Privacy Impact Assessment
for the

Data Management Hub

DHS/ALL/PIA-076

October 29, 2019

Contact Point
Lori Vislocky
Office of Intelligence & Analysis
(202) 447-4385

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

Abstract

The Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) manages data on behalf of DHS Components when there is a need to share that data with the Intelligence Community (IC) and other national security partners or to support DHS mission use cases and applications using a secure data environment. The Data Management Hub (or "Data Hub") is a set of technical components that facilitates the storage, enrichment, tagging, and movement of DHS and partner data by I&A on the classified network fabric. The goal of the Data Hub is to provide a single authoritative data store of datasets in order to reduce data duplication and improve the authorized usage of data for data-sharing and analysis. It also centralizes and streamlines the data formatting, tagging, and transfer of data for approved internal and external mission applications, including bulk sharing with national security partners and other government agencies.

The Data Hub is a series of technical components and, while it does not itself use specific information about individuals, it supports the storage and use of data and datasets that contain personally identifiable information (PII). The Data Hub simply transports and stores data and datasets; there is no data or dataset inherent to it. As such, data or datasets that use the Data Hub process will be listed in the appendices to this PIA.

Overview

The Data Hub ingests datasets and maintains the data in a DHS-owned and controlled cloud computing environment on a classified network. More specifically, it consists of the following elements:

- The storage of unclassified DHS data holdings in a secure environment, which are detailed in individual appendices to this PIA;
- Information management policies based on the data; data owner; privacy, civil liberties and civil rights; and information safeguarding considerations to ensure compliance, such as the automated removal of data consistent with retention requirements;
- Services to enrich, filter, and tag datasets according to mission needs;
- Logging of system activity and the ability to export the information for audit; and
- A platform to transfer data to approved mission applications, including bulk transfer to national security partner environments.

These components are data/dataset agnostic and may be modified to transport and store a wide range of data types (including various datasets). By providing a centralized environment for the data storage and management services listed above, the Data Hub allows DHS to maintain source system data outside the source system with greater efficiencies and increased capabilities to support classified mission use cases.

The data within the Data Hub will be refreshed from the original source system at rates as close to real time as possible. The near real-time refresh will enable data to be updated or corrected and remain analytically relevant to the mission use cases the data supports. Recognizing that this is a privacy risk, the refresh rate is one of the many factors that the appropriate governance bodies and supporting technical teams will consider during the data ingest planning process. I&A will regularly assess system capacity and examine ways to shorten the refresh rate for data sources ingested into the Data Hub.

The Data Hub's data transfer platform communicates with various data endpoints over the TS/SCI-level network to send and receive data through defined flows. The Data Hub uses services that are secured with encryption and in compliance with DHS and IC policies and directives. The Data Hub's data transfer platform will enable DHS to deliver data to authorized mission users, who may include a secure, classified environment managed by a national security partner for its internal collection of the data or a mission-specific application (*e.g.*, a search tool) approved by appropriate oversight offices, such as the DHS Office of the General Counsel, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and Component legal and privacy offices (collectively, the "Oversight Offices").

The Data Hub's enrichment and tagging functionalities provide a range of capabilities, including formatting data, filtering data, enriching data elements by leveraging lookup data sources, and programmatically applying security markings and other data tags. The Data Hub can develop and apply these enrichment capabilities and tags based on the needs of particular mission use cases.[1]

The Data Hub will also consist of development enclaves that are separate from all production and operational functions that the Data Hub carries out. In some instances, it may be beneficial to use real DHS data for testing and development purposes in order to more effectively evaluate the accuracy of a new or emerging capability. For example, using real data can allow the technical staff to account for details in the data (*e.g.*, empty values in "optional" fields in a form) or edge cases that may not be represented in mock or "dummy" data. I&A will work with DHS Component and Headquarters Privacy Offices to request the use of data for development purposes by submitting all appropriate privacy compliance documentation that describes the effort (*e.g.*, what data will be used, the duration of the test, when data will be deleted). Use of the data in the development environment will be dependent on this approved documentation.

