Privacy Impact Assessment

for the

SURVEYOR Integrated Data Environment (IDE)

DHS Reference No. DHS/USCG/PIA-032

March 27, 2023

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), United States Coast Guard (USCG) is developing an Integrated Data Environment (IDE) system called SURVEYOR. This system will be the USCG's enterprise cloud-based data architecture to consolidate USCG data source silos, and enable the use of data as an enterprise strategic asset for data-informed execution of USCG business and mission operations. USCG is publishing this Privacy Impact Assessment (PIA) because SURVEYOR maintains data from systems and data sources that contain personally identifiable information (PII).

Overview

USCG is responsible for ensuring the Nation's maritime safety, security, and stewardship. USCG has 11 statutory missions codified in the Homeland Security Act of 2002.[1] These missions are: Ports, Waterways, and Coastal Security; Drug Interdiction; Migrant Interdiction; Defense Readiness; Law Enforcement; Marine Safety; Search and Rescue (SAR); Aids to Navigation; Living Marine Resources; Marine Environmental Protection; and Ice Operations. The purpose of SURVEYOR is to enable data transparency for the organization, integration of data and the reduction of information silos, and collaboration between data users; and to provide the capability for automation, auditing, publishing, and advanced analytics of USCG functions across all business and mission sets. SURVEYOR provides USCG leadership and personnel with mission critical capabilities that enable analysis and visualization of USCG data, data governance, and assistance with decision-making processes across the enterprise, as well as sharing of data with USCG mission partners. These partners include DHS components, the Department of Defense (DoD), domestic entities such as state and local law enforcement agencies, international entities such as maritime governing bodies, and industry mission partners such as those responsible for securing and operating the Maritime Transportation System.

SURVEYOR is a cloud-based architecture of technology components that provide data transparency, integration, visualization, and advanced analytic capabilities. SURVEYOR ingests and integrates raw data[2] from USCG source systems within all of USCG data domains (e.g., finance, personnel, operations, cyber), and from other DHS components, other government agencies (e.g., federal, state, local, tribal, and territorial government entities), DoD, industry, and academia for development of all-domain analytics to empower data-informed decision-making at

[1] 6 U.S.C. § 468(a).
[2] "Raw data" is data that has not been processed for use. In SURVEYOR, all incoming data from source system feeds or manually uploaded from files is considered raw data until it completes the ingestion process and becomes curated data.

all levels of the USCG. Curated data[3] in SURVEYOR may be shared with USCG mission partners for the execution of USCG statutory missions. Users of SURVEYOR will also have the ability to publish analytic products to USCG, other DHS components, DoD, and other mission partner applications as needed, after appropriate review. USCG analytic products are the result of analytic processes that combine disparate data to generate new insights (e.g., charts, maps, graphs, reports, dashboards, and other actionable insights).[4]

Technical Components

The SURVEYOR architecture includes multiple elements to enable the functions of the Integrated Data Environment:

- Data governance tools: Enable data governance, transparency, and stewardship through metadata management, data quality monitoring, and privacy compliance review and documentation across USCG data domains.
- Data platform: The foundation of the Integrated Data Environment which performs data ingestion, processing, integration, aggregation, and storage functions.
- Analytic tools: A suite of modern analytics tools and coding languages in a secure environment within the SURVEYOR system to perform advanced analytics and visualization development. In-platform analytic tools provide robust security and access control for analytics without risk of improperly or unintentionally altering source system data.
- Curated data views: Data visualizations generated from curated data, accessible based on need-to-know for job function and user roles. Curated data views are a type of analytic product.
- Interoperability: A standardized and streamlined mechanism to publish or share data with USCG mission partners to increase interoperability and mission success.

All elements are supported by technology components deployed within the USCG secure cloud computing architecture and use USCG network infrastructure to connect with data source systems for secure transfer of data into or out of SURVEYOR. User access to SURVEYOR is granted with a common access card (CAC) through the USCG network; SURVEYOR is not accessible from the public internet.

[3] "Curated data" is the organization and integration of data collected from various sources. Curated data in SURVEYOR is data that has completed the ingestion process and is tagged with required attributes including source system, retention schedule, sensitivity, and classification, and has a metadata record to support management and governance of the data. Curated data sets may be from a single source or multiple source systems.
[4] For more information *see* Data Visualization, Integration, and Analytics section on page 4 of this Privacy Impact Assessment.

User Groups

SURVEYOR users include USCG employees and specified USCG contractors. User access may be considered for non-USCG personnel on a case-by-case basis.

