See* Appendix A of DHS/ALL/PIA-046(b) DHS Data Framework, dated February 27, 2014, for a listing of the compliance documentation associated with these data sets. Appendix A is available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-046b-appendix-a-dhs-data-framework-20150227.pdf.

the unclassified data on the classified network allows DHS personnel to perform classified searches of the unclassified data. (The terms of the searches may be classified, which means that the classified search terms can only be entered on the classified domain, even if they are being used on unclassified data.)

Access to this data in the classified domain will be limited to: (1) I&A intelligence analysts and support staff for intelligence analysts (e.g., data scientists, research analysts) and (2) CBP personnel conducting targeting and intelligence analysis and support personnel to the extent needed (e.g., attorneys providing legal advice). Technical personnel (e.g., system administrators) will be responsible for loading the data onto the classified domain and performing system administration functions, but they will not have access to the actual data after the loading is complete.

The data will be used to conduct predicated searches[16] based on intelligence or law enforcement information for the following counterterrorism functions: (1) intelligence analysis performed by I&A or CBP and (2) the identification of individuals for additional scrutiny by CBP. Specifically, DHS will be comparing classified data against unclassified CBP data. These functions will be performed to identify individuals supporting the terrorist activities of ISIL, AQAP, al-Nusrah Front, affiliated offshoots of these groups, or individuals seeking to join the Syria-Iraq conflict.

CBP's and I&A's searches will be tailored, as much as practicable, to identify the individuals supporting the terrorist activities described above. However, it is possible that CBP's or I&A's subsequent analysis of the results of the searches could identify incidentally an individual who may be subject to additional scrutiny for another reason. For example, a search may be performed to identify a foreign fighter, but the subsequent analysis may indicate another violation of law, such as human smuggling. While CBP or I&A are not permitted to seek to identify this individual through further counterterrorism searches, DHS may retain, use, and share according to its authorities any non-terrorism information that is identified incidentally. For CBP, non-terrorism information identified incidentally as a result of a counterterrorism search will be covered under the Automated Targeting System SORN.[17] For I&A, non-terrorism information identified incidentally as a result of a counterterrorism search will be covered under the Enterprise Records System SORN.[18]

---

[16] The search functions available for the Interim Manual Data Transfers will be modeled on the search functions available in the Pilot/Prototype, Limited Production Capability, and Initial Operational Capability phases of the Data Framework. Specifically, the Data Framework's three search types are: person search, characteristic search, and trend search.

[17] *See* DHS/CBP-005 – Automated Targeting System SORN, dated May 22, 2012, 77 Fed. Reg. 30297. Available at: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

[18] *See* DHS/IA-001 – Enterprise Records System (ERS) SORN, dated May 15, 2008, 73 Fed. Reg. 28128. Available at: http://www.gpo.gov/fdsys/pkg/FR-2008-05-15/html/E8-10888.htm.

Only CBP and I&A personnel who already have access to APIS, ESTA, I-94, and PNR information during the normal course of their duties will have access to APIS, ESTA, I-94, and PNR information during the interim manual data transfers. CBP and I&A personnel currently perform targeting and intelligence analysis on these data sets. Consequently, the authorized users and uses of APIS, ESTA, I-94, and PNR information do not change under the interim manual data transfers.

If DHS identifies terrorism information[19] in this data, then DHS will share that information, including with other U.S. Government partners, as required by law, permitted by law, or consistent with binding international agreements.

I&A's analytic results from these searches are covered by its Enterprise Records SORN.[20] CBP's analytic results from these searches are covered by the Automated Targeting System SORN. [21]

The interim manual transfers are permitted for 180 days, with the option to extend the manual transfers in 90 day increments until the Data Framework can meet the mission need. Once the Data Framework is able to meet the mission need, the interim manual transfers will be stopped, and all data from the interim manual transfers will be purged to comply with the data quality requirements of the Data Framework.

As with other phases of the Data Framework, data refreshes will be limited. Consequently, I&A and CBP personnel will be required to confirm the accuracy of information in the source IT system prior to completing any analysis or referring an individual for additional scrutiny.