In addition to original mission records, the Data Hub also provides to the partner any record updates (*e.g.*, changes to existing records made by the source system) as part of its ongoing delivery of data. Included in the data delivery is the automated tagging and formatting that occurs to prepare data for analytical use. In addition to delivering data, this capability can also be used to retrieve results from external sources. For example, when necessary and approved, the Data Hub

[1] The Data Hub allows DHS to stay true to the values in the data fields, while allowing for updates to format.

can pull unclassified information residing in a classified environment from that external source in the classified environment and deliver it through a secure cross domain transfer, where it can be shared with operators via unclassified systems.

To enhance DHS analytic capabilities, analytic tools will be created to leverage the data available within the Data Hub. These tools are not part of the Data Hub environment but are external applications. As these tools are developed in response to mission use cases, they will be reviewed by the appropriate governance bodies and offices and described in separate privacy compliance documentation. In all of these scenarios, access control policies would be established with guidance and concurrence from the data owner to ensure data is accessible only to authorized users.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

I&A's role within the IC is to facilitate information sharing and conduct appropriate research and analysis to support information sharing between DHS Components, the IC, and other national security and law enforcement partners per the National Security Act,[2] as amended; the Homeland Security Act,[3] as amended; Executive Order 12333,[4] as amended; and Executive Order 13388.[5]

I&A's legal authorities to collect and use the information collected by DHS Components are found in the Homeland Security Act, as amended by the Intelligence Reform and Terrorism Prevention Act (IRTPA) and the Implementing Recommendations of the 9/11 Commission Act of 2007;[6] the Homeland Security Act of 2002, §§ 201-202,[7] and Executive Orders 12333[8] and 13284[9] (recognizing I&A a part of the IC).

Under Title 6, United States Code, Section 121(d), the Secretary of Homeland Security, acting through the Under Secretary for Intelligence and Analysis (USIA), has the responsibility, among other things:

- To establish and use, in conjunction with the DHS Chief Information Officer, a secure communications and information technology infrastructure, including data-mining

[2] The National Security Act of 1947, Pub. L. 80-253, 61 Stat. 495 (codified as amended at 50 U.S.C. § 15).
[3] The Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135.
[4] Executive Order 12333, 46 FR 59941 (December 8, 1981).
[5] Executive Order 13388, 70 FR 62023 (October 25, 2005).
[6] Implementing Recommendations of the 9/11 Commission Act of 2007, 6 U.S.C. § 101 (2015).
[7] 6 U.S.C. §§ 201-2002.
[8] *See* Footnote 15.
[9] Executive Order 13284, 68 FR 4075 (July 31, 2003).

and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of other responsibilities assigned in Section 121, and to disseminate information acquired and analyzed by DHS, as appropriate [Subparagraph 13];

- To ensure, in conjunction with the DHS Chief Information Officer, that any information databases and analytical tools developed or used by DHS are compatible with one another and with relevant information databases of other agencies of the Federal Government, and treat information in such databases in a manner that complies with applicable federal law on privacy [Subparagraph 14];
- To coordinate with elements of the intelligence community and with federal, state, and local law enforcement agencies, and the private sector, as appropriate [Subparagraph 16];
- To provide intelligence and information analysis and support to other elements of the Department [Subparagraph 17];
- To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components [Subparagraph 18]; and
- To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence [Subparagraph 19].

The Secretary has delegated these responsibilities to the USIA in DHS Delegation No. 08503. Further, as an element of the IC, I&A is authorized by Section 1.6(c) of Executive Order 12333, as amended, to provide specialized equipment, technical knowledge, or assistance of expert personnel for use by a department or agency, or when lives are endangered, to support local law enforcement agencies.[10]

I&A must ensure that any materials it receives are protected from unauthorized disclosure, and that any intelligence information is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

No data or datasets are inherent to the Data Hub. However, the data transported and maintained by the Data Hub are covered by source system System of Records Notices (SORN). The specific SORNs for each relevant dataset will be listed in the appendices of this PIA.