The vast majority of SURVEYOR users are Operational Users with 'view only' access to curated data views related to their official duties. Operational Users have only limited access to the underlying data. Curated data views are accessible to Operational Users based on the individual user's job functions and user roles within a user's command or program office. Access to personally identifiable information and other information about individuals is limited to only those Operational Users with a verified need-to-know the information to perform their official duties.

There is a small subset of Analytic Users in SURVEYOR who have access to both raw and curated data and analytic tools to perform advanced analytics in specific data domains. Analytic Users work with datasets within those data domains relevant to their job function, which may be a single data domain, or multiple data domains. Finally, there are a limited number of SURVEYOR Administrators who have access to the entire platform, including all data, to perform system management and auditing functions. Administrator use of the platform is monitored and is governed by strict business rules for appropriate use.

Data Integration, Visualization, and Analytics

The data integration and analytic tools in SURVEYOR provide capability for descriptive, predictive, and prescriptive analytics to improve operations and mission support for the USCG's 11 statutory mission areas. Data may be ingested through a direct connection with a source system, connection with an intermediate data distribution system or data warehouse, or in cases where a system connection has not been completed or is not possible, data may be manually uploaded.

Data integration and analytics in SURVEYOR are focused on three key areas:

- Organizational Readiness: Leaders and decision-makers at all levels of the USCG require visualization and analysis of workforce, asset, and mission readiness data, and other similar information. Data is primarily from USCG source systems in the personnel, logistics, and finance data domains, but may include data from other DHS components, other government agencies (e.g., federal, state, local, tribal, and territorial government entities), DoD, industry, and academia. Analyses may include workforce modeling and forecasting to inform recruiting and workforce management actions; predictive maintenance for cutters, boats, aircraft, and other critical assets; trend analysis, forecasting, and scenario-based evaluation of resource allocation, siting, and deployment for future mission demands; budget analysis and forecasting; program performance against service level standards; and similar advanced analytics to improve organizational readiness.
- Maritime Domain Awareness: Operational commanders at all levels of the USCG require

visualization and analysis of force laydown, potential threat, maritime activity, weather, and similar data, primarily from the operational and intelligence data domains, but also from other DHS components, other government agencies (e.g., federal, state, local, tribal, and territorial government entities), DoD, industry, and academia. Analyses may include pattern analysis, trend analysis, forecasting, and scenario-based risk assessment of port congestion; modeling and forecasting asset deployment and relocation in advance of forecast hurricanes or flood events; sensor data pattern analysis and object detection to provide greater surveillance capabilities; and similar advanced analytics to improve maritime domain awareness.

- Mission Execution: Operational commanders, mission support personnel, and program managers at all levels of the USCG require visualization and analysis of situation reports, after-action reports, post-mission records, and similar data, primarily from the operational data domain, but also from other DHS components, other government agencies (e.g., federal, state, local, tribal, and territorial government entities), DoD, industry, and academia. Analyses may include pattern analysis, trend analysis, forecasting, and scenario-based modelling of personnel and asset demand across the statutory mission areas; pattern, trend, and optimization analyses to respond to distress calls more quickly and accurately and increase efficiency in interdiction and enforcement activities; pattern analysis, trend analysis, link analysis, and predictive analytics of cybersecurity data to identify and manage cyber risks in the Maritime Transportation System; and similar advanced analytics to improve mission outcomes.

SURVEYOR Governance

The USCG has established a formal data analytics governance process to ensure that proposals for new curated data views, analytic products, and other analyses are reviewed prior to deployment in SURVEYOR to ensure compliance with USCG strategic priorities and legal, policy, privacy, and ethical requirements. The process includes identifying the analytic question or problem, identifying proposed datasets and their sources, reviewing the use of identified datasets for alignment with the above governance requirements, the source system's System of Records Notice (SORN) (including any future SURVEYOR System of Records Notice) and/or Privacy Impact Assessment, completing or updating any required privacy documentation (e.g., Privacy Threshold Analysis (PTA)), establishing a data sharing agreement with terms and conditions that govern data access, use, sharing, and data disposal with data owners as required, and determining the technical approach for data ingestion and integration.

Similar to the concept of DEVSECOPS (development, security, and operations), wherein security is considered through all phases of software development and operation, SURVEYOR development integrates both security and privacy in the development of analytics and operation of the system. The combination of attribute-based and role-based access controls allows more

controlled access to data and information than is possible in legacy systems.

