Privacy Impact Assessment

for the

S&T Operations and Requirements Analysis Division

DHS Reference No. DHS/S&T/PIA-043

February 9, 2022

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS, or the Department) Science and Technology Directorate (S&T) Operations and Requirements Analysis Division (ORA) provides analytical expertise by conducting capabilities, requirements, operations, and alternatives analyses to maximize efficiency and effectiveness for the Homeland Security Enterprise. S&T ORA uses Systems of Systems Operational Analytics, hereinafter referred to as SoSOA, a virtual, web-based environment that meets DHS and Homeland Security Enterprise critical mission and operational needs, to help DHS improve its structured analytics, data integration, and data collaboration. S&T is publishing this Privacy Impact Assessment (PIA) because ORA uses systems, such as SoSOA, containing personally identifiable information (PII) and privacy-sensitive information to perform analysis and to assess the privacy risks associated with the use, maintenance, dissemination, and disposal of privacy-sensitive data stored in systems or cloud environments and used to make operational decisions.

Overview

ORA uses its technical and analytic expertise to identify DHS capability gaps, perform mission and requirements analysis, and perform operations analysis to improve DHS operations. Furthermore, ORA conducts research, development, testing, and evaluation (RDT&E) of advanced computational and analytics technologies to support critical DHS missions throughout the Department. This work responds to, and fulfills, critical missions and authorities under 6 U.S.C. § 182, *Responsibilities and Authorities of the Under Secretary for Science and Technology*.

This Privacy Impact Assessment is scoped to cover ORA's use of technical and analytic expertise that may support S&T and DHS, along with DHS Components' use of SoSOA. In addition, this Privacy Impact Assessment covers ORA's use of technology and the data associated with that technology for structured analytics, data visualization, and collaboration purposes within SoSOA. Additional privacy reviews may need to be done separately by the Component providing the data if the DHS Component is using analytical information provided by ORA.

ORA works with S&T programs and DHS Components, who may leverage the Homeland Security Enterprise,[1] to facilitate technical problem-solving for homeland security analytic missions, such as counterterrorism, border security, and national preparedness and resilience. ORA's mission also expands to conducting RDT&E activities to deliver effective and innovative insight, methods, and solutions to address DHS and Homeland Security Enterprise critical needs. Furthermore, ORA supports the Under Secretary for Science and Technology, who serves as the

[1] DHS Instruction Number 034-06-001, *Department Reporting Requirements*, defines the Homeland Security Enterprise as "[t]he collective efforts and shared responsibilities of federal, state, local, tribal, territorial, non-governmental, private-sector, and international partners—as well as individuals, families, and communities—to maintain critical Homeland Security capabilities."

chief scientific and technological advisor for the Secretary of Homeland Security,[2] by providing relevant analysis and reporting for essential operational decisions. In sum, ORA enables S&T to meet its responsibilities for identifying technologies, concepts, and processes that have the potential to be incorporated into operational environments for the purpose of increasing the effectiveness, efficiency, and safety of the Department, Components, and Homeland Security Enterprise personnel and missions.

SoSOA

ORA developed SoSOA, a virtual web-based environment for collaborative operational analysis, that provides technical services to DHS across all Components while improving their structured analytics, data visualization, and collaboration. SoSOA allows ORA to conduct collaborative operational analysis, data visualization, and requirements management to refine technical problems, capability gaps, data sets (which may include privacy-sensitive information), technology, operational assessments, and mission performance that meet DHS and Homeland Security Enterprise critical mission and operational needs. SoSOA systematically exploits large volumes of information and converts data into an organized and consumable format, using refined methodologies and analytic tools/applications. SoSOA will incrementally become a DHS enterprise product that integrates data across DHS Components using cloud-based software, infrastructure, and common platform to service identified use cases.

This Privacy Impact Assessment provides an overview of ORA's activities and use of SoSOA. The specific types of tools, applications, data, and analysis to be used for any given ORA project, using SoSOA, will depend on the mission use case(s) supporting the project. SoSOA is expected to be used exclusively by DHS users. It is currently being used by S&T ORA; however, the user community will eventually, through partnership and collaboration, extend to other DHS Components.

ORA RDT&E Activities

ORA selects actionable research activities based on optimizing the return from limited research and development resources. As part of each research activity, ORA works with the S&T Privacy Office and the S&T Office of General Counsel, as well as other DHS Component compliance offices, to establish guidelines for the collection, analysis, and disposition of data. When ORA conducts RDT&E without an operational partner, those activities do not result in any operational action; rather, ORA uses technical results from experiments and pilots to inform the development of next-generation mission and operations technologies. While ORA does not use data for operational purposes, when working with a DHS Component, ORA may leverage Components' authorities to conduct RDT&E in order to support that Component's operational activities. ORA's analysis may be included in instances where DHS Components report

[2] *See* DHS Delegation: 10001-01, Delegation to the Under Secretary for Science and Technology, April 28, 2014.

information to appropriate federal, state, or local authorities, should exigent circumstances arise (such as significant threat to life and property).