[10] Technical support of this nature must be approved in advance by the DHS Associate General Counsel for Intelligence pursuant to Executive Order 12333.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A System Security Plan (SSP) is underway in support of the Data Hub's Authority to Connect, which is expected to be granted concurrently with the completion of this PIA, along with other compliance requirements.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The data maintained by the Data Hub is provided by source systems, which have their own approved records retention schedules. This data will be maintained by the Data Hub in accordance with those schedules. Please refer to the appendices of this PIA for relevant retention schedule information.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The provisions of the Paperwork Reduction Act are not applicable to the Data Hub as no information is collected directly from members of the public. However, the source system information transferred to the Data Hub may be subject to the Paperwork Reduction Act. Datasets that interact with the Data Hub are outlined in the addenda of this PIA, but the source system PIAs should be referenced to determine applicability to the Paperwork Reduction Act.[11]

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The Data Hub will support the use of a variety of information, as such information will be collected from a variety of different sources. Initially, the Data Hub will be used for datasets that support the Department's screening and vetting mission to determine whether an individual poses a threat to national security, border security, homeland security, or public safety and the U.S. Government's visa, naturalization, immigration benefit, immigration enforcement, travel, and border security decisions. For example, the Data Hub will support the use of data such as border crossing information, applications for travel submitted by individuals from countries participating

[11] DHS source system PIAs can be found here: https://www.dhs.gov/privacy.

in the Visa Waiver Program, or other travel information. The Data Hub will first support U.S. Customs and Border Protection's (CBP) Electronic System for Travel Authorization (ESTA)[12] information; as other datasets are added in support of other DHS missions (*e.g.*, border security, cyber security, immigration enforcement), the privacy documentation will be amended via appendices that describe each dataset and its use.[13]

The Data Hub will provide services based on mission use cases, including:

- Ingest of data in support of approved information sharing agreements;
- Receipt and distribution of results information from IC agencies;
- Storage and correlation of data;
- Filtering, enrichment, and tagging of data;
- Management of access to data by individual users and infrastructure, according to pre-determined rules and standards;
- Management of the retention of data according to approved record schedules;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for redress processes, Privacy Act (PA)/Freedom of Information Act (FOIA) requests, discovery in litigation, and other data retrieval requirements.

The PIAs and SORNs that apply to each relevant dataset will differ and are listed in the appendices of this PIA.

2.2 What are the sources of the information and how is the information collected for the project?

The Data Hub will support the use of a variety of information; as such information will be collected from a variety of different sources. The source system information, including PIAs and SORNs that apply to each relevant dataset, are listed in the appendices of this PIA.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The Data Hub will support the use of a variety of information; as such information will be collected from a variety of different sources. These sources themselves may use commercial sources or publicly available information, which then may be transported or maintained by the Data Hub. However, the Data Hub itself does not use this type of information. Should the Data Hub begin to use publicly available or commercial sources, privacy documentation will be updated

[12] *See* DHS/CBP/PIA-007(d) Electronic System for Travel Authorization, *available at* https://www.dhs.gov/privacy.
[13] Please see Appendix A of this PIA for the mission use cases.

as appropriate.

2.4 Discuss how accuracy of the data is ensured.

The data within the Data Hub will be refreshed from the original source system at rates as close to real time as possible.[14] A number of technical measures are also in place to ensure data integrity is not affected during the transport and storage of data. Other technical measures have been developed to quickly identify data problems (such as data corruption) should they occur. For example, all data must pass a schema validation check to confirm the expected format and content prior to Data Hub ingest. Any records that fail this check will be identified and shared back with the source system to take appropriate action. The Data Hub also leverages tools to evaluate system performance and identify issues, such as data latency, that require optimization to minimize such risks.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that changes or corrections made to PII in the underlying source systems will not be updated or pushed to the Data Hub, leading to inaccurate or out-of-date information being stored, shared, or used for mission purposes.

