Privacy Impact Assessment

for the

Data Analytics Cloud System

DHS Reference No. DHS/OIG/PIA-003

September 28, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) is responsible for conducting and supervising independent and objective audits, inspections, and investigations of Department of Homeland Security's programs and operations. The Office of Inspector General's Office of the Chief Data Officer (OCDO) established the Data Analytics Cloud System (DACS) to ingest, store, manage, and analyze information necessary for these audits, inspections, and investigations, as well as information necessary to improve Office of Inspector General's operational effectiveness and efficiency. The Office of the Chief Data Officer acquires, integrates, and analyzes large volumes of data from Department of Homeland Security systems, other government agencies, public sources, and vendors that frequently include personally identifiable information (PII) and sensitive PII (SPII).

Overview

Under the Inspector General Act of 1978,[1] as amended, the Office of Inspector General is responsible for conducting and supervising independent and objective audits, inspections, and investigations of Department of Homeland Security's programs and operations. In order to fulfill these responsibilities, Department of Homeland Security components, among other sources, promptly provide data and access to auditors, inspectors, and other personnel authorized by the Office of Inspector General, to include any files, records, reports, and other information as requested.[2] The Department of Homeland Security's Office of Inspector General has used personally identifiable information and sensitive personally identifiable information data from Department of Homeland Security systems for audit, inspection, and investigative purposes since its formation in 2003. As Department of Homeland Security systems have grown in number, size, and complexity, the Office of Inspector General's technical capability has needed to scale accordingly to oversee these systems effectively and efficiently. The Data Analytics Cloud System provides an advanced data analytics platform and secure, governed data repository platform leveraged by analysts, auditors, inspectors, and investigators to promote economy, efficiency, and effectiveness, and prevent or detect fraud in programs, initiatives, and services offered and/or sponsored by Department of Homeland Security components. Results from analytical products may lead to or support audit or inspection recommendations, management advisories, administrative sanctions, fines, civil monetary penalties, or criminal prosecutions. The Data Analytics Cloud System comprises specialized software tools and services that provide the following data analysis, architecture, and engineering capabilities:

[1] 5 U.S.C. § 2.
[2] For more information on DHS OIG, *see* Department of Homeland Security Management Directive System, MD Number 0810.1 (June 10, 2004), *available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf.

- Data Integration;
- Data Warehousing;
- Business Intelligence;
- Graph and Network Analysis;
- Geospatial Analytics;
- Visual Analytics;
- Natural Language Processing and Semantic Text Analysis; and
- Machine Learning.

Datasets coming into the Data Analytics Cloud System from U.S. Department of Homeland Security systems are typically collections of flat files exported from the respective component's system and provided to the Office of Inspector General by the component using Department of Homeland Security-approved secure transfer methods; however, the datasets may also be provided in the form of database backup files or direct connections from the Data Analytics Cloud System to a component's database. Data from other government agencies, public sources, and vendors are typically acquired from Secure File Transfer Protocol (SFTP) sites, Application Programming Interfaces (API), or other Department of Homeland Security-approved secure transfer methods. Flat files that are not downloaded from an outside source directly into the Data Analytics Cloud System are staged on a file server in Office of Inspector General's Homeland Security Inspector General Network (HSIGN) and moved securely into the Data Analytics Cloud System. Once in the Data Analytics Cloud System, datasets are loaded into relational or non-relational data repositories which can then be accessed by authorized Office of Inspector General staff and contractors for ad-hoc queries, visual analytics and data analysis, business intelligence, and machine learning in support of Office of Inspector General's mission.

Only authorized Office of Inspector General users with a validated need-to-know are provided access to the front end/user facing portion of the Data Analytics Cloud System. Access is explicitly granted by application administrators. System maintenance is only performed by system administrators who have been vetted and approved via the Office of Inspector General's Office of the Chief Information Officer (OCIO) Privileged Access Request process. The information stored within the Data Analytics Cloud System may be shared with U.S. Department of Homeland Security components, U.S law enforcement agencies, other Office of Inspector Generals, and Congress as required.

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?