ORA's RDT&E activities include:

- Requirements Analysis is used to support the development, integration, implementation, and/or fielding of required new capabilities for DHS Components and offices. This includes stakeholder engagement, gap analysis, budget allocation, program oversight, and prioritization methodology analysis.
- Operations Analysis is used to monitor and ensure the adequacy and operations of existing DHS capabilities. This includes business case analysis, cost analysis and estimating, analytical programming support, modeling and simulation, and verification and validation.

Data Sources and Use

To execute the above activities, ORA receives, sends, and uses data, which may involve personally identifiable information, only within the scope of established data handling guidance and in compliance with DHS policies.[3]

- Federal, State, Local, Tribal, and Territorial Government Data: For critical missions of DHS, and in accordance with DHS authorities, ORA may collaborate with government data owners in data analytics activities. In those cases, legal determinations, appropriate collaborative agreements, and privacy oversight will be used to establish guidelines for specific activities. Appropriate data handling guides will be developed for each data source that is part of activity.
- Research Data: ORA uses research data from government (e.g., federal, state, local, tribal, and territorial), industry, and academia. ORA will use appropriate data from these sources, where data has been developed and curated for the furtherance of research and development. For example, ORA partnered with a DHS component to pair radar system performance data with terrain and atmospheric data to evaluate overall performance and determine how many individual radar systems were needed.

Once the proper legal and privacy reviews are conducted, the above data sets may potentially be comingled with DHS Component or other government data in furtherance of research and development. Results of ORA's analysis would then be used by DHS for developing mission

[3] DHS 4300A Sensitive System Handbook is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01, Information Technology System Security. See U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, available at https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

strategy, understanding technical risk, justifying acquisitions, characterizing capability gaps, or driving performance improvements. However, no data sets containing personally identifiable information that are collected for a specific purpose and evaluated for an activity will be re-purposed for other or future initiatives. Data from projects is not shared with other partners unless specific agreements are put in place to address data sharing requirements.

ORA may conduct analysis to include testing and evaluation in support of DHS operational requirements with a DHS component, where the authorities of the DHS Component benefiting from the outputs will guide the activity, and the data collected or received may include personally identifiable information. Prior to using that data, ORA coordinates with the DHS Component or partner to ensure that ORA's role is limited to RDT&E. This would be documented in the development of a Memorandum of Understanding (MOU). Each authorized data set that ORA uses is subject to the data owners' specified controls and handling guidance, privacy oversight, and security controls, which are further clarified in a data handling guide. The guide includes instructions for sharing, destruction, and certification of removal of data from ORA or other S&T systems at the end of the activity. At the conclusion of the project, personally identifiable information is retained and/or destroyed in accordance with applicable federal record schedules. Researchers may retain aggregated research data (without personally identifiable information) in accordance with applicable federal record schedules, as it may help inform future RDT&E efforts.

As a result of legal and privacy reviews, the types of data to be used in each activity are rationalized and minimized to the data sets required to enable appropriate research results. Prior to the use of any data set for analysis, the S&T Privacy Office conducts a privacy review to determine whether additional privacy compliance documentation is needed, for example, in the form of a Privacy Threshold Analysis (PTA), Privacy Impact Assessment, and/or System of Records Notice (SORN).

Data elements from DHS Components, other government agencies, industry, or academia that may be used in ORA research activities may include the following:

- Full Name;
- Home Street Address;
- Home Phone Number;
- Business Street Address;
- Business Phone Number;
- Email Address;
- Employer Identification Number (EIN);

- Social Security number (SSN);
- Taxpayer Identification Number (TIN);
- Encounter ID Number (EID);
- Fingerprint Number (FIN);
- Date of Birth;
- Gender/Sex;
- Passport Number;
- Citizenship/Nationality;
- Country of Birth;
- IP Addresses;
- Facial Images;
- Video; and
- Audio.

Other information collected and stored by ORA may include:

- Protected critical infrastructure information;
- Law Enforcement Sensitive data provided by a Component to ORA that is historical in nature and not related to an active investigation;
- Video recording data; and
- Other non-privacy sensitive information derived from publicly available information from industry, academia, or from federal, state, local, and tribal government. entities.

The Account Request for a SoSOA user collects the individual's:

- First Name;
- Last Name;
- Display Name;
- Department;
- Government Email Address;
- Government or Contractor status; and

- Unique Cloud Factory ID.