Mitigation: This risk is partially mitigated. Protocols are in place to ensure that updates to data are transferred to the Data Hub (and any onward sharing or use, as approved) in as close to near-real time as possible. For example, I&A and the component source system technical teams implement alerts to notify their respective staff if there is an outage or backlog causing delays in delivery. Early notification of potential issues allows the technical staff to implement a fix. If the issue requires significant time and resources to be resolved, technical teams provide notifications to the mission users alerting them of the issue and implications. The timing of these notifications is coordinated in advance with component source systems and users and documented in I&A's Standard Operating Procedures. System performance is regularly monitored and reviewed to ensure the rate of data flows is consistent with mission requirements. If it is later determined that some of that information was incorrect, the original record should not be modified but annotated to indicate the inaccurate data and the new, correct information. Inaccurate data would not be erased, but it would be clear from the totality of the updated record which data was found to be inaccurate and which is correct.

Privacy Risk: There is a risk the Data Hub technology will not have appropriate security safeguards, putting individual PII at risk of breach or compromise.

Mitigation: This risk is mitigated. Because the Data Hub is being maintained on a

[14] The whole dataset is not re-ingested every time. I&A establishes transactional flows with the Components, meaning all subsequent updates to an application, record, etc., are pushed through to the Data Hub, as opposed to the entire dataset.

classified network, DHS follows the information technology security requirements established in DHS's *Sensitive Compartmented Information Systems* 4300C *Instruction Manual*; National Institute of Standards and Technology Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; and Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*. The system will be required to receive an Authority to Connect, which requires the DHS Chief Information Security Officer's and DHS Chief Privacy Officer's approval. Access controls are established to ensure data is accessible only to authorized users and user activity is logged for audit, oversight, and accountability purposes.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The Data Hub will support the use of a variety of information and will provide services based on mission use cases,[15] including:

- Ingest of data in support of approved information sharing agreements;
- Receipt and distribution of results information from IC agencies;
- Storage and correlation of data;
- Filtering, enrichment, and tagging of data;
- Management of access to data by individual users and infrastructure, according to pre-determined rules and standards;
- Management of the retention of data according to approved record schedules;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for redress processes, Privacy Act (PA)/Freedom of Information Act (FOIA) requests, discovery in litigation, and other data retrieval requirements.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. The Data Hub will not use technology to conduct electronic searches, queries, or

[15] Specific mission use cases will be outlined in the appendices for each dataset. The Data Hub will first support CBP ESTA information; other datasets will be added in support of other DHS missions (*e.g.*, border security, cyber security, immigration enforcement).

analyses to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. I&A technical staff will provide services on behalf of other DHS Components and consistent with their requirements; DHS Component staff will not have administrator access to the Data Hub. DHS Components will be responsible for participating in the data ingest planning process to ensure source system protections and rules are documented and carried out by I&A.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the stated purposes of the collection of data are inconsistent with the activities that the Data Hub supports.

Mitigation: This risk is mitigated. The purposes for use of the data, as documented in Privacy Act SORNs, PIAs, Privacy Act Statements/Notices, and information sharing agreements, will be reviewed as a part of the process to on-board new use cases (*e.g.*, new information sharing agreements). This will help to ensure that individuals who provide the information receive adequate public notice of the purposes for collection and uses of the data. The process under which such reviews occur will vary according to the intended use of the data at issue. For example, if the Data Hub is providing support to the execution of bulk information sharing agreements with national security partners, the DHS Data Access Review Council (DARC) would serve as the forum for the Oversight Offices to review the data sharing proposed. If the Data Hub is supporting the development of a uniform baseline of screening and vetting, then separate, interagency legal and privacy, civil rights, and civil liberties (PCRCL) working groups would provide oversight. I&A is developing a cloud strategy that, among other things, will include a process by which internal DHS enterprise mission requests supported by the Data Hub are evaluated and approved. Until this strategy is finalized, I&A will submit requests to use the Data Hub for enterprise-wide missions unrelated to the development of a uniform baseline of screening and vetting to Oversight Offices (*e.g.*, legal, privacy, and civil rights and civil liberties) on a case-by-case basis using the DARC.