The Inspector General Act of 1978 and The Homeland Security Act of 2002[3] permit the Office of Inspector General to collect information necessary for the Office of Inspector General to perform audits, inspections, investigations, and legal analysis on programs and operations within the Department of Homeland Security. Department of Homeland Security Management Directive System MD Number 0810.1[4] states the roles and responsibilities of the Heads of U.S. Department of Homeland Security Organizational Elements (OE), Department of Homeland Security employees, and the Office of Inspector General in collecting any files, records, reports, or other information that may be requested either orally or in writing.

A significant portion of the information that the Office of Inspector General receives and stores within the Data Analytics Cloud System is obtained from Department of Homeland Security components. Because of the unique authority of the Office of Inspector General to oversee virtually any program or portion of the Department of Homeland Security, nearly all information at each component potentially could be required for an Office of Inspector General purpose.

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

The majority of the information that the Data Analytics Cloud System uses is collected by source systems performing the original collection, and thus covered by the individual System of Records Notices for those systems. Department of Homeland Security component data remains covered by these source system, System of Records Notices until it is processed or incorporated into an Office of Inspector General audit, inspection, or investigation reporting.

The DHS/OIG-002 Investigative Records System of Records Notice[5] covers the information and records the Office of Inspector General processes during its audits, inspections, and investigations and incorporates into its reports. This System of Records Notice also covers the collection of information from other government agencies, commercial sources, and publicly available sources.

---

[3] 6 U.S.C. § 101.
[4] Department of Homeland Security Management Directive System, MD Number 0810.1 (June 10, 2004), https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf.
[5] *See* DHS/OIG-002 Investigative Records System of Records, 80 Fed. Reg. 44372 (July 27, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns. The Office of Inspector General is currently updating this System of Records Notice to provide greater transparency for its collections.

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

The Data Analytics Cloud System is a Minor Application within the Office of Inspector General's Cloud Operations Resource Environment (CORE) boundary in Microsoft's FedRAMP High certified Azure Government cloud environment. The Office of Inspector General's Cloud Operations Resource Environment obtained an Authority to Operate (ATO) on October 1, 2018.

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

Retention of records stored in the Data Analytics Cloud System is governed by existing Office of Inspector General records retention schedules approved by the National Archives and Records Administration (NARA). The Data Analytics Cloud System records related to the Office of Investigations are governed by N1-563-08-4[6] and N1-563-07-5.[7] Records related to employee performance fall under records retention schedule N1-GRS-95-3, item 23a4.[8] In addition, the Office of Inspector General retention schedule N1-563-09-10[9] applies to any other Office of Inspector General related items pertaining to Reports, Work Papers, Correspondence, and Other 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.

The information collected as part of the Data Analytics Cloud System is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

Data collected and aggregated by the Data Analytics Cloud System is obtained from a wide

[6] *See* DHS OIG NARA Retention Schedule #N1-563-08-4, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-08-004_sf115.pdf.
[7] *See* DHS OIG NARA Retention Schedule #N1-563-07-5, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-07-005_sf115.pdf.
[8] *See* DHS OIG NARA Retention Schedule #N1-GRS-95-3 item 23a4 for work performance history records https://www.archives.gov/files/records-mgmt/memos/grs-2-2-initial-review-package.pdf.
[9] *See* DHS OIG NARA Retention Schedule #N1-563-09-10, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-09-010_sf115.pdf.

range of sources which includes any system relevant to the subject matter of the Office of Inspector General audit, inspection, and/or investigation. This can include information on members of the public, Department of Homeland Security employees and contractors from components, as well as information from other government agencies and systems, publicly available sources, and third-party data aggregators. The list below provides examples of the types of information that the Data Analytics Cloud System may use:

- Name;
- Date of birth;
- Social Security number;
- Telephone and cell phone numbers;
- Physical and mailing addresses;
- Email addresses;
- Physical description;
- Citizenship;
- Biometrics;
- Financial institution information;
- Benefits received;
- Assets;
- Photographs;
- Education;
- Medical Information;
- Travel Information including Passport information;
- Criminal History;
- Work Experience;
- Relatives;
- Business and personal contacts;
- Office of Inspector General's employee information; and
- Any other information relevant to the subject matter of an Office of Inspector General audit, inspection, or investigation.