SoSOA Users and Role Management

Access to SoSOA will be granted by S&T SoSOA System Administrators and will be limited to users within the DHS network; no users external to DHS will be authorized. DHS and S&T are the account owners and provide all necessary credentialing services. Users will access the SoSOA web application from DHS-approved computing devices via single sign-on authentication using the DHS Application Authentication system.[4] SoSOA users are assigned specific roles, either system administrators, data stewards, analysts, or viewers, as appropriate and in accordance with the legal and policy guidelines developed for each research activity. This enables ORA to control user access to appropriate data sets and applications required for each research activity based on a user's role. These roles can be assigned on a per-application, per-table, and per-file basis. As an example, a single user can be a part of multiple groups that respectively gives the user ingest/upload privileges for a specific database, edit privileges within a certain application, and view-only privileges for a specific dataset. If the user is not a part of a group with specific permissions to a portion of the SoSOA environment, they will not have access to that portion.

Access to SoSOA is granted through an Account Request form that is processed and approved by SoSOA project owners and system administrators. Accounts and access are granted in accordance with DHS policies, such as those found in the DHS 4300A Sensitive Systems Policy Handbook, which requires users to be cleared by personnel security and agreements to be executed including rules of behavior for usage of government systems. Further, each user receives general security and privacy training annually and is provided specific training on handling different types of data being used, when required, prior to gaining access to any ORA system.

SoSOA Cloud Environment Systems

S&T Cloud Factory, a cloud platform that leverages Amazon Web Services (AWS) GovCloud infrastructure (a FedRAMP-approved system), provides tenancy to both the pre-production and production environments within the DHS boundary. Personally identifiable information will only be stored in the production environment. All data, including personally identifiable information, is encrypted both in transit and at rest. Access to data stored in SoSOA is limited to S&T authorized users based on their roles (e.g., system administrators, data stewards, analysts, or viewers) and auditing mechanisms are also associated with role-based access to the data sets. The cloud provider does not have any access or rights to the data stored in the SoSOA environment, and the data is encrypted and accessible only by DHS authorized users determined

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY PRIVACY IMPACT ASSESSMENT FOR THE APPLICATION AUTHENTICATION SYSTEM (APPAUTH), DHS/ALL/PIA-060 (2019), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

though role-based controls. This is the setting S&T requires for cloud providers and it cannot be turned off. S&T uses the appropriate cloud-based computing environment (to include infrastructure, platform, security boundaries, applications, and services) to control the user's community access. Only DHS authorized users with a need-to-know will be permitted access to the SoSOA environment.

SoSOA Data Handling

Any dataset maintained and used in SoSOA follows appropriate handling processes and procedures, which are outlined in the Rules of Behavior and Terms of Service. Data used for SoSOA functions is limited to the scope of the task aligned with role-based access. Data sets are stored separately based on the purpose of the task and account for data source. ORA does not generate new data sets, but instead performs analysis on existing data and creates data/analytic outputs from the source data (e.g., visualizations and dashboards).

Data stored in the comma-separated values (CSV) file format (e.g., Microsoft Excel) can be uploaded to SoSOA by DHS Data Stewards using the SoSOA Ingest Application. The data is then parsed to detect data headers and data types by multiple Application Programming Interfaces (API) running in the SoSOA environment. Once the data is prepared, it gets sent to a SoSOA database. Authorized users can then interact with that data using one of the SoSOA applications, which may produce additional files that are stored within the SoSOA application. Analysis applications within SoSOA also allow users to upload files directly within those applications, making the data available only for authorized users within those applications. S&T System administrators will be notified of each new upload into the SoSOA environment and will review uploads weekly for privacy compliance.

SoSOA users with access to data can perform data exports. Each SoSOA application has different export capabilities. Tableau, a visualization software, provides functionality to export data in tables and reports; Jupyter allows data files to be downloaded. All activities related to administrative privileges are audited, logged, and limited to S&T personnel. All SoSOA data download actions are logged, and data is regularly backed up. Jobs are automatically scheduled to offload the data from SoSOA into secure and redundant Amazon Web Services storage, such as Amazon Simple Storage Service.

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?

ORA, as part of DHS S&T, conducts RDT&E of advanced computational and analytics technologies that have potential to benefit DHS Components' critical missions and fulfill S&T's mission responsibilities under 6 U.S.C. § 182, *Responsibilities and Authorities of the Under*

Secretary for Science and Technology. Prior to initiating a new project, S&T authorities under 6 U.S.C § 182 are viewed in conjunction with the requirements set forth in the Privacy Act of 1974 along with DHS policy to ensure all data sets are properly collected.

Data is collected and used in accordance with authorities that enable RDT&E activities within S&T or in partnership with the data owner. Prior to the acquisition or use of any data set for analysis, the S&T Privacy Office, in conjunction with legal counsel, conducts a review to determine if the information is consistent with the appropriate authorities and privacy requirements. The privacy review will determine if the collection of information is consistent with the authorities. This Privacy Impact Assessment will be updated, as appropriate, to discuss any further authorities for collection and use.