Privacy Risk: There is a risk that the Data Hub will share information with partners that do not have authority to collect or use the data.

Mitigation: This risk is mitigated. Processes have been developed to ensure oversight and compliance for all datasets being added to the Data Hub. These processes ensure that representatives from the Oversight Offices will review and approve the use cases that the Data Hub supports, as appropriate.

Privacy Risk: There is a risk that personnel authorized to access information in the Data Hub could use their access for unapproved or inappropriate purposes, such as performing searches on themselves, supervisors, or coworkers.

Mitigation: The DHS I&A Chief Information Officer employs audit trails on all DHS systems, which are reviewed if a problem or concern arises regarding the use or misuse of the information. Additional reporting capabilities will be developed in coordination with representatives from I&A CIO, Privacy, CRCL, and General Counsel. When users log in, they must acknowledge and consent to monitoring before access will be provided.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This PIA and its appendices provide notice of the privacy risks related to the Data Hub and how information will be transported and maintained. However, the Data Hub itself does not and cannot provide direct notice to individuals that their information will be used by the Data Hub because it does not interface with those individuals.

It is the responsibility of the source systems that provide the data to the Data Hub to provide notice to individuals from whom information is collected. These source systems and their respective PIAs and SORNs, which provide program-specific guidance on notice, are outlined in the appendices of this PIA.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals do not have the opportunity to consent to use of their information by the Data Hub. However, individuals may have the opportunity to decline to provide the information when it is initially collected by the source system. These source systems and their respective PIAs and SORNs, which provide program-specific guidance on consent, are outlined in the appendices to this PIA.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may be unaware of the Data Hub, and what potential impacts it has on individuals and their data.

Mitigation: This risk cannot be fully mitigated, particularly given that the Data Hub itself does not and cannot provide direct notice to individuals that their information will be used by it. Due to the sensitive and classified nature of analysis performed on the TS/SCI-level network, it may not be possible for individuals to be informed when their information is part of use cases that the Data Hub supports.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Because the datasets that interact with the Data Hub will be governed by different SORNs, the retention periods for each will be different. The retention of the data is determined on a program-by-program basis based on the authorities of the Component or agency that owns the data. The retention period for each dataset is outlined in the addenda to this PIA.

Representatives from the DHS Oversight Offices review and evaluate retention periods per use case to ensure those periods are appropriate. Specifically, if the Data Hub is providing support to the execution of bulk information sharing agreements with national security partners, the Data Access Review Council (DARC) would serve as the forum for the Oversight Offices to review the data sharing proposed. If the Data Hub is supporting the development of a uniform baseline of screening and vetting, then separate, interagency legal and privacy, civil rights, and civil liberties (PCRCL) working groups would provide oversight. I&A is developing a cloud strategy that, among other things, will include a process by which internal DHS enterprise mission requests supported by the Data Hub are evaluated and approved. Until this strategy is finalized, I&A will submit requests to use the Data Hub for enterprise-wide missions unrelated to the development of a uniform baseline of screening and vetting to the Oversight Offices on a case-by-case basis using the DARC.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the Data Hub may retain information longer than necessary.

Mitigation: This risk is partially mitigated. The relevant retention period for each dataset is documented internally in documents that outline the handling requirements for the dataset. This documentation collectively and consistently defines (in accordance with the record retention schedules) the authorized retention period. DHS will tag the data in accordance with source system retention period to ensure that records are deleted in alignment with their respective records schedule. If system outages or maintenance periods prevent records from being deleted during a certain window of time, those records will be deleted immediately upon the restoration

of the system. I&A CIO will provide reports that include the number of records deleted over defined or requested periods of time.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The Data Hub may be used to share data with a variety of partners both internal and external to DHS.