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

The Data Analytics Cloud System collects, aggregates, and stores data obtained from a wide range of sources. The majority of collected information comes from records maintained by Department of Homeland Security components. Information stored and processed by the Data Analytics Cloud System can also be obtained from other government agencies; government contractors and vendors; commercial sources, including third-party data aggregation firms; and publicly available sources, which may include public websites, news sources, open social media sites, and public geospatial data. For example, to support an audit or investigation related to disaster relief grants, analysts and investigators may leverage the Data Analytics Cloud System to collect and analyze information originally collected by Federal Emergency Management Agency (FEMA) systems, transaction information from financial institutions, and public records obtained from commercial sources.

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

External commercial data or publicly obtained data will be used as appropriate for comparative analysis to assist with audit, inspection, investigation, and other reviews. This includes sources such as third-party data aggregators, publicly available social media sites, and open source media (e.g., newspaper articles, news websites, maps).

2.4 Discuss how accuracy of the data is ensured.

Data Analytics Cloud System is purpose-built as a data aggregator — collecting data from existing sources versus being a primary data collector/entry application. Accuracy of information is principally the responsibility of the underlying source system. However, the Office of Inspector General conducts an initial analysis of data ingested into the Data Analytics Cloud System to ensure completeness, accuracy, and reliability for audit, inspection, and/or investigation purposes. Data collected for audits and/or inspections are subject to project-specific reliability assessments as part of established audit and inspection processes and procedures. Data completeness, accuracy, and reliability assessments may include steps like analyzing and comparing record counts of flat file extracts obtained from components to both the expected record counts and the data loaded into the Data Analytics Cloud System from the extracts. It also includes comparing data obtained from the system to reports or analysis provided separately by the component, and verifying data displayed in a corresponding front end user interface to the respective back-end database tables. Individuals, agencies, and/or components impacted by an audit and/or inspection will be given an opportunity to correct erroneous information. Data collected for an investigation will be verified

for accuracy as part of the investigation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of overcollection given the breadth of sources the Office of Inspector General receives data from.

Mitigation: This risk is partially mitigated. The Office of Inspector General limits the data collected for analysis by scoping its information requests to only that data which is necessary for the Office of Inspector General to conduct its audit, inspection, and investigation responsibilities. As part of its audit, inspection, and investigation processes, the Office of Inspector General conducts a planning and survey period to determine what information is appropriate to receive. This is important not only in protecting against over-collection, but also ensures that Office of Inspector General personnel only use the information that is necessary for them to conduct their responsibilities in accordance with Government Auditing Standards.[10]

The initial scope of information will be defined according to audits, inspections, and/or investigations that are planned by the Office of Inspector General. This scope may expand depending on findings or in the case of an audit/inspection transitioning into a formal investigation.

Privacy Risk: There is a risk of inaccurate data given Data Analytics Cloud System uses source system data from other sources.

Mitigation: This risk is partially mitigated. Primarily, accuracy is the responsibility of the source system as the Data Analytics Cloud System does not collect information directly. However, the Office of Inspector General has multiple steps in place to ensure accuracy of the information used. The Office of Inspector General conducts initial analysis of data ingested into the Data Analytics Cloud System to ensure completeness, accuracy, and reliability for its audit, inspection, and investigation responsibilities. During the planning and survey period, the Office of Inspector General personnel and Component personnel engage in technical discussions to ensure data transfer is secure and compatible.

Data collected for audits and/or inspections are subject to project-specific reliability assessments as part of established audit and inspection processes and procedures, such as comparing data obtained from the system to reports or analysis provided separately by the component. Data collected for an investigation is verified for accuracy as part of the investigation process. The Office of Inspector General uses the totality of the information available to it during its investigations which ensures that inaccurate data would not alone impact any actions taken by

[10] *See* Government Auditing Standards: 2018 Revision Technical Update (April 2021), *available at* https://www.gao.gov/products/gao-21-368g.

the Office of Inspector General.

Further quality assurance processes are in place, including vetting of sources and review of outputs (e.g., Work Papers derived from analysis conducted via the Data Analytics Cloud System). Additionally, all audit and inspection reports are subjected to review prior to publication.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The Data Analytics Cloud System collects information from source systems to support the Department of Homeland Security Office of Inspector General's oversight of the Department's programs and systems and promote effectiveness and efficiency. The Office of Inspector General regularly collects data from the Department of Homeland Security systems, other government sources, and commercial or publicly available data during the course of audits, inspections, and investigations. The Data Analytics Cloud System serves as the central repository for these large and/or complex datasets that require specialized applications to ingest, assess, manage, and analyze.