Key Changes: Standard Data Framework Model Versus Interim Manual Transfers

The interim manual data transfers deviate from the existing Data Framework model in four key ways, which are described below. The risks and any applicable risk mitigations

[19] "[T]errorism information" is defined in Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, which states "the term 'terrorism information' — (A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to: (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and (B) includes weapons of mass destruction information." 6 U.S.C. § 485(a)(5).
[20] *See* DHS/IA-001 – Enterprise Records System (ERS) SORN, dated May 15, 2008, 73 Fed. Reg. 28128. Available at: http://www.gpo.gov/fdsys/pkg/FR-2008-05-15/html/E8-10888.htm.
[21] *See* DHS/CBP-005 – Automated Targeting System SORN, dated May 22, 2012, 77 Fed. Reg. 30297. Available at: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

associated with these changes are discussed in the subsequent privacy analysis.

1. ***Extracting Data from non-Source IT Systems:*** Data will be pulled from CBP's Automated Targeting System[22] instead of directly from the source IT systems. This change is due to the limited technical ability of source IT systems and the current Data Framework iteration to support regular and timely extracts of data. This change reduces the burden on source IT systems—which will still be working to meet the extract requirements of the current phase of the Data Framework—and increases the speed with which DHS will be able to set up the interim manual data transfers to meet the critical mission need.

2. ***Transferring Data Directly to Cerberus:*** During the interim manual data transfers, data will be moved directly from the Automated Targeting System to Cerberus, which is DHS's data lake on the classified domain.[23] For the initial manual transfer, DHS will transfer data directly to Cerberus using encrypted portable media (e.g., hard drives). For subsequent manual transfers, DHS will use a one-way, secure transfer mechanism to move the unclassified data from the unclassified network to the classified network. Under the standard Data Framework model, data is moved from the source IT system to Neptune,[24] which is DHS's data lake on the unclassified domain. In Neptune, data is tagged and then transferred to Cerberus using a "cross domain guard," which permits the automated, secure transfer of data from an unclassified domain to the classified domain. DHS is not able to use the standard Framework model because all Neptune resources are currently focused on supporting deployment of the Initial Operational Capability phase of the Data Framework.

3. ***Data Tags for Access Control Policy Enforcement:*** Because data is moving directly from the Automated Targeting System to Cerberus, it will not be tagged in Neptune. In the standard Data Framework model, Neptune tags data as either core biographic, extended biographic, or encounter information. These tags lay the foundation for automated policy enforcement. Neptune also applies metadata tags for data provenance (e.g., from which system the data came) and retention. During the interim data transfers, the tags will only include the names of the data fields in the record (e.g., name, phone number) and a unique identifier that names the record ID in the source system (e.g., the unique ID for the record in ESTA) and allows a user to retrieve the

[22] *See* DHS/CBP/PIA-006 *et seq.* Customs and Border Protection Automated Targeting System, originally issued August 3, 2007 and updated on December 2, 2008, June 1, 2012, January 31, 2014, and September 16, 2014. Available at: http://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[23] *See* DHS/ALL/PIA/046-3(b) Cerberus, dated February 27, 2015. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-046-3-6-cerberus-02272015.pdf.
[24] *See* DHS/ALL/PIA/046-1(b) Neptune, dated February 27, 2015. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-046-1-b-neptune-20150227.pdf.

same record in the source system. I&A will create and apply an additional "time to live" tag for the data to inform when the record needs to be deleted from the classified network. Although some tags will be applied to the data, DHS will not apply the core, extended, or encounter tags that enable the automated application of access control policies.

4. ***Dynamic Access Control Policies:*** The hallmark of the Data Framework is its use of dynamic access control policies to evaluate user attributes (e.g., organization, clearance, training), data tags, and context (i.e., the authorized purpose and function being performed) to grant or deny access to DHS data based on legal authorities and appropriate policies of the Department or DHS Components. Because the data will not be tagged in Neptune, DHS will be unable to apply dynamic access control policies to the interim manual data transfers. During the interim manual data transfers, access to the data will be limited to authorized CBP and I&A users, which will be documented in the Concept of Operations signed by CBP and I&A. Consequently, DHS will be able to restrict access as a matter of policy, although it will not be able to utilize the Data Framework's dynamic access control policies to provide technical restrictions on access.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon Federal Agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). Section 222 of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. Given that the Data Framework is a program rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the fair information principles. This PIA examines the privacy impact of the Data Framework operations as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