Data integration and visualization across USCG data domains with data quality monitoring allow enhanced error detection to identify source system inaccuracies, which will be visible to domain data stewards, and which source system owners can correct. As part of the governance review process, the governance team will work to ensure that the quality of the data supporting the data view or analytic product is appropriate for the proposed use.

Data transparency and metadata management provide data owners and stewards greater visibility and control of access to and sharing of their domain data. In-platform analytics and visualization greatly reduce necessity of data downloads to import into other analytic or visualization tools.

Personally Identifiable Information

SURVEYOR ingests, integrates, and aggregates information about individuals from USCG source systems within all of USCG data domains (e.g., finance, personnel, operations, cyber) for development. SURVEYOR can also share curated data with USCG mission partners and publish analytic products to other USCG mission partner applications. The notice and purpose for the collection of this information by USCG is provided to the individual through initial collection by the source system, as applicable, and is documented in the respective Privacy Impact Assessment(s) and System of Records Notice(s) for those source systems. SURVEYOR does not collect information about an individual directly from an individual, except as required for user access to the system; therefore, USCG does not directly notify individuals of use of their data in SURVEYOR.

Access to information about individuals in SURVEYOR is limited to those SURVEYOR users with a verified need-to-know the information to perform their official duties. Data ingested into SURVEYOR is tagged with attributes that include data classification, data sensitivity (including personally identifiable information), source system, data retention, and data domain. SURVEYOR user access controls are based on both data attributes and user roles. This allows strict control over the visualization and use of all data, with access only to those users with a verified need-to-know. Information about individuals, including personally identifiable information, is only shared outside of DHS pursuant to "Routine Uses" in applicable System of Records Notices or through any applicable interconnection security agreement with DHS, DoD, and other government mission partners, or other information sharing agreement. Information about external sharing is discussed in Section 6.

As SURVEYOR ingests data from operational systems, analytic products may identify individuals of interest for enforcement actions (e.g., expired merchant mariner credentials, warrant for arrest). USCG may use this data operationally, as well as share the data with other DHS Components or government enforcement agencies as appropriate to fulfill USCG's 11 statutory

missions. USCG will not use this information as the sole determiner for an enforcement action against an individual. Instead, USGC personnel will use analytic products from SURVEYOR in conjunction with other relevant information when engaging in an enforcement action that may adversely impact an individual. Any required data checks, verification, or corroboration that must be used with SURVEYOR data will be determined during the USCG data analytics governance process prior to deployment.

The data ingested in SURVEYOR, including information about individuals, is retained in SURVEYOR for only as long as specified in the source system System of Records Notice. At the end of the retention period, SURVEYOR will flag the dataset for purging from SURVEYOR. Data will be purged either automatically within the system, or manually by system administrators depending on operational and technical requirements that will be determined within the governance process. Raw and curated data purged from SURVEYOR will no longer be reported or displayed in curated data views or recurring analytic products. When an analytical product is considered a new record, it will have its own retention schedule. Retention schedules will be determined during the data analytics governance process prior to deployment of an analytical product.

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?

Data in SURVEYOR is ingested or uploaded from other systems, and collection of personally identifiable information is handled by those source systems with legal authorities explained in their respective Privacy Impact Assessments and System of Records Notices. SURVEYOR only collects information directly from individuals that is necessary for user access, management, and monitoring for responsible use of the Integrated Data Environment.

Data ingested into SURVEYOR from source systems is authorized, in part, pursuant to the following:

5 United States Code (U.S.C.) § 301, 5501-5597; 10 U.S.C. §§ 503, 1043, 1147; 10 U.S.C. Subtitle A, Part II, Chapter 55, Medical and Dental Care, as applicable; 14 U.S.C. §§ 1, 2, 81, 88, 89, 91, 92(I), 92®, 93, 94, 102, 141, 143, 350-373, 475, 504(a)(17), 512, 620, 632, 634, 645, 648, 681; 687, 936, 3705; 19 U.S.C. § 1401; 33 U.S.C. §§ 1221 et seq 1223, 1321; 37 U.S.C. § 406; 40 U.S.C. § 1315; 42 U.S.C. §§ 213, 253; 32 Code of Federal Regulations (CFR) Part 199; 42 CFR Parts 31–2 - 31.10; 49 CFR 1.45, 1.46; and COMDTINST M1100.2F, Coast Guard Recruiting Manual; 46 U.S.C. §§ 2306, 3306, 3717, 12501; 46 U.S.C. Subtitle VII, § 3306; 50 U.S.C. § 191; 33 U.S.C. § 1223; the Magnuson-Stevens Fisheries Conservation and Management Act, 16 U.S.C. § 1801; the Lacey Act, 16 U.S.C. §§ 3371-3378; the Endangered Species Act, 16 U.S.C. §§ 1531-

1544; the National Marine Sanctuaries Act, 16 U.S.C. §§ 1431-1445; The Espionage Act; The Ports and Waterways Safety Act (PWSA); and The Maritime Transportation Security Act of 2002 (MTSA), Pub L. 107-295.