Because some datasets may contain information involving Special Protected Classes (SPC) of individuals,[16] special sharing, and handling requirements may need to be implemented as part of the Data Hub for particular sharing agreements or mission use cases. The Data Hub will implement the appropriate safeguards needed to properly identify and tag SPC data to allow the proper execution of applicable sharing requirements and restrictions. Training related to the data for particular datasets and any special restrictions on handling, use, and disclosure of that data, including SPCs, will also be provided as applicable.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Because source system agencies and partners each have different authorities and will be governed by different SORNs, the compatibility of the external sharing to be technically implemented by the Data Hub will be analyzed on a case-by-case basis. This will be outlined in the appendices of this PIA.

Before executing a mission request, each request is reviewed by the appropriate Oversight Offices. Specifically, if the Data Hub is providing support to the execution of bulk information sharing agreements with national security partners, the DARC would serve as the forum for the Oversight Offices to review the data sharing proposed. If the Data Hub is supporting the development of a uniform baseline of screening and vetting, then separate, interagency legal and privacy, civil rights, and civil liberties (PCRCL) working groups would provide oversight. I&A is developing a cloud strategy that, among other things, will include a process by which internal DHS enterprise mission requests supported by the Data Hub are evaluated and approved. Until this strategy is finalized, I&A will submit requests to use the Data Hub for enterprise-wide missions

[16] *See* 8 U.S.C. § 1367, Penalties for unauthorized disclosure of information of special protected classes, *available at* https://www.govinfo.gov/app/details/USCODE-2011-title8/USCODE-2011-title8-chap12-subchapII-partIX-sec1367.

unrelated to the development of a uniform baseline of screening and vetting to the Oversight Offices on a case-by-case basis using the DARC.

6.3 Does the project place limitations on re-dissemination?

The re-dissemination limitations of the information shared via the Data Hub are likely to vary for each dataset or information sharing agreement. Internal project documentation for that use case, as well as information sharing agreements between the source system agency and partner will outline these requirements.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The Data Hub maintains logs of the information shared between agencies.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that authorized users, who are exposed to PII as a routine part of their official duties, may make an inappropriate disclosure of information, either intentionally or unintentionally.

Mitigation: This risk is mitigated through the provision of annual specialized training on privacy and Intelligence Oversight, including the appropriate and inappropriate uses and disclosures of the information to all IC program personnel. I&A personnel use of systems and access to data is monitored and audited. Should a user inappropriately disclose this information, he or she is subject to the loss of access, as well as disciplinary action up to and including the loss of a security clearance or termination.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

The Data Hub moves and stores data for a variety of purposes. It does not exercise any separate authority to collect, retain, use, or share information. It does not own any data, but rather sponsors the technology in which the records are housed. Therefore, the Data Hub does not receive or have the authority to determine individual requests for access.

Notwithstanding applicable exemptions, DHS reviews all requests for access under the Privacy Act of 1974 or Freedom of Information Act on a case-by-case basis. When such a request is made, and compliance would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained

within this system, the applicable exemption may be waived at the discretion of I&A and the data owner in accordance with procedures and points of contact published in the applicable SORN.

Under the Information Sharing Environment (ISE) Privacy and Civil Liberties Protection Policy,[17] the Department has also established a process to permit individuals, regardless of citizenship or immigration status, to file a privacy complaint. Individuals who have privacy complaints concerning analytic division intelligence activities may submit complaints to the Privacy Office at privacy@dhs.gov. Individuals may also submit complaints alleging abuses of civil rights and civil liberties or possible violations of privacy protections by I&A employees, contractors, or grantees to the Office of the Inspector General by filling out an allegation form located at https://www.oig.dhs.gov/hotline,.