The Data Analytics Cloud System produces analytical outputs that are then used by Office of Inspector General personnel in the course of their audits, inspections, and investigations. For example, Office of Inspector General personnel may be working to understand the disbursement of funds for a Department of Homeland Security assistance program. The Data Analytics Cloud System can run analysis on the data to determine if funds were provided inappropriately (e.g., to entities outside a disaster area). Office of Inspector General personnel use these analytical outputs to develop work papers during their audits, inspections, and investigations, and eventually incorporate them into formal reporting.

Data in the Data Analytics Cloud System is subject to the same processes, procedures, standards, and security requirements as data stored and analyzed by auditors, inspectors, investigators, and analysts outside of the Data Analytics Cloud System.[11, 12, 13]

[11] *See* Government Auditing Standards: 2018 Revision Technical Update (April 2021), *available at* https://www.gao.gov/products/gao-21-368g.
[12] *See* Quality Standards for Inspection and Evaluation (December 2020), *available at* https://www.ignet.gov/sites/default/files/files/QualityStandardsforInspectionandEvaluation-2020.pdf.
[13] *See* Quality Standards for Investigations (November 2011), *available at* https://www.ignet.gov/sites/default/files/files/invprg1211appi.pdf.

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.

The Data Analytics Cloud System leverages technology to conduct electronic searches, queries, and analysis to discover existing patterns or anomalies. However, there are currently no plans to use the system for predictive analysis. The Data Analytics Cloud System is designed to ingest historical data from a variety of disparate sources for processing and analysis; such results are then used to identify, investigate, and verify fraud, misconduct, criminal activity, misuse, or waste of government to support financial and performance audits of the Department's components, and increase the efficiency and effectiveness of internal Office of Inspector General operations.

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

Only the Department of Homeland Security's Office of Inspector General personnel have direct access to the Data Analytics Cloud System — both at the user and system administrator level. Only authorized Office of Inspector General members are allowed access to the data stored within the Data Analytics Cloud System. Requests for data processed by the Data Analytics Cloud System must be formally requested through established channels. Requestors may include Department of Homeland Security components and Office of Inspector Generals from other government agencies. Only designated Office of Inspector General members have the authority to approve transfers of data from the Data Analytics Cloud System.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of improper use of the Data Analytics Cloud System data given the breadth of information maintained.

Mitigation: This risk is mitigated. Only authorized users are granted access to the Data Analytics Cloud System, and only authorized Privileged Users have access to the system and application administrator functions comprising the Data Analytics Cloud System. Furthermore, only Privileged Users specifically designated as database administrators have administrator access to the databases within the Data Analytics Cloud System boundary. All Privileged Users must successfully complete the Privileged Access Request process prior to being granted access.

Access to the user-facing portion of the Data Analytics Cloud System is strictly controlled by Site Administrators who verify the need to know for authorized Office of Inspector General members and provide access permissions at a granular level. All Office of Inspector General users are required to complete Cybersecurity Awareness Training and Privacy Training on an annual

basis, which includes a module on user responsibility for protecting personally identifiable information and sensitive personally identifiable information. In addition, all Office of Inspector General users must acknowledge and sign the Office of Inspector General Rules of Behavior that also covers user responsibilities for protecting sensitive information.

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.

The Department of Homeland Security provides notice to the public through this Privacy Impact Assessment and the Office of Inspector General System of Records Notice. However, due to the fact the information ingested into the Data Analytics Cloud System is collected from source systems, the Office of Inspector General is unable to provide specific notice to individuals. The Office of Inspector General relies on the notice provisions and requirements of the agency responsible for originally collecting the information. The applicable Privacy Impact Assessments and System of Records Notices for the source systems provide notice of the collection of the information. More specifically, Department of Homeland Security's System of Records Notices provide notice of sharing of source system data through the following routine use: "Disclosures may be made to: …an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function." Further, because the Data Analytics Cloud System maintains potentially sensitive information related to audits and investigations, it is not always feasible or advisable to provide notice to individuals at the time their information is collected.