DHS Components and offices will work with ORA to ensure that storage and use of data for operational purposes in SoSOA is consistent with their applicable authorities. Specific uses of operational data will not be described in this Privacy Impact Assessment and will be covered separately by the appropriate DHS Component privacy office, which will be responsible for developing activity-based privacy compliance documentation as appropriate. Each proposed project will be reviewed for privacy compliance and may be the subject of a distinct Privacy Threshold Analysis.

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

ORA may receive copies of data sets from DHS Components, which may include personally identifiable information. In SoSOA, the data owner, project owner, or data steward will aggregate this information prior to sharing with ORA. In turn, ORA will use this aggregated data to perform specific tasks to assist in policy and operational needs when requested. For example, S&T may recommend the number of DHS staff needed to capture fingerprints or the number of devices needed by DHS staff to perform a task. The data will only be used as reference and will not be altered. The S&T Privacy Office will coordinate with the data source to ensure a System of Records Notice review is completed on a case-by-case basis.

ORA collects, maintains, and uses data for RDT&E purposes consistent with the purpose and routine uses of the DHS/S&T-001 Research, Development, Test, and Evaluation Records System of Records Notice[5] and respective component System of Records Notices used by data owners for the original data collection. Similarly, any data maintained or used in SoSOA for operational purposes will be subject to the respective System of Records Notice governing the

[5] The DHS/S&T-001 Research, Development, Test, and Evaluation Records System of Records Notice is being updated to more clearly account for the collection of publicly available information, including social media. The current version is *available at* https://www.dhs.govystem-records-notices-sorns.

original data collection.

DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[6] covers the records maintained to provide users authorized access to ORA systems, such as SoSOA.

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

Yes. ORA completed a System Security Plan (SSP) for SoSOA, which supported the system's full DHS accreditation in April 2021. This SSP captures the functions and features of the system, including all the hardware and software accessible to SoSOA users.

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

ORA follows National Archives and Records Administration (NARA) and DHS applicable record schedules throughout the course of each project. Since ORA is not the originator of the information used to perform analysis, ORA will adhere to the source data records retention schedule of any data ingested.

Any data maintained and used in SoSOA for operational purposes is covered under the previously established records schedules for source system records.

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.

ORA systems, such as SoSOA, are not subject to Paperwork Reduction Act (PRA) requirements because information is collected from other data sources. The Paperwork Reduction Act requirements are addressed on a project-by-project basis. However, information from source systems may be subject to the Paperwork Reduction Act when originally collected. S&T will update this Privacy Impact Assessment accordingly should Paperwork Reduction Act requirements arise.

Section 2.0 Characterization of the Information

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

[6] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792, (November 27, 2012), *available at* https://www.dhs.govystem-records-notices-sorns.

Data types originating from DHS Components, other government agencies (e.g., federal, state, local, tribal, and territorial government entities), industry, and academia that may be used in ORA research activities may include the following information:

- Full Name;
- Home Street Address;
- Home Phone Number;
- Business Street Address;
- Business Phone Number;
- Email Address;
- Employer Identification Number (EIN);
- Social Security number (SSN);
- Taxpayer Identification Number (TIN);
- Encounter ID Number (EID);
- Fingerprint Number (FIN);
- Date of Birth;
- Gender/Sex;
- Passport Number;
- Citizenship/Nationality;
- Country of Birth;
- IP Addresses;
- Facial Images;
- Video; and
- Audio.

Other information collected and stored by ORA may include:

- Protected critical infrastructure information;
- Law Enforcement Sensitive data provided by a Component to ORA that is historical in nature and not related to an active investigation;
- Video recording data; and

- Other non-privacy sensitive information derived from publicly available information or from federal, state, local, tribal, and territorial government entities.

The Account Request for a SoSOA user collects the individual's:

- First Name;
- Last Name;
- Display Name;
- Department;
- Government Email Address;
- Government or Contractor status; and
- Unique Cloud Factory ID.

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

The data used in ORA RDT&E activities originates from DHS components, other government agencies (i.e., federal, state, local, tribal, and territorial government entities), industry, and academia. Prior to the use of any data set for analysis, the S&T Privacy Office conducts a privacy review. ORA provides a description of the data set, if personally identifiable information is included, data source(s), and how data is transferred. The S&T Privacy Office will then use the information provided by ORA to determine if the collection is consistent with the information sharing agreement. ORA researchers may receive data provided by a data-sharing partner once the project-specific legal and privacy reviews are conducted. These reviews are properly documented and governed through an information sharing access agreement (ISAA), such as a Memorandum of Understanding.

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

Yes. ORA uses publicly available information to perform its analysis. As a result of legal and privacy reviews, the types of data to be used in each activity are analyzed and minimized to the data sets required to enable appropriate research results.