The procedures for submitting FOIA or Privacy Act requests for I&A programs are available in 6 CFR Part 5. Please contact:

Office of Intelligence & Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528
Attn: FOIA Officer
Email: I&AFOIA@hq.dhs.gov

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Because the Data Hub does not exercise any separate authority to collect, retain, use, or share information, it does not operate or provide direct support for any specific redress process. Individuals should also refer to the applicable PIA and SORN for each relevant dataset to determine the procedures that allow individuals to correct inaccurate or erroneous information.

Individuals may request access to their records under the FOIA process noted above, and I&A may assist in routing requests to the appropriate entity. Individuals may also file a privacy complaint as previously described.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals can identify the procedures for correcting their information for a particular dataset by reviewing the program's applicable PIA and SORN, which can be found in the appendices of this PIA.

7.4 Privacy Impact Analysis: Related to Redress

[17] DHS Privacy and Civil Liberties Policy Guidance Memorandum, 2009-01, (June 5, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.

Privacy Risk: Without the ability to access and correct their information, individuals have limited ability to ensure the accuracy of information held and used in the Data Hub.

Mitigation: Although the ability of an individual to access and correct information stored by I&A is limited given the function of the Data Hub, controls are in place to partially mitigate this risk. Individuals are able to seek redress and correct information with the Components or agencies that originally collected the information stored in the Data Hub, which will be implemented in the Data Hub consistent with any corrections or updates made in the source system for that information.

In addition, as noted earlier, individuals, regardless of citizenship or legal status may request access to their records under FOIA. Individuals may also file a privacy complaint with the DHS Privacy Office.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

I&A takes appropriate action when violations of its privacy policies are found. Individuals who fail to implement safeguards will be held accountable through disciplinary or corrective actions. Violation may result in the revocation of access or disciplinary measure. Violations by users outside of the DHS will additionally result in the reporting of the misuse to the user's agency for additional processing and review. For additional information on the consequences of accountability for violation of federal laws, regulations, directives, or DHS policy, see the DHS Privacy Incident Handling Guidance.[18]

The DHS Office of the Inspector General reviews DHS programs and activities, including those within I&A, to promote effectiveness and prevent abuse. In addition, the DHS Privacy Office can conduct a Privacy Compliance Review.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

The Data Hub will provide services to specific mission use cases. Depending on the mission use and datasets involved, training can be provided for individuals using those datasets through an approved mission application.

8.3 What procedures are in place to determine which users may access the information and how does the project determine

[18] https://www.dhs.gov/publication/privacy-incident-handling-guidance.

who has access?

Decisions about access to the data are facilitated by representatives from the Office of General Counsel, Privacy Office, and Office of Civil Rights/Civil Liberties, as well as data owner. Once decisions are made concerning the access controls for different categories of users, those decisions are documented and written procedures are developed for how those privileges will be granted, managed, and subject to review by oversight offices. Specifics concerning the access controls and permissions for specific mission use case will vary.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Each request is reviewed by the Oversight Offices to ensure compliance with the law and that information sharing and other privacy, civil rights, and civil liberties protections are sufficient. Specifically, if the Data Hub is providing support to the execution of bulk information sharing agreements with national security partners, the DARC would serve as the forum for the Oversight Offices to review the data sharing proposed. If the Data Hub is supporting the development of a uniform baseline of screening and vetting, then separate, interagency legal and privacy, civil rights, and civil liberties (PCRCL) working groups would provide oversight. I&A is developing a cloud strategy that, among other things, will include a process by which internal DHS enterprise mission requests supported by the Data Hub are evaluated and approved. Until this strategy is finalized, I&A will submit requests to use the Data Hub for enterprise-wide missions unrelated to the development of a uniform baseline of screening and vetting to the Oversight Offices on a case-by-case basis using the DARC.

Responsible Officials

Benjamin Stefano
Chief Information Officer
Office of Intelligence & Analysis
Department of Homeland Security

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

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

Please refer to separate Appendix for list of approved datasets in the Data Management Hub (Data Hub). The Appendix can be found on the DHS Privacy website at DHS/ALL/PIA-076 Data Management Hub | Homeland Security.