For information collected from commercial and publicly available sources, this Privacy Impact Assessment serves as the primary form of notice to individuals. The Office of Inspector General does not, however, individually provide notice when collecting publicly available information, for example, that is voluntarily posted on publicly accessible platforms.

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

The Data Analytics Cloud System is designed to be leveraged as a data analytics system in support of audits and investigations involving programs provided and/or administered by Department of Homeland Security components. Therefore, it is often not possible/feasible for an individual to be given the opportunity to decline/opt out – particularly in the case of a criminal investigation.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that information collected by another Department of Homeland Security component, or other source, is collected and maintained in the Data Analytics Cloud System.

Mitigation: The risk is partially mitigated. This Privacy Impact Assessment and the very nature of Office of Inspector General's responsibilities (outlined in publicly available information about the Office of Inspector General[14]), provide notice of the Data Analytics Cloud System and the collection of this type of information. Additionally, source system collections require notice provisions such as Privacy Act Statements and Privacy Notices, as applicable, when collecting information. However, because the Office of Inspector General relies on these notice provisions by the source systems, individuals may not know that their information is shared with and maintained in the Data Analytics Cloud System.

Section 5.0 Data Retention by the Project

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

Retention of records within the Data Analytics Cloud System are governed by existing Office of Inspector General records retention schedules N1-563-07-5, N1-563-08-4, and N1-563-09-10. Specific retention requirements will depend on whether the record is related to an audit, inspection, or investigations case.

Records Schedule N1-563-07-5

The National Archives and Records Administration -approved records schedule N1-563-07-05 continues to apply to Office of Inspector General investigative records. Complaint and investigative record files that involve substantive information relating to national security or allegations against senior Department of Homeland Security officials, that attract national media or congressional attention, or that result in substantive changes in the Department's policies or procedures are permanent records and are transferred to National Archives and Records Administration 20 years after completion of the investigation and all actions based thereon. All other complaint and investigative record files are destroyed 20 years after completion of the investigation and all actions based thereon. Government issued accountable property records, training and firearms qualification records, and management reports are destroyed when no longer needed for business purposes.

Records Schedule N1-563-08-4

The National Archives and Records Administration -approved records schedule NI-563-

[14] *See* https://www.oig.dhs.gov/.

08-4 covers investigations that may be undertaken for any Department of Homeland Security employee or contractor who is suspected of criminal activity including known or alleged fraud and abuse, and irregularities and violations of laws and regulations. Other investigations included within NI-563-08-4 are background investigations conducted on employee and contractor personnel for security and/or suitability purposes, criminal and non-criminal intelligence investigations of persons, groups or organizations that involve, or could involve, the use of threats, force or violence, and security investigations involving alleged crimes against the Department of Homeland Security or its employees. Documents contained in the investigative files may include, but are not limited to, investigative reports and related documents, such as correspondence, notes, attachments and working papers, also included may be statements by suspects, personal history summaries on suspects, photos, court documents and newspaper clippings.

It is the responsibility of Department of Homeland Security personnel to dispose of duplicate records and other non-records materials that do not have lasting administrative or legal value. Any evidence and other materials retained at the close of a case will be considered part of the case file. All retention provisions in the schedule apply to both the case file and any retained evidence or other related case materials If the investigation is program specific and has a current records disposition schedule (e.g., Office of Inspector General, Office for Civil Rights and Civil Liberties (CRCL)), the document will be filed and retained according to the program records disposition schedule.

Counterintelligence Case Files Disposition: Documentation of activities designed to identify and prevent potential threats within all Department of Homeland Security components. These files may also contain executive summaries written by division personnel used to brief the Secretary and Executive Secretariat. In addition, other Federal agencies may send copies of counterintelligence reports for reference to current Department of Homeland Security cases or the case file may contain "derivative memos" that describe a threat assessment compiled by outside sources. Temporary — cutoff is at the end of the fiscal year when the case is closed. These files are destroyed 20 years after cutoff.

Criminal Investigation Case Files: Case files developed during investigations of known or alleged fraud and abuse, and irregularities and violations of laws and regulations. The case files are related to Department of Homeland Security personnel and programs administered or financed by the Department of Homeland Security, including contractors and others having a relationship with the Department. Temporary — cutoff is at end of the fiscal year, in which the case is closed. These files are destroyed 20 years after cutoff.