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

SURVEYOR is a USCG enterprise Integrated Data Environment, a system that includes personally identifiable information sourced from various USCG systems or other U.S. Government systems, as authorized by their own System of Records Notice(s) and relevant Privacy Impact Assessment(s). As system development continues, and new source systems are onboarded and new purposes for such data are identified, the USCG and the DHS Privacy Office will continually assess whether a new SURVEYOR System of Records Notice is necessary to be published in the Federal Register. Further, as data connections are supported within the USCG enterprise with SURVEYOR, interfaces will be updated in Appendix A.

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

SURVEYOR received an Authority to Operate with Conditions (ATO-C) on March 3, 2022.

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

SURVEYOR follows National Archives and Records Administration (NARA) and DHS applicable record schedules. Since SURVEYOR is not the originator of the information, data ingested is retained in accordance with the data retention schedule established for the source systems.[5]

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.

SURVEYOR is not subject to Paperwork Reduction Act (PRA) requirements because information within SURVEYOR is collected from other data sources which provide the required notices, as applicable. Some source systems contain information subject to the Paperwork

[5] As USCG develops its own SURVEYOR System of Records Notice, USCG will also work with NARA to determine if a SURVERYOR-specific retention schedule is necessary and will update this Privacy Impact Assessment as appropriate.

Reduction Act and state the OMB control number in their respective Privacy Impact Assessments and on any relevant collection forms.

Section 2.0 Characterization of the Information

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

Information SURVEYOR collects

SURVEYOR directly collects from individuals only information that is necessary for user access, management, and monitoring for responsible use of the Integrated Data Environment. This information is collected from SURVEYOR users, including USCG personnel (e.g., active duty, reserve, civilian), USCG contractors, and USCG Auxiliarists. Specific information collected may include, but is not limited to:

- Name;
- DoD ID Number (from CAC);
- Electronic Data Interchange Personal Identifier (EDIPI);
- Assigned Command and Command Address;
- Government Email Address and Phone Number;
- Employment Status (i.e., Military, Civilian, Contractor, Auxiliary);
- Supervisor Name, Government Email, and Government Phone Number;
- Community of Interest (for assigned work roles); and
- Data Domain (for Analytic Users).

Information SURVEYOR uses, disseminates, or maintains

SURVEYOR accesses certain information from a variety of data sources to enable users to visualize, analyze, and interpret existing data more effectively, without changing or impacting the integrity of the data in the original source system(s). Data about individuals in source systems may include data about USCG personnel (e.g., active duty, reserve, and civilian personnel) and contractors, as well as members of the public such as Auxiliary personnel, USCG family members, and others who interact with the USCG.

Data types originating from USCG systems or programs, DHS components, other government agencies (e.g., federal, state, local, tribal, and territorial government entities), industry, and academia that may be used in SURVEYOR or shared with DHS, DoD, and other government partners includes, but is not limited to:

- Full Name;
- Home Street Address;
- Home Phone Number;
- Business Street Address;
- Business Phone Number;
- Email Address;
- Employer Identification Number (EMPLID);
- 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; and
- Video and Audio (e.g., sensor data).

Other information used in SURVEYOR may include:

- Protected critical infrastructure information;
- Law Enforcement Sensitive data (e.g., data from the Marine Information for Safety and Law Enforcement (MISLE) system[6]); and
- Information derived from publicly available information or from federal, state, local, tribal, and territorial government entities.

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. COAST GUARD, PRIVACY IMPACT ASSESSMENT FOR THE MARINE INFORMATION FOR SAFETY AND LAW ENFORCEMENT (MISLE), DHS/USCG/PIA-008 (2009), *available at* https://www.dhs.gov/privacy-documents-us-coast-guard.