2.4 Discuss how accuracy of the data is ensured.

The data owner is responsible for the accuracy, completeness, and quality of the data provided to ORA, as ORA is not the originator of the data. While the accuracy, timeliness,

completeness, and quality of the data may be relevant for the ORA research activity being conducted, since RDT&E data is not used to make determinations about individuals, data accuracy, timeliness, completeness, and quality is not a key privacy concern in this context. ORA does not attempt to make, nor does it have authority to make, operational decisions. If a Component decides to use data held by ORA for an operational purpose, the Component is responsible for verifying the accuracy of the data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that SoSOA will ingest data from different sources that operate under different authorities.

Mitigation: This risk is mitigated. The data owners, project owners, and the respective DHS component privacy offices are required to review individual and aggregated data to be ingested by SoSOA. They ensure that the use of this data is consistent with the underlying authorities as well as the purpose of the original collection as stated in the pertinent System of Records Notice. Data sources and authorities are associated with specific SoSOA projects. Furthermore, data is logically isolated on a project basis, which prevents comingling of data between projects or unauthorized user access.

Privacy Risk: There is a risk that ORA is collecting more personally identifiable information than necessary for ORA to perform its RDT&E activities.

Mitigation: This risk is partially mitigated, as the information required is not always identified at the initiation of a project. At project initiation, ORA will meet with the S&T Privacy Office to discuss how to minimize the personally identifiable information used while performing the required research and then work with the program to complete a Privacy Threshold Analysis for each project. For every activity, data obtained or collected is limited to the purpose of that specific activity. Data collected for one purpose or activity is not shared or used for another project or activity. All personally identifiable information is deleted or returned to the data owner once the project is completed. However, as needed and in accordance with the appropriate file plan, ORA may retain aggregated and anonymized research data (without personally identifiable information), as it may help inform future RDT&E efforts.

Privacy Risk: There is a risk that information about individuals is not accurate, relevant, timely, and complete.

Mitigation: This risk is partially mitigated. ORA depends on the accuracy and quality of information provided by the data owners and source systems. In most instances, the owner of the data (e.g., another DHS Component) manages data quality. ORA will inform the data owner if it identifies data quality or integrity issues with the data it receives, and the data owner is responsible

for addressing issues related to the accuracy and quality of their data. Regardless, ORA's use of SoSOA is limited to RDT&E and does not make operational decisions about an individual. One of the goals of ORA's RDT&E is to evaluate the accuracy, timeliness, and completeness of the data DHS uses.

Similarly, the owner of any data used for operational purposes will manage data quality in most instances and be responsible for the accuracy and quality of the data.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

ORA's collection and use of data is scoped at the beginning of each analysis activity to accomplish an RDT&E objective to enable complex, timely, mission-focused decisions across DHS and the Homeland Security Enterprise. This scoping occurs as a collaboration between the S&T Privacy Office, the S&T Office of General Counsel, and ORA researchers. ORA identifies proposed data sets, proposed data components, and a technical approach that will be needed to complete the activity for every research effort. ORA also identifies potential partners such as federal, state, and local government entities to participate in analysis activities. S&T will conclude an information sharing access agreement, such as a Memorandum of Understanding that sets the terms and conditions that govern data access, use, sharing, and data disposal with the partner(s) or data provider(s). Final agreements must be reviewed and approved by the respective legal and privacy oversight functions of the parties, prior to agreement execution.

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.

Yes. ORA will produce information regarding the functional performance of electronic search, query**,** and analysis technologies. The results of RDT&E will inform partners (e.g.**,** DHS operational Components) regarding the accuracy, reliability**,** and other operational characteristics of such technologies for decision making.

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

Only DHS authorized individuals, which may include individuals from other DHS Components, may access ORA-managed systems such as SoSOA. All users must be active DHS employees with a valid Personal Identity Verification (PIV) card and must complete a user account request and accept pre-established rules of behavior before access is granted. Users only have access to the data and application(s) required based to fulfill their specific roles, which are assigned

by the S&T system administrator.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: ORA may use stored information beyond the purpose of an RDT&E activity.

Mitigation: This risk is partially mitigated. Users and administrators of ORA-managed systems are held accountable for the protection of personally identifiable information by S&T's use of access controls, audit logs, and training. All user activity in ORA-managed systems, such as SoSOA, are logged. User activity will be reviewed on regular and ad-hoc bases. Patterns of usage should be consistent with the analysis goals and results that an individual's work products indicate. Discovery of unauthorized use of these systems will be reported immediately to management, compliance, and legal authorities for remedial or punitive action. Intentional unauthorized use will result in a permanent prohibition of access, as outlined in the Rules of Behavior and Terms of Service.