As noted in other Data Framework PIAs,[25] due to the privacy sensitivities surrounding big data, DHS has implemented transparency about the Framework outside of its traditional privacy documentation process. DHS promoted the Data Framework as part of the White House Big Data Review,[26] and the Data Framework is described in the White House's final big data report.[27] DHS also provided three public briefings on the Data Framework during meetings of its Federal Advisory Committee, the DHS Data Privacy and Integrity Advisory Committee.[28]

Privacy Risk: Despite efforts to provide transparency outside of the traditional privacy documentation process, there is a risk that individuals may not be aware their PII is being compared against information, including classified information, from U.S. Government or foreign government partners.

Mitigation: The PIAs and SORNs for the relevant systems (i.e., APIS, ESTA, I-94, and PNR) articulate the use of PII for counterterrorism purposes. Some of the compliance documents expressly note that the PII will be compared against DHS or non-DHS information to identify security threats. For example:

- ***APIS:*** The APIS SORN states that "[APIS] information will be used to perform counterterrorism and/or intelligence activities; to assist law enforcement activities; to perform public security queries that identify risks to the aircraft or vessel, (sic) to its

[25] *See* DHS/ALL/PIA-046 DHS Data Framework, dated November 6, 2013, for a description of the Data Framework's Pilot/Prototype Phase. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf. *See* DHS/ALL/PIA-046(a) DHS Data Framework, dated August 29, 2014, for a description of the Data Framework's Limited Production Capability Phase. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-pia-046-a-dhs-data-framework-08292014.pdf. *See* DHS/ALL/PIA-046(b) DHS Data Framework, dated February 27, 2015, for a description of the Initial Operational Capability Phase. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-046b-dhs-data-framework-20150227.pdf.
[26] *See* the White House 90-Day Review for Big Data website for more information. Available at: http://www.whitehouse.gov/issues/technology/big-data-review.
[27] *See* the White House report "Big Data: Seizing Opportunities, Preserving Values," May 2014. Available at: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.
[28] *See* the DHS Privacy website for archived meeting materials. Available at: http://www.dhs.gov/dhs-data-privacy-and-integrity-advisory-committee-meeting-information.

occupants; or to the United States…."[29] The APIS PIA notes that DHS will use APIS information "…to perform law enforcement queries and to identify high-risk passengers and crew members who may pose a risk or threat to vessel or aircraft safety or to national security, while simultaneously facilitating the travel of legitimate passengers and crew members."[30]

- ***ESTA:*** The ESTA SORN states that, "DHS may also vet ESTA application information against security and law enforcement databases at other Federal agencies to enhance DHS's ability to determine whether the applicant poses a security risk to the United States and is eligible to travel to and enter the United States under the Visa Waiver Program."[31] The ESTA PIA notes that, "CBP vets the ESTA applicant information against selected security and law enforcement databases at DHS…" and adds that "[the Automated Targeting System] also retains a copy of ESTA application data to identify potential high-risk ESTA applicants."[32]

- ***I-94:*** The SORN that covers I-94, states that the information "…is used for entry screening, admissibility, and benefits purposes."[33] Under the Immigration and Nationality Act, an individual may be inadmissible to the United States if the individual is a member of a terrorist organization or has engaged in terrorism-related activity,[34] so using the data for admissibility purposes includes counterterrorism screening and vetting. The I-94 PIA explains that DHS may use I-94 information to identify travel patterns to "…enhance national security, facilitate legitimate travel, and ensure the integrity of the U.S. immigration system."[35] The PIA further notes that DHS shares departure information with the FBI and the Intelligence Community for