Non-Referral Files: Files containing information or allegations which are of an investigative nature, but do not relate to a specific investigation. These include anonymous vague allegations not warranting an investigation, matters referred to constituents or other agencies for handling, and support files providing general information which may prove useful in

investigations. Temporary — these files are destroyed when they are 5 years old.

Records Schedule N1-563-09-10

The National Archives and Records Administration -approved records retention schedule N1-563-09-10 covers records related to Office of Inspector General Audit and Inspection reports, supporting documentation and Work Papers, Office of Inspector General correspondence, policy and procedural guidance, and other records maintained by various Office of Inspector General components. Excluded are Office of Inspector General Investigative case files and the Enforcement Data System, which are covered under N1-563-07-5.

Performance Audit and Inspection Reports may include external peer review reports, which the Office of Inspector General issues regarding other federal Offices of Inspector General. The records include both classified and unclassified versions of reports. Permanent — cutoff is at end of fiscal year in which the report is issued and transferred to National Archives 5 years after cutoff.

Financial Reports, Attestation Engagements, and Advisory Reports includes financial statement audit reports and financial assistance (grants) reports. Temporary — cutoff is at end of fiscal year in which the report is formally closed (i.e., after final resolution and implementation of all findings and recommendations). These records are destroyed or deleted 15 years after cutoff.

Supporting Documentation and Workpapers Documentation of audit and inspections work performed to support report findings, conclusions and recommendations, include pre-audit or inspection findings, planning materials, internal and external report correspondence, draft reports and Department of Homeland Security management's response, and final reports. These records are created and maintained in either paper form or electronically. Temporary — cutoff is at end of fiscal year in which the report is formally closed (i.e. after final resolution and implementation of all findings and recommendations). These records are destroyed or deleted 15 years after cutoff.

The Office of Counsel retention policy is determined based on whether a case is tied to an investigation, audit, or inspection and would follow both the N1-563-07-5 and N1-563-08-4 National Archives and Records Administration documents. If a case is not related, then the records will follow the National Archives' General Records Schedule N1-563-09-10.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that records will be retained longer than necessary due to the vast amount of electronic records with various retention schedules.

Mitigation: This risk is mitigated. In order to mitigate this risk a data governance council comprised of representatives from Data Analytics Cloud System's Offices of Innovation, Audits, Inspections and Evaluations, Investigations, and Management meets periodically to review records stored in the Data Analytics Cloud System. During these reviews, the council will (1) determine active data sets to be removed from active use and backed up to virtual cold storage for temporary

retention, and (2) review data sets in virtual cold storage and flag them as appropriate for permanent destruction, transfer to the National Archives, or other action, as required to meet the requirements of the approved records retention schedules.

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.

The Office of Inspector General shares information within the Department of Homeland Security, and with other U.S. law enforcement agencies other federal agencies, and Congress. As a part of normal agency operations, information may be requested through authorized points of contact from the Office of Inspector General of the Chief Data Officer or the Office of General Counsel. The investigations, inspections, and audit reports are then provided to the Department's components, law enforcement, and Congress on an as-needed basis. The Office of Inspector General may share information outside of the Department of Homeland Security consistent with Section (b)(3) routine uses published in the Office of Inspector General System of Record Notice, when other law enforcement agencies (such as state or local law enforcement)[15] or other federal agencies request it, or if necessary to protect the safety of an individual.[16]

The following are examples of U.S. law enforcement agencies in which the Office of Inspector General would provide a report to: Sheriff's offices or the FBI in the context of criminal investigations.

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

Consistent with the Investigative Records System of Records Notice, the Data Analytics Cloud System will provide information within the Department, and with U.S. law enforcement agencies and Congress. As an example, the information shared is done so in accordance with the following routine uses:

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which

[15] 5 U.S.C. 552a(b)(7).
[16] 5 U.S.C. 552a(b)(8).

includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. To a federal, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive when the security of the borders which the Department of Homeland Security is tasked with maintaining are at risk of being compromised.

L. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

6.3 Does the project place limitations on re-dissemination?

The Office of Inspector General places limitation on the re-dissemination of information derived from the Data Analytics Cloud System at the time of sharing, specific to that data. The Office of Inspector General is permitted to share information processed by the Data Analytics Cloud System to other Office of Inspector Generals as per the Inspector General Empowerment Act.[17] In addition, other Department of Homeland Security components can also make a formal request for data processed by the Data Analytics Cloud System. All requests must be received, vetted, and approved by authorized staff from the Office of Inspector General's Office of the Chief Data Officer and the Office of General Counsel. Upon release of Office of Inspector General's information, the requesting agency is notified of the purpose in which they are receiving the information and are advised that the information shall not be disclosed and/or re-disseminated further without authorization from Office of Inspector General. Further, any data shared containing personally identifiable information and/or sensitive personally identifiable information is properly identified and redacted where necessary prior to disclosure or release of information.

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

OIG will maintain all appropriate data use agreements, memoranda of understanding, or similar documents for disclosures of information to account for any data shared outside the Department. These documents will outline the legal authority for the disclosure; the purpose of the disclosure; and responsibilities of the party receiving the disclosed information. The documents will also outline retention procedures for timely destruction of identifiable records, and security procedures for the disclosed information.

Also, the Office of Inspector General program offices requesting information from the Data

[17] Pub. L. 114-317.

Analytics Cloud System maintain records of any disclosure outside of the Department. The documentation process may be by paper or electronic recording consisting of the date, nature, and purpose of each disclosure. Additional information will include the name and contact information of the individual or agency to whom the disclosure was provided.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk data from the Data Analytics Cloud System could be improperly shared.

Mitigation: This risk is mitigated. Only authorized Office of Inspector General personnel have access to data maintained by the Data Analytics Cloud System and only authorized Office of Inspector General members from the Office of the Chief Information Officer have system administrator access to the Data Analytics Cloud System systems. All Office of Inspector General personnel are required to complete training regarding the safe handling of personally identifiable information and sensitive personally identifiable information and the Office of Inspector General has implemented protocols to address privacy incidents, such as in case of an inadvertent release of sensitive information.

Although the Office of Inspector General can only account for how information is safeguarded and disclosed while in its possession, all requests must be approved prior to disclosure and any data shared containing personally identifiable information or sensitive personally identifiable information is properly identified and redacted where necessary.

Section 7.0 Redress

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

Individuals may request access to information collected by the Data Analytics Cloud System through the Freedom of Information Act (FOIA)[18] and provisions of the Privacy Act of 1974 at https://www.oig.dhs.gov/foia. Request can also be made by email, telephone, or mail:

OIG Office of Counsel
Phone: 202-254-4001
Fax: 202-254-4398
Email: FOIA.OIG@OIG.DHS.GOV

Mailing Address:
245 Murray Lane SW
Mail Stop - 0305

[18] 5 U.S.C. § 552.

Washington, D.C. 20528-0305
DHS OIG FOIA Request Form[19]

The Office of Inspector General only maintains ownership of its own data. Therefore, the Office of Inspector General will refer FOIA and Privacy Act requestors seeking non- Office of Inspector General data to the appropriate Department of Homeland Security component(s). Individuals who would like to make a FOIA request outside of Office of Inspector General should contact the particular corresponding component.

All requests must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information.[20] Individuals must verify their identity by providing their full legal name, current address and data and place of birth. All requests must be signed and notarized or submitted consistent with federal statute regarding Unsworn Declarations Under Penalty of Perjury.[21] If there is no specific form provided to the requestor, all statements must clearly state the following:

- Explanation on why the particular Department may utilize the information on you;
- List the component(s) who may use the information;
- Provide what types of records the component(s) have on the individual
- Provide detailed information that would assist the FOIA staff to research any records pertaining to the individual's request.

Individuals must understand that each case submitted will be evaluated by the Office of Inspector General on a case-by-case basis and must meet the requirements under FOIA[22] or the Privacy Act of 1974, as amended.

Individuals usually are not notified of investigations until the near end of an investigation. This is to make sure the individuals do not become prematurely aware they are subjects of an investigation. Notification comes in the form of Grand Jury target letters in certain cases and the individual is only aware when called in for an interview or when a warrant is executed. Therefore, redress ability is limited, and the individual subjects of an investigation would not know there are records to correct during an investigation.