All users receive training for their system user role and the acceptable use of the rights/privileges associated with their user role. All users complete a user account request and agree to a system-specific rules of behavior. All DHS personnel including users of ORA-managed systems are required to complete privacy training. Users are required to complete data-specific training when information requires special protection. System administrators will audit user access to personally identifiable information in compliance with privacy principles and all applicable privacy protection requirements. Data obtained for a project is only collected for the purpose of the specific project. Data, which may include personally identifiable information, collected for one purpose is not shared or used for another project or initiative. Data is purged or returned to the data owner at the end of RDT&E activity. All users must be active DHS employees and valid Personal Identity Verification card to access ORA-managed systems.

Privacy Risk: There is a risk that information collected or generated under RDT&E authorities may be used for operational purposes.

Mitigation: This risk is partially mitigated. ORA does not use data for operational purposes. The RDT&E products that come from ORA applications, such as SoSOA, may be used by decision makers in support of Component-specific operations. All data that ORA uses for RDT&E is logically separated from data used for operational purposes, and access to either form of data is limited to those with a need to know with the proper role-based access. Unless there is explicit Privacy and Component approval, data used for RDT&E purposes will not be comingled with data used for operational purposes.

In the event ORA partners with an operational Component and the operational Component seeks to use the RDT&E information for operational purposes, the Component must determine

that the proposed use falls within the Component's operational authorities. If a Component decides to use ORA's data for an operational purpose, the Component is accountable for verifying the accuracy of S&T data.

The Component's Privacy Office also must determine that the data use is consistent with the Component's applicable System of Records Notice(s). In addition, Components may be required to complete additional privacy compliance requirements (e.g., Privacy Threshold Analysis, Privacy Impact Assessment) before the operational use.

Section 4.0 Notice

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

This Privacy Impact Assessment functions as the primary form of notice to individuals that ORA conducts research on government, commercial, research consortia, and open-source data sets. Appropriate legal and privacy reviews will be conducted before data is collected to ensure all legal, privacy, and DHS policies are adhered to properly. Government data will be collected in accordance with authorities that enable research and development activities within ORA or in partnership with the data owner.

DHS Components provide individuals with notice at the initial collection into DHS Component source systems. The source systems have undergone appropriate privacy analysis and appropriate privacy compliance documents have been completed. In addition, the data's use by ORA has been determined to be compatible with the purpose for which the data was originally collected. S&T will conduct similar analysis when using other government data (e.g., federal, state, local, tribal, and territorial), industry, and academia.

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

In most cases, ORA ingests copies of data provided and authorized by the data owners and source systems, such as other government agencies. For government agency data, consent for the collection of the data, and the opportunity to decline or opt out, occurred when the government agency initially collected the data. The use of government agency data by ORA must be determined to be compatible with the purpose of the original collection.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive notice that their information may be used in ORA activities, which may include support of operational decisions.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment provides notice that ORA may collect or store information about individuals for the purposes described in this Privacy Impact Assessment in accordance with legal, privacy, and DHS policies. Much of the data transferred to ORA is owned by data sharing partners. Individuals consent to uses, decline to provide information, or opt out during the initial information collection, by the data sharing partner. Components, whose data is used by ORA, are responsible for providing notice to the public for their use of that data through Privacy Impact Assessments, System of Records Notices, and Privacy Act Statements/Notices, as appropriate. The S&T Office of General Counsel and S&T Privacy Office will review the authorities and terms associated with the use of each data set and ensure they are acceptable for ORA activities. Only data that complies with legal, privacy, and DHS policies for research can be used by ORA.

Section 5.0 Data Retention by the Project

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

ORA will not retain research data beyond the end of a specific research activity. However, as needed and in accordance with the appropriate file plan, ORA may retain aggregated and anonymized research data (without personally identifiable information), as it may help inform future RDT&E efforts. Once the effort is concluded, ORA must delete or return data sets to the data owner, depending on the data source. Per the DHS/S&T-001 Research, Development, Test, and Evaluation Records System of Records Notice, personally identifiable information collected during the project is retained for the duration of the project; at the conclusion of the project, personally identifiable information is returned to the providing Component or destroyed. SoSOA will abide by the established data retention policy for each applicable data source for any external data used for operational purposes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that ORA may retain data longer than necessary.

Mitigation: This risk is mitigated. ORA fully mitigates this risk through routine reviews and audits. At the end of each project, the Information System Security Officer (ISSO) will ensure that data is properly disposed in accordance with DHS guidelines and appropriate privacy documentation is updated.

Section 6.0 Information Sharing

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.

No. Data is not shared outside of DHS.

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

Data is not shared outside of DHS.

6.3 Does the project place limitations on re-dissemination?

Data is limited to sharing internally within DHS upon privacy and legal review to ensure that the sharing of the information is both authorized and properly documented adhering to DHS privacy policies.