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

SURVEYOR only accepts information about individuals from USCG and U.S. Government source systems where data is collected in accordance with a respective System of Records Notice and/or Privacy Impact Assessment. Data is transmitted to SURVEYOR via a direct connection with those systems, a connection with the Enterprise Service Bus (ESB) and similar USCG data distribution services, a connection with the Coast Guard Business Intelligence (CGBI) Enterprise Data Warehouse,[7] or, for cloud-based systems, a connection with an authorized secure cloud access point. In circumstances when a direct connection has not been completed or is not possible, information may be manually uploaded.

SURVEYOR may accept enrichment data from state, local, tribal, and territorial government entities, industry, or academia, which may be connected through an application programming interface (API) or manually uploaded.

2.3 As data connections are supported within the USCG enterprise with SURVEYOR, interfaces will be updated in Appendix A. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

SURVEYOR does not use information about individuals obtained from commercial sources or publicly available data. SURVEYOR may accept other publicly available enrichment data from state, local, tribal, and territorial government entities, industry, or academia, such as relevant information from academic researchers about arctic weather conditions. Further, SURVEYOR may ingest various commercial datasets to add relevant business, operational, or mission information data layers. Examples of those datasets include, but are not limited to, imagery, remotely sensed weather and environmental data, or Automatic Identification Systems (AIS) data, that do not include information about individuals.[8]

2.4 Discuss how accuracy of the data is ensured.

The data quality and accuracy of the information in SURVEYOR is dependent on the quality and accuracy of data within the source systems. For example, if a record within a source system is either updated or deleted, that change will be reflected in SURVEYOR after that system's

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. COAST GUARD, PRIVACY IMPACT ASSESSMENT FOR COAST GUARD BUSINESS INTELLIGENCE (CGBI), DHS/USCG/PIA-018 (2012), *available at* https://www.dhs.gov/privacy-documents-us-coast-guard.

[8] Automatic Identification System (AIS) vessel tracking data feeds include vessels' GPS coordinates, Maritime Mobile Service Identity (MMSI) numbers, vessel names, destinations, and cargo types.

next data refresh with SURVEYOR. SURVEYOR does not alter or transform data in the source systems. Data refresh rates are determined by the data quality requirements of the curated data view or analytic product and the technical constraints of the source systems, which are assessed through the data analytics governance process before the visualization or product is deployed. Dimensions of data quality such as accuracy, timeliness, completeness, consistency, uniqueness, and validity are monitored through a combination of automated and manual quality checks. As noted previously, data quality monitoring allows enhanced error detection to identify source system inaccuracies, which will be visible to domain data stewards, and which source system owners can correct. As part of the governance review process, the governance team will work to ensure that the quality of the data supporting the data view or analytic product is appropriate for the proposed use.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information will be included in SURVEYOR that is not necessary or relevant to accomplish the USCG purpose to inform data-driven execution of USCG business and mission operations.

Mitigation: This risk is mitigated. In addition to legal, policy, privacy, and ethical review, the data analytics governance process ensures that only those data sources that are necessary to inform business and mission operations are ingested, and only those curated data views and analytic products that serve the same purpose are published or deployed. If the data analytics governance process determines that a prospective data view, analytic product, or other analysis is a new use of information about an individual not covered in the System of Records Notice and/or Privacy Impact Assessment for the respective source system(s) that collected the information, then the appropriate privacy compliance documentation (e.g., Privacy Threshold Analysis, Privacy Impact Assessment, and/or System of Records Notice) will be completed.

Privacy Risk: There is a risk that corrections made to personally identifiable information in the underlining source systems will not be reflected in SURVEYOR, thus leading to inaccurate or out-of-date information being stored, shared, or used.

Mitigation: This risk is partially mitigated. The data quality requirements of the curated data view or analytic product are assessed through the data analytics governance process before the data view or product is deployed. Data refresh rates are determined by the data analytics governance process, that incorporates the technical constraints of the source systems. The data analytics governance process will also determine if any additional safeguards may be necessary for new uses of data that may impact an individual, including the need for users to corroborate or validate any information found in SURVEYOR prior to final adverse USCG action. Finally, dimensions of data quality such as accuracy, timeliness, completeness, consistency, uniqueness,

and validity will be monitored through a combination of automated and manual quality checks within SURVEYOR by designated data stewards.

Privacy Risk: There is a risk that data analysts working in SURVEYOR will combine data elements from more than one source system to create a more sensitive data set.