[29] *See* DHS/CBP-005 - Advance Passenger Information System (APIS), dated March 13, 2015, 80 Fed. Reg. 13407. Available at: https://www.federalregister.gov/articles/2015/03/13/2015-05798/privacy-act-of-1974-department-of-homeland-securityunited-states-customs-and-border-protection.
[30] *See* DHS/CBP/PIA-001(f) - Advanced Passenger Information System (APIS) Update National Counterterrorism Center (NCTC), dated June 5, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-apis-update-20130605.pdf.
[31] *See* DHS/CBP-009 - Electronic System for Travel Authorization (ESTA), dated November 3, 2014, 79 Fed. Reg. 65414. Available at: https://www.federalregister.gov/articles/2014/11/04/2014-26100/privacy-act-systems-of-records.
[32] *See* DHS/CBP/PIA-007(d) - Electronic System for Travel Authorization, dated November 3, 2014. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-cbp-esta-11032014.pdf.
[33] *See* DHS/CBP-016 Nonimmigrant Information System, dated March 13, 2015, 80 Fed. Reg. 13398. Available at: https://www.federalregister.gov/articles/2015/03/13/2015-05804/privacy-act-of-1974-department-of-homeland-securityunited-states-customs-and-border-protection-016.
[34] *See* 8 U.S.C. § 1182(3) for terrorism-related grounds for inadmissibility. More information is also available at: http://www.uscis.gov/laws/terrorism-related-inadmissability-grounds/terrorism-related-inadmissibility-grounds-trig.
[35] *See* DHS/CBP/PIA-016 - U.S. Customs and Border Protection Form I-94 Automation, dated February 27, 2013. Available at: https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/pia-cbp-16-I-94-automation-20130227.pdf.

counterterrorism and national security purposes, indicating that this information will be compared with intelligence and FBI information for counterterrorism purposes.[36]

- ***PNR:*** PNR information is covered by the SORN and PIA for CBP's Automated Targeting System. The Automated Targeting System SORN explains that PNR may be used to prevent, detect, investigate, and prosecute terrorist offenses and related crimes.[37] The Automated Targeting System PIA states that "PNR is used in conjunction with other data noted above to identify individuals requiring additional screening prior to entering the country."[38] The "other data" referenced includes both DHS and non-DHS data sources. For PNR information covered by the "Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security,"[39] the use of PNR information—identifying individuals seeking to join the Syria-Iraq conflict or supporting the terrorist activities of ISIL, AQAP, al-Nusrah Front, or affiliated offshoots of these groups—is within the scope of Article 4 of the Agreement.

DHS believes the existing SORNs and PIAs support DHS's comparison of information from these source IT systems with other information for counterterrorism purposes.

DHS has updated the source IT system SORNs to explicitly clarify that the information will also be stored on both the DHS unclassified and classified domains.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

---

[36] *See* DHS/CBP/PIA-016 - U.S. Customs and Border Protection Form I-94 Automation, dated February 27, 2013. Available at: https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/pia-cbp-16-I-94-automation-20130227.pdf.

[37] *See* DHS/CBP-006 - Automated Targeting System, dated May 22, 2012, 77 Fed. Reg. 30297. Available at: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

[38] *See* DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, dated June 1, 2012. Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

[39] *See* "Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security," dated December 14, 2011. Available at: https://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf.

Including ESTA, APIS, I-94, or PNR information in interim manual data transfers does not change the initial collection of the information. Similarly, the interim manual data transfers do not change the opportunities available for individuals to decline to provide information. The circumstances of collection and consequences of declining to provide the information remain the same as those of the source IT system but are summarized below for transparency.

- ***APIS:*** Advance Passenger Information is collected directly from travelers and transmitted to DHS by air and sea carriers. Rail and bus carriers may also collect information directly from travelers and voluntarily submit Advance Passenger Information to DHS. Air and sea travelers who decline to submit Advance Passenger Information would be precluded from traveling to or from the United States by air or sea. Rail and bus travelers may choose a carrier that is not voluntarily providing Advance Passenger Information to DHS.
- ***ESTA:*** Individuals voluntarily submit an ESTA application to travel to the United States under the Visa Waiver Program (VWP). If an individual declines to provide the information necessary to complete an ESTA application, the individual will not be permitted to travel to the United States under the VWP and will need to apply for a visa through a U.S. consulate or embassy.
- ***I-94:*** The electronic Form I-94 is created during the inspection process at the time of admission to or parole into the United States, when the CBP officer pulls information from the traveler's APIS record and the Department of State's Consolidated Consular Database, and enters any additional data obtained during the inspection process. If a traveler declines to provide the information to the CBP officer to complete the Form I-94, then it is likely that he or she will not be admitted or paroled into the United States because he or she did not provide sufficient information to meet the admissibility requirements of the Immigration and Nationality Act.
- ***PNR:*** DHS receives PNR information from commercial air carriers, which is provided to the air carriers directly by passengers or by travel agents on behalf of passengers seeking to book travel. Because DHS does not require commercial air carriers to collect certain PNR data elements and instead requires carriers to provide DHS access to the PNR data they otherwise collect, the PNR data elements submitted to DHS by a commercial air carrier may vary. If an individual does not provide at least a minimal amount of information, then it is unlikely that he or she will have provided enough information to the air carrier or travel agent to successfully book a ticket.