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

Data is not shared outside of DHS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that users may unintentionally share personally identifiable information with a third party.

Mitigation: This risk is mitigated. In the event ORA unintentionally shares personally identifiable information with a third party, or in the case of any other suspected or confirmed privacy incident, ORA will respond to and mitigate the incident in accordance with DHS's Privacy Incident Handling Guidance.[7] For awareness, all SoSOA users must complete mandatory DHS annual training ("Privacy at DHS: Protecting Personal Information") that addresses proper handling of PII. In addition, all users sign a DHS Rules of Behavior and agree to the system's Terms of Service that spell out the general guidelines of all systems involved before access into the system is granted.

[7] *Available at* https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf.

Section 7.0 Redress

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

ORA only maintains a copy of an individual's record from the data owner or source system. Therefore, individuals can gain access to their information by following the access procedures outlined in the Privacy Impact Assessments and System of Records Notices of the source systems. For information that ORA receives from government data owners, such as DHS components, individuals can gain access to their information by following access procedures outlined in the Privacy Impact Assessments and System of Records Notices of the data owner's source systems.

For information ORA receives or collects from commercial data providers, research consortia, and open sources, any individual who may desire to access whatever information ORA may have collected under this initiative may submit a Freedom of Information Act (FOIA) or Privacy Act request to the DHS FOIA Office to the address below, or electronically at https://foiarequest.dhs.gov/.

Chief Privacy Officer/Chief Freedom of Information Act Officer
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

The DHS/S&T-001 Research, Development, Test, and Evaluation Records System of Records Notice contains instructions for accessing information under the "Notification Procedure" section.

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

ORA only maintains a copy of an individual's record from the data owner or source system. An individual may access their record through the originator of the information (e.g., DHS Component) for any information that ORA receives in order to support a DHS Component's operations. If a Component decides to use ORA's data for an operational purpose, the Component is accountable for verifying the accuracy of S&T data. Individuals desiring to correct inaccurate or erroneous information can seek the support of the originating system's public records or Component FOIA/Privacy Act Officer.

Individuals who are seeking access to any record collected under this initiative may submit a FOIA or Privacy Act request for information that ORA uses for RDT&E purposes. DHS/S&T-001 Research, Development, Test, and Evaluation Records System of Records Notice contains instructions for accessing information under the "Notification Procedure" section.

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

ORA notifies individuals of the redress procedures for this initiative through this Privacy Impact Assessment and through the DHS/S&T-001 Research, Development, Test, and Evaluation Records System of Records Notice. ORA receives information from data sharing partners for RDT&E purposes and to provide analysis to DHS components' operations. Individuals who want to amend their information would need to do so by contacting the data sharing partner that initially collected the information. The System of Records Notices and Privacy Impact Assessments for the data owners' source systems explain how individuals can correct erroneous information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be able to correct inaccurate or erroneous information about themselves that is used in ORA activities.

Mitigation: This risk is partially mitigated. Much of the data used by ORA is a copy of data provided by systems owned by DHS Components. Therefore, redress of inaccurate or erroneous information is obtained through the originating owner of the data. When performing RDT&E activities, ORA is not using personally identifiable information for operational purposes and thus, does not depend on the accuracy of the data regarding an individual. If ORA uses personally identifiable information to make recommendations on operational decisions, these are not related to a benefit or service but the general management of resources. If a Component decides to use ORA's data for an operational purpose, the Component is responsible for verifying the accuracy of S&T data..

Section 8.0 Auditing and Accountability

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

All data within ORA-managed systems is audited while it is maintained within the system, regardless of the environment. Actions against data, including events, such as data loading, editing, and access by applications or users, is logged and timestamped. All system logs are maintained on a dedicated host within Cloud Factory, and access to the logging host is restricted only to authorized DHS log administrators. Deletion documentation is provided to the end user once the pilot/test is completed to ensure the data has been purged appropriately. Users are required to follow system-specific rules of behavior and their DHS Component's information use policies. The cloud provider does not have any access or rights to the data stored in the SoSOA environment. The data is encrypted and role-based access controls are used to ensure the data is accessible only to authorized DHS users. This is a setting required by S&T of cloud providers and cannot be turned

off. S&T uses the appropriate cloud-based computing environment (to include infrastructure, platform, security boundaries, applications, and services) to control the user community access. Only DHS authorized users with a need-to-know will be permitted access to the SoSOA environment.

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

All DHS personnel, including users and system administrators of ORA systems, are required to complete annual privacy training. Data-specific training will be required by DHS Components as necessary (e.g., Cybersecurity and Infrastructure Security Agency (CISA) Protected Critical Infrastructure (PCII) training will be provided to any user accessing that data).