Mitigation: This risk is partially mitigated. While the risk remains that a data analyst could combine data elements to create a more sensitive data set, all SURVEYOR users are required to complete annually and prior to being granted access to the system, at a minimum, USCG Federal Cyber Awareness Training and DHS Protected Personal Information Training. These trainings instruct attendees how to determine the sensitivity of different data. This includes what makes personally identifiable information datasets sensitive. These trainings focus on limiting access of sensitive data sets to those with a verified need to know. Additionally, prior to any new uses of data, any potential risks of combining disparate datasets would be analyzed during the data analytics governance process, and dissemination controls could then be deployed. Analysts would also then be instructed on proper handling procedures for such datasets to ensure proper use and dissemination. Finally, data ingested into SURVEYOR is tagged with an attribute for the source data domain, and SURVEYOR user access control is based on both data attributes and user roles. This allows strict control over the visualization and use of data, with access to information about individuals granted only to those with a verified need-to-know, even when combined with other datasets.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

SURVEYOR enables authorized users to access data from multiple source systems to develop and automate descriptive, predictive, and prescriptive analytics to inform decision-making at all levels of the USCG. Analytic products from each of the key areas of Organizational Readiness, Maritime Domain Awareness, and Mission Execution will inform actions to advance USCG strategic priorities and execute mission and business operations across the 11 statutory missions. SURVEYOR's data integration allows analytic results from one key area to inform further analysis and actions in the other key areas. For example, results of a scenario-based forecast model for future search and rescue mission demand in a particular region in Mission Execution would integrate with an analysis of resource allocation, siting, and deployment in Organizational Readiness.

Analytic products in SURVEYOR may be used for workforce management in the aggregate, such as identifying future skills sets required to meet emerging missions, mapping current workforce competencies to future mission requirements, and identifying groups of members with competencies and skills required to meet short-term mission deployments for

incident response.

Prospective data views, analytic products, and other analyses are reviewed through the data analytics governance process prior to onboarding in SURVEYOR to ensure compliance with USCG strategic priorities and legal, policy, privacy, and ethical requirements.

Curated data views and analytics products will typically be aggregated so as not to be linked or linkable to an individual, but those SURVEYOR users with a verified need-to-know will have access to person-level information, to include personally identifiable information. While SURVEYOR does not itself collect social security numbers, full or partial social security numbers may be embedded in source system data and ingested into SURVEYOR, with collection covered under the source system System of Records Notice and/or Privacy Impact Assessment. The data analytics governance process will limit incoming social security numbers to the maximum extent possible, engineer data tables with other identifiers when possible, and remove social security numbers from the system when identified as unnecessary and exclusion is possible. Social Security numbers will not be viewable to users without a need-to-know and unless specifically required for their official duties.

As SURVEYOR ingests more data from operational systems within USCG, SURVEYOR analytical products may identify individuals of interest for enforcement actions (e.g., expired merchant mariner credentials, warrant for arrest). USCG may use this data operationally, as well as share the data with other DHS components or government enforcement agencies as appropriate to fulfill USCG's 11 statutory missions. This operational use provides USCG personnel notice of potential violations that may lead to actions that impact individuals (e.g., notification of expired merchant mariner credential or expired vessel registration/documentation prior to a USCG law enforcement boarding activity). The data analytics governance process will assess whether current operational processes are sufficient to ensure personnel verify or corroborate information derived from SURVEYOR prior to USCG taking an adverse action against an individual (e.g., a USCG Boarding Officer may examine merchant mariner documents or vessel registration/documentation during a law enforcement boarding before a violation is issued) and enable redress for individuals to dispute potential adverse actions taken against them by USCG (e.g., an individual may challenge civil penalties through appeals processes).Any additional required data checks, verification, or corroboration that must be used in conjunction with a SURVEYOR analytical product will be determined during the USCG data analytics governance process prior to deployment.[9]

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

[9] As SURVEYOR development continues, USCG will collaborate with the DHS Privacy Office to determine if and when this Privacy Impact Assessment should be updated.

use such results.

SURVEYOR will have the ability to conduct queries of multiple databases to discover predictive patterns and connections between entities and events. SURVEYOR tools will assist users in recognizing relationships between disparate or previously un-synthesizable data. SURVEYOR users will use this ability across the USCG mission space for purposes such as predicting maintenance requirements, ensuring personnel at USCG stations are meeting mandatory qualification criteria, or making operational decisions for patrols and searches. SURVEYOR analytics may identify individuals of interest for enforcement actions (e.g., expired merchant mariner credentials, warrant for arrest) based on integration of data from source systems. This information will not be the sole determiner of taking adverse action against an individual, but may be used in conjunction with other information to determine whether to take an adverse action against an individual.