The inclusion of these data sets in the Data Framework does not impact an individual's ability to access or correct his or her information, consistent with the published SORN for the source

IT systems. As these are all CBP systems, individuals may submit a Freedom of Information Act (FOIA) or Privacy Act request with CBP at http://www.cbp.gov/site-policy-notices/foia or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002

General complaints about treatment or requests for redress can be made to the DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA 901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

Privacy Risk: Once an individual has provided APIS, ESTA, PNR, or I-94 information to DHS, he or she does not have an opportunity to withhold his or her information from the Data Framework. Consequently, there is a risk that an individual did not consent to having his or her information used in this manner.

Mitigation: As noted under the "Principle of Transparency," DHS has clearly articulated that it will use APIS, ESTA, PNR, and I-94 information for counterterrorism purposes, which includes activities such as the identification of high risk individuals traveling to, through, or from the United States and the comparison of travel records with derogatory information, such as the analysis performed by I&A analysts or CBP personnel within the Framework. (Please see the "Principle of Transparency" for a more detailed analysis of the notice provided for each data set.) This risk is further mitigated by the fact that the transfer of these data sets from the unclassified domain to the classified domain does not change DHS's use of the information or the protections afforded by the source IT system SORN. Consequently, there is no new collection, use, or dissemination of PII.

Privacy Risk: There is a risk that individuals will not have the same correction abilities once the information is moved to the classified network through interim manual data transfers.

Mitigation: As with other iterations of the Data Framework, this risk cannot be fully mitigated and will remain until DHS has near real-time refresh. During the interim manual data transfers, corrections provided by an individual may not be made in Cerberus in a timely fashion due to the potential lag time in data refreshes. The delay in updating corrections could result in analysis or additional scrutiny based on incorrect or incomplete information.

To partially mitigate the potential impact on individuals, users of the interim manual data transfers must verify the accuracy of the data in the source IT system before completing a final analytical product; disseminating a raw intelligence product (e.g., intelligence

information report); or using the data operationally (e.g., to identify individuals for additional scrutiny, referring an individual to the Department of State for a visa revocation).

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Both CBP and I&A already have access to ESTA, APIS, I-94, and PNR information in the unclassified domain to support their counterterrorism activities. Transferring data to the classified domain does not change the purpose for which DHS collected or uses the information.

As noted in the "Principal of Individual Participation," DHS collected the information to support its counterterrorism activities, including the identification of high risk individuals traveling to, through, or from the United States. The purpose of the interim manual data transfers is confined to the identification of individuals supporting the terrorist activities of ISIL, AQAP, al-Nusrah Front, affiliated offshoots of these groups, or individuals seeking to join the Syria-Iraq conflict. These individuals qualify as high risk travelers who may be subject to intelligence analysis or additional scrutiny. This purpose will be documented in the Concept of Operations signed by CBP and I&A.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Privacy Risk: Because DHS is transferring entire data sets to the classified network, there is a risk that DHS will transfer more information than is directly relevant and necessary to identify individuals supporting the terrorist activities of ISIL, AQAP, al-Nusrah Front, affiliated offshoots of these groups, or individuals seeking to join the Syria-Iraq conflict.

Mitigation: DHS has reviewed each of the data sets to ensure they contain fields that would be reasonably likely to contain information that would match terrorism information provided to DHS by the FBI and Intelligence Community. Every 180 days until the conclusion of the transfers, CBP and I&A will provide a report or briefing to the Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel that confirms the continued need for these data sets to identify individuals supporting the terrorist

activities of ISIL, AQAP, al-Nusrah Front, affiliated offshoots of these groups, or individuals seeking to join the Syria-Iraq conflict.