All users sign DHS Rules of Behavior and agree to the system's Terms of Service that spell out the general guidelines of all systems involved before access into the system is granted. Depending on the project involved, additional training and guidance may be provided, prior to, and while engaged with, the project.

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

ORA-managed systems can only be accessed via government-furnished equipment (GFE). A user must be an active DHS employee and a valid Personal Identity Verification card and must complete a system-specific user account request and rules of behavior form.

Access to ORA-managed systems like SoSOA are granted through an account Request form that is processed and approved by project owners and system administrators.

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?

ORA establishes documented agreements with any partners or data providers, such as Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), or Cooperative Research and Development Agreements (CRADA), that set the terms and conditions that govern data access, use, sharing, and deletion. Final agreements must be reviewed and approved by the respective legal and privacy oversight authorities of the parties, prior to execution.

ORA privacy risk analysis also addresses proposed information sharing for specific initiatives. A DHS adjudicated Privacy Threshold Analysis is required before any data is transferred, stored, or made available for access by ORA personnel. The Privacy Threshold

Analysis will discuss the personally identifiable information and personally identifiable information sources, how ORA will use the personally identifiable information, how ORA shares and disposes of the personally identifiable information, and other personally identifiable information-related matters. Once the project Privacy Threshold Analysis is approved, personally identifiable information may be uploaded and stored within ORA-managed systems in connection with the specific ORA RDT&E activity.

Privacy Risk: There is a risk that improper configuration of the cloud computing environment would expose data to all cloud environment users with access as opposed to authorized users only.

Mitigation: This risk is mitigated. ORA-managed systems such as SoSOA leverage system assessments, independent control assessments, and continuous monitoring in the same manner as all DHS IT systems. Compliance and vulnerability scans of the system are conducted at least on a weekly basis. The cloud provider does not have any access or rights to the data stored in the SoSOA environment, and the data is both encrypted and accessible only DHS authorized users determined by role-based controls. This is a S&T required setting for cloud providers that cannot be turned off. S&T uses the appropriate cloud-based computing environment (to include infrastructure, platform, security boundaries, applications, and services) to control the user community access. Only DHS authorized users with a need-to-know will be permitted access to the SoSOA environment.

Contact Officials

Lorraine Castillo
Office of Systems Engineering
Operations and Requirements Analysis
Science and Technology Directorate
(202) 254-5317

Maria Petrakis
Privacy Officer
Science and Technology Directorate
stprivacy@hq.dhs.gov

Responsible Official

Daniel Cotter
Director, Office of Science and Engineering
Science and Technology Directorate

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security

(202) 343-1717

Appendix
Operations and Requirements Analysis Division
Project and Activities

International Cooperative Administrative Support Services (ICASS)

ORA will provide SoSOA's data analytics and visualization capabilities to the DHS Office of International Affairs (OIA) to identify and resolve unexpected cost increases using annual invoice data concerning all DHS personnel based at international DHS locations. This information is available to the DHS Office of International Affairs via the Department of State International Cooperative Administrative Support Services (ICASS) system, and the sharing of information is pursuant to a memorandum of understanding. The DHS Office of International Affairs user will have access to financial information, such as post location, fiscal year, cost center (procurement, performance, or management of good or services), total costs by position and incumbent, and time breakdown by position and incumbent. DHS Office of International Affairs will pull data from the Department of State International Cooperative Administrative Support Services, including personally identifiable information about all DHS personnel overseas. Specific data elements include:

- Employee First Name; and
- Employee Last Name.

Data will be downloaded from ICASS by OIA users and uploaded to SoSOA in a comma-separated values format using the SoSOA Ingest Application. Data will be loaded twice per year: the first upload will include the projected data for the year; and the second upload will include the final data for the year.

Individuals seeking to correct inaccurate or erroneous information, contained in this dataset, should follow the procedures of Department of State.

Appendix (continued)
Operations and Requirements Analysis Division
Projects and Activities

ORA will use SoSOA to provide data modeling and analysis support to DHS Headquarters for data related to evacuated foreign nationals. The information used for this analysis is available in DHS sources in aggregated format. Data sources are performing aggregation of the data prior to uploading into SoSOA.

Once the aggregated data is available in SoSOA, ORA analysts will use different tools and services to create interactive data visualizations, known as dashboards, to be responsive to operational decisions related to the individuals described above. However, ORA does not require and will not use any data containing personal information, including personally identifiable information, to provide this support. Instead, ORA will only use aggregate information provided to ORA for specific tasks to assist with policy and operational needs when requested. ORA will not engage in any form of data sharing related to individuals or privacy sensitive technologies.

ORA will not make any recommendations on any specific determinations or decisions about individuals. For example, ORA will not perform analysis to assess whether individuals are associated with a particular activity. Instead, ORA will provide recommendations such as the number of DHS personnel required to capture and process fingerprints, or the number of fingerprint capture devices DHS staff may need.