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

No other DHS components have assigned roles and responsibilities within the system. Additionally, information resulting from SURVEYOR data integration and analytics may be shared with other DHS components, DoD, and other government partners as appropriate.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that data originally collected for specific purposes is used for other purposes.

Mitigation: This risk is mitigated. The data analytics governance process includes legal, policy, privacy, and ethical review before new data sources may be ingested into SURVEYOR, and before data views or analytic products are published or deployed in the SURVEYOR production environment. Accordingly, SURVEYOR only uses data for the original purposes for which it was collected by the source system.

Privacy Risk: There is a risk that USCG will use inaccurate or out of date data when making operational decisions that may adversely affect individuals.

Mitigation: This risk is partially mitigated. Source system data stewards will be responsible for monitoring their data for quality and timeliness, and identifying data that should be deleted (based on retention periods or other reasons) or data that should be updated. Those changes will then be reflected in SURVEYOR during the next data refresh. In addition, SURVEYOR governance tools will enable data stewards to catalogue, check, and evaluate the data across source systems to further ensure data quality. The Integrated Data Environment allows USCG the opportunity to utilize overlapping datasets to validate and verify data quality. SURVEYOR's analytical products will allow users greater insights into data quality than separate

uses of disparate systems.

Dimensions of data quality such as accuracy, timeliness, completeness, consistency, uniqueness, and validity will be monitored throughout the data lifecycle by a combination of automated and manual quality checks within SURVEYOR by designated data stewards. If data stewards determine that the quality of data within SURVEYOR is insufficient for the business or mission need, they will initiate remedial or mitigating action (e.g., notifying source system owners of inaccurate data, reinitiating the data analytics governance process, updating information sharing agreements to implement more frequent refresh rates).

During the onboarding of a new dataset or analytical process in SURVEYOR, USCG will use the data analytics governance process to determine if its data use may impact an individual prior to deployment. The process will ensure that data refresh rates from source systems are aligned with the mission need. This may include, if necessary, implementing a data refresh as close to real time as possible. If technical or policy constraints prohibit adequate data updates within a dataset, then the governance process may require safeguards, such as placing warnings in the system reminding users of requirements to corroborate or validate any information found in SURVEYOR prior to final adverse USCG action.

Privacy Risk: There is a risk that a user will have access to information about individuals without a documented need-to-know.

Mitigation: This risk is mitigated. Data ingested into SURVEYOR is tagged with attributes that include data classification, data sensitivity, source system, and data domain. SURVEYOR user access control is based on both data attributes (attribute-based access control) and user roles (role-based access control). This allows strict control over the visualization and use of data, with access to information about individuals granted only to those with a verified need-to-know.

SURVEYOR user activity is logged, and audit mechanisms are in place to investigate any suspected inappropriate use or unauthorized access to data. SURVEYOR is also deployed within the USCG's secure cloud computing architecture, where USCG CYBER Command serves the role of cloud security service provider (CSSP) with responsibility for monitoring user activity.

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 only information that SURVEYOR collects directly from individuals is user account information. All other information is ingested from other source systems. SURVEYOR does not

provide notification to individuals whose data is collected by a source system that their information is now being used by SURVEYOR. However, general notice of the existence, contents, and uses of this system, and the source systems, is provided by the publication of this Privacy Impact Assessment and the associated Privacy Impact Assessments and System of Records Notices for the source systems. For source systems that collect information from government forms, Privacy Act Statements and privacy notices inform individuals about why the information is being collected and how that information may be shared.

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

The only information that SURVEYOR collects directly from individuals is user account information, which is mandatory for access control and system management. Individuals may refuse to have a user account, but in order to have access, they must consent to providing information to the system.

For the information in SURVEYOR, the agency, program, or source system(s) that originally collected the information from individuals may provide individuals with the opportunity to consent, decline to provide information, or opt out, in accordance with their own requirements. These programs, however, may not be able to provide an individual with the opportunity to consent or decline to the use of their information depending on the nature of those systems (e.g., law enforcement use).

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that SURVEYOR does not provide sufficient notice of collection of information.

Mitigation: This risk is partially mitigated. Notice is provided through the publication of this Privacy Impact Assessment and the source system Privacy Impact Assessments and/or System of Records Notices. If there is a form associated with the collection of information by the source systems, then notice of information collection is provided with the form. However, USCG does not provide notice to individuals that their information is maintained in SURVEYOR.