Privacy Risk: There is a risk that data could be retained in the classified domain for longer than is allowed in the original DHS IT system.

Mitigation: This risk cannot be mitigated to the same degree as under the standard Data Framework model because it deviates from the protections of the standard model, which uses technical mechanisms to ensure the application of retention requirements. The standard model relies on the original DHS IT systems to notify the Data Framework of changes, deletions, or corrections to data, which original DHS IT systems are to provide with each refresh of data. With respect to retention, the Framework would delete data upon receiving a notification from the source IT system. As an additional safeguard, the Data Framework tags each data set with a retention period and therefore can remind the underlying source IT system of an upcoming retention expiration date if the Data Framework has not already received a deletion notification.

The interim manual data transfers will include *ad hoc* refreshes based on mission needs, which means that DHS cannot rely on notifications from the source IT systems to perform deletions. Similarly, because the data will not be tagged in Neptune prior to being transferred to Cerberus, DHS will not be able to rely on retention tags as an additional safeguard. Although the standard controls of the Data Framework provide more robust (and often automated) technical safeguards, it is possible to mitigate this risk during the interim manual data transfers by using manual implementation of safeguards set forth in policy documentation consistent with applicable legal obligations.

To mitigate this risk during the interim manual data transfers, DHS (1) will document the retention requirements of the source IT systems in the Concept of Operations signed by CBP and I&A and (2) will manually implement the requirements. For example, Cerberus will tag the data with a "time to live" date, which will be used to manually delete information in accordance with source IT system requirements. For PNR, DHS will manually implement the same supplemental retention requirements currently required for PNR in the Automated Targeting System (e.g., masking of the data beginning 180 days after it is received by DHS in the Automated Targeting System; redaction of sensitive fields).

Additionally, every 180 days until the conclusion of the transfers, CBP and I&A will provide a report or briefing to the Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel that documents their retention of the data, so that these oversight offices may verify the retention requirements of the source IT systems are being satisfied.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Privacy Risk: There is a risk that DHS will be less capable of detecting uses of the data for purposes other than identifying individuals supporting the terrorist activities of ISIL, AQAP, al-Nusrah Front, affiliated offshoots of these groups, or individuals seeking to join the Syria-Iraq conflict.

Mitigation: Because the data will not be tagged according to the Data Framework standards and DHS cannot apply its dynamic access control policies, this risk cannot be mitigated in an automated fashion. The hallmark of the Data Framework is its ability to apply automated dynamic access control policies, which combine data tags with information about the user and use (i.e., authorized purpose and function) to ensure that only authorized users are able to utilize information for authorized uses. However, during the interim manual data transfers, DHS will mitigate this risk through the manual application of protections. First, DHS will document the authorized use in the Concept of Operations document signed by CBP and I&A. Second, every 180 days until the conclusion of the transfers, CBP and I&A will provide a report or briefing to the Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel that outlines their use of the data, so that these oversight offices may verify the use is restricted to identifying individuals supporting the terrorist activities of ISIL, AQAP, al-Nusrah Front, affiliated offshoots of these groups, or individuals seeking to join the Syria-Iraq conflict. The report or briefing will also include the number of instances where non-terrorism information was identified incidentally as a result of subsequent analysis or a counterterrorism search.

Privacy Risk: There is a risk that DHS will share PII outside of the Department for a purpose that is not compatible with the purpose for which the PII was collected.

Mitigation: DHS will only share information from the interim manual data transfers outside of DHS if that information constitutes terrorism information. This requirement will be outlined in the Concept of Operations document signed by CBP and I&A.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The use of interim manual data transfers deviates from the existing Data Framework model of extracting data only from the source IT systems, which is a core data quality

protection of the Data Framework.

Privacy Risk: Because the data will not be pulled from the source IT systems (with the exception of PNR), there is a risk that any errors introduced when the information was transferred from the source IT system to the Automated Targeting System will be replicated when the data is transferred from the Automated Targeting System to Cerberus.

Mitigation: To partially mitigate this risk, users of the Framework must verify the accuracy of the data in the source IT system (i.e., APIS, ESTA, I-94, or the Automated Targeting System for PNR) before completing a final analytical product; disseminating a raw intelligence product (e.g., intelligence information report); or using the data operationally (e.g., to identify individuals for enhanced scrutiny). This risk cannot be fully mitigated as long as DHS is pulling data from the Automated Targeting System instead of the source IT system. The risk represents one of the primary reasons the Data Framework seeks to only pull data from the source IT systems. The risk does not apply to PNR, for which the Automated Targeting System is the source IT system.