[19] DHS OIG FOIA Request Form FOIA Request Form, *available at* https://www.oig.dhs.gov/sites/default/files/assets/PDFs/OIG_Cert_Ident_Form.pdf.
[20] 6 CFR Part 5.
[21] 28 U.S.C. § 1746 - a law that permits statements to be made under penalty of perjury as a substitute for notarization.
[22] Department of Homeland Security (DHS), Freedom of Information Act Regulations (FOIA), 80 Fed. Reg. 45101 (July 29, 2015).

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

The procedures for correcting inaccurate or erroneous information are referenced in Section 7.1 above. Individuals may not be able to access their records within the Data Analytics Cloud System because it may be part of a confidential criminal investigation. Releasing an individual's records may have an impeding effect on the investigation. In addition, Office of Inspector General obtained exemptions from its System of Records Notice based on the need to maintain the confidentiality of its investigations.[23]

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

This Privacy Impact Assessment and the Office of Inspector General System of Records Notice provides information to individuals on redress procedures. Source system Privacy Impact Assessments and the Office of Inspector General System of Records Notices also provide information to individuals if they wish to access or correct records maintained by Department of Homeland Security components or other government agencies.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know what procedures exist on collecting or correcting information.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment and the System of Records Notice provide information on the redress provisions available to individuals. However, because the Office of Inspector General System of Records Notice has been exempted from certain provisions of the Privacy Act through the issuance of its corresponding Final Rule, not all records may be accessed or amended.

Further, because much of the data the Data Analytics Cloud System maintains is originally from other source systems, the Office of Inspector General relies on the notice of redress provisions of those systems to provide sufficient information to individuals.

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?

Access to the Data Analytics Cloud System requires the use of two factor authentication and access is only provisioned to Office of Inspector General personnel with a need-to-know. User

[23] Final Rule for Privacy Act Exemptions, 75 Fed. Reg. 67909 (November 4, 2010).

accounts are configured using Role-Based Access Controls and Active Directory Group Policies for account auditing. The Data Analytics Cloud System itself can only be accessed using the Department of Homeland Security network with a Personal Identity Verification (PIV) card and PIN number to obtain access to the environment. Audit logs are configured to track any user login attempts, any modification made and by who, and the when the modification was made for systems within the system. User accounts will automatically disable accounts for users who have not been logged into the Data Analytics Cloud System within 45 days. The Office of Inspector General security team performs the following audit techniques within the Data Analytics Cloud System environment:

- Independent Verification and Validation (IV&V);
- Risk Assessments;
- Self-Assessments;
- Vulnerability Scanning;
- Third-party audits; and
- Audit reviews by General or Government Accountability Office (GAO).

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

Office of Inspector General employees are required to take annual security awareness training and role-based training (e.g., training for ISSOs, Authorizing Officials (AO), network and system administrators, and managers). All Office of Inspector General users are required to participate in mandatory annual privacy training. Furthermore, Office of Inspector General personnel responsible for conducting audits, inspections, and investigations are trained on the risks associated with improper use of information and the Office of Inspector General's responsibilities.

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

Data Analytics Cloud System user accounts are assigned based on discretionary Role-Base Access Controls, Active Directory Group Policies, and Access Control Lists in conjunction with device and application configuration baselines, which are used to automatically enforce logical access to applications, devices, and information. Supervisors and application administrators determine an individual's user account creation, termination, and level of access via user account and access action request forms, where they are reviewed for approval and ultimately approved or rejected.

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?

All project reviews, approved information sharing, Interconnection Systems Agreement, (ISA), Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), and other new uses of information within the Data Analytics Cloud System must comply with Department of Homeland Security Sensitive Systems Handbook and Policy Directive 4300A. All appropriate documentation and requirements must be approved by all authorizing officials of each system such as:

- System Owner (SO);
- Chief System Security Officer (CISO);
- Information System Security Manager (ISSM);
- Information System Security Officer (ISSO); and
- Program Manager (PM).

Contact Official

Bridget Glazier
Deputy Chief Information Officer
Office of Chief Information Officer/OIG
Bridget.Glazier@oig.dhs.gov

Responsible Official

Roy Jones
Chief, Information Law Division
Office of Counsel/OIG

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