Privacy Risk: There is a risk that PII transferred outside of the original IT system and into the classified domain will not be accurate, relevant, timely, or complete because of the lack of automated refresh.

Mitigation: This risk is very similar to the one identified in the "Principle of Individual Participation." As with other iterations of the Data Framework, the risk cannot be fully mitigated and will remain until DHS has near real-time refresh. To partially mitigate the risk, users of the Data Framework must verify the accuracy of the data in the source IT system before completing a final analytical product; disseminating a raw intelligence product (e.g., intelligence information report); or using the data operationally (e.g., to identify individuals for additional scrutiny).

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Privacy Risk: For the initial manual transfer, there is a risk that the transfer of data through portable media (e.g., hard drive) will result in the loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of the data.

Mitigation: The data includes PII being transferred through a computer readable extract (CRE) and therefore must be transferred in accordance with DHS Sensitive Systems

Policy Directive 4300A,[40] which specifies, among other requirements, that: the PII must be encrypted on the CRE; the CRE must be documented and tracked; and the CRE must be destroyed or erased within 90 days unless there is a continued need for the data that is documented by the data owner and audited periodically by the DHS Component privacy officer.

Privacy Risk: For subsequent manual transfers, there is a risk that the transfer of data through a one way transfer mechanism will result in the loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of the data.

Mitigation: The data will be sent on DHS networks, which are encrypted and are in compliance with DHS Sensitive Systems Policy Directive 4300A. DHS will use a secure one way transfer mechanism to isolate the data from unauthorized and malicious processes, users, and devices when it moves from the unclassified to classified networks, ensuring that data cannot escape. All data sources undergo a robust security review to obtain approval before being transferred. Use of the one transfer mechanism provides assurance that sensitive information will not be disclosed inadvertently and allows for enhanced confidentiality and data integrity.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Privacy Risk: There is a risk that the use of PII will not be auditable to demonstrate compliance with these principles and all applicable privacy protection requirements.

Mitigation: This risk cannot be fully mitigated during the use of interim manual data transfers. The standard Data Framework model employs tamper-resistant audit logs that contain the user name and the query performed. Because the data is not tagged in Neptune and DHS is therefore not able to apply the dynamic access control policies based on those tags, DHS will not be able to audit whether the dynamic access control policies were applied correctly (i.e., whether users were only able to perform queries on a particular data set based on an authorized purpose and function).

Although DHS will not be able to apply and audit its dynamic access control policies, DHS will be able to perform auditing to ensure only authorized users are able to access the

[40] *See* DHS Sensitive Systems Policy Directive 4300A, Version 8.0, dated March 14, 2011. Available at: http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

data. To partially mitigate the risk, the users and uses will be identified in the Concept of Operations signed by CBP and I&A, and I&A will use existing audit capabilities to determine whether access is limited to the specified group of users.

The key difference is that the accountability mechanisms of the interim manual data transfers will not be as sophisticated as those that are planned under the standard Data Framework model. In other words, the authorized users and uses will be outlined in the Concept of Operations signed by CBP and I&A, but DHS will only be able to perform audits to validate the authorized users. DHS will not be able to use technical controls to audit the authorized uses. To further mitigate the risk, every 180 days until the conclusion of the transfers, CBP and I&A will provide a report or briefing to the Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel that outlines their use of the data and application of the privacy protections that are outlined in this PIA and will be outlined the Concept of Operations signed by CBP and I&A.

Conclusion

As noted above, the use of interim manual data transfers does not provide all of the robust, automated privacy protections of the standard Data Framework model. Although DHS has crafted mitigations for the privacy risks associated with this approach, not all risks can be fully mitigated until the Data Framework is fully implemented. Nevertheless, the Department must act to meet the critical mission need and will revert to the standard model once the Data Framework is capable of meeting the mission need.

Responsible Officials

Clark Smith
DHS Office of Intelligence and Analysis
Chief Information Officer

Approval Signature Page

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security