Privacy Risk: There is a privacy risk that individuals do not have the opportunity to consent to their information being used by SURVEYOR.

Mitigation: This risk is partially mitigated. The only information that SURVEYOR collects directly from individuals is user account information. For data ingested from source systems, USCG does not provide individuals the opportunity to consent to their information being used by SURVEYOR. However, USCG ensures that SURVEYOR's use of source system data is compatible with the purpose of its original collection. SURVEYOR also does not change or modify the underlying source system data, and traditional Privacy Act rights of correction and redress

remain for the source systems which will be reflected in SURVEYOR via data refreshes. It is incumbent on the source systems, to the extent permitted by law, to offer individuals the opportunity to consent to provide their information and provide notice, as appropriate, at the time of collection.

Section 5.0 Data Retention by the Project

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

Datasets ingested in SURVEYOR are governed and retained in accordance with the source system System of Records Notices and their own NARA-approved retention periods. Manual data uploads for specific analyses will only be retained until the end of the analytic activity.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that SURVEYOR will retain data for longer than is necessary or for a longer period than allowable under the source system's retention schedule.

Mitigation: This risk is partially mitigated. SURVEYOR datasets are refreshed and updated regularly from source systems. The retention period and timestamp are part of the metadata that is tagged to a dataset upon ingestion. At the end of the retention period for ingested data, or after the end of analytic activity for manually uploaded data, the system will flag the dataset for purging from SURVEYOR, which will be reviewed by a data steward to verify the data purge. Data purged from SURVEYOR will no longer be reported or displayed in data views or analytic products.

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.

All or a portion of the records or information may be disclosed to other USCG mission partners through authorized channels and liaisons to national and international governing bodies, agencies, and departments. Disclosure of information outside of DHS is only authorized when the receiving party has established a need-to-know that coincides with execution of USCG statutory missions and the original purpose for which the information was collected by the source system(s). All sharing will be documented as required by the Privacy Act of 1974, as amended. If a new SURVEYOR System of Records Notice is published, it will contain specific descriptions of normal agency operations, the purposes and uses for such operations, and identify reasons for the sharing of information and who may access it outside of DHS, as articulated in the routine uses.

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

the SORN noted in 1.2.

All sharing will be in accordance with applicable law, including the published "Routine Uses" in the source systems' associated System of Records Notices, as listed in Appendix A, which will be ensured through the data analytics governance review process.

6.3 Does the project place limitations on re-dissemination?

Data about individuals, including personally identifiable information, may only be disseminated in accordance with the specific limitations on re-dissemination as determined by the data analytics governance process. These limitations will necessarily be informed by the sensitivity and pre-existing limits placed on the data in source systems, as described in the relevant source system Privacy Impact Assessments and System of Records Notices. Users will be required to ensure such restrictions are honored prior to sharing with partners through a pre-existing information sharing agreement. Specific limitations on the re-dissemination are established on a case-by-case basis with each outside receiving entity. Information sharing agreements are governed by a need-to-know and mission requirements and are reviewed by the USCG Privacy Office.

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

All external sharing of personally identifiable information will be catalogued in accordance with the Privacy Act of 1974. Maintenance of such disclosures will be determined during the data analytics governance process. Ad-hoc requests for information will be documented manually either within SURVEYOR or by the user. SURVEYOR will also record the routine electronic transmission of records outside of DHS. All disclosures of records will be made in accordance with the appropriate source system Privacy Impact Assessment and System of Records Notice, and in accordance with any applicable Memorandum of Understanding (MOU), Information Sharing Agreement (ISA), or Memorandum of Agreement (MOA).

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of unauthorized re-dissemination or improper sharing of information from SURVEYOR.

Mitigation: This risk is mitigated. User access agreements require acknowledgement by users of restrictions on exporting from SURVEYOR data, data views, and analytic products, especially those that contain information about an individual. Proposals for disseminating SURVEYOR data views and analytic products are reviewed by the data analytics governance process before deployment for compliance with user access control and governing information sharing agreements. Data dissemination about individuals within DHS may only occur after the

data analytics governance process to ensure compliance with specific limitations on re-dissemination as described in the relevant source system Privacy Impact Assessments. For external sharing, information about individuals, including personally identifiable information, may be shared outside of DHS pursuant to "Routine Uses" in applicable source system System of Records Notices or through any applicable information sharing agreement following review through the data analytics governance process. Any external sharing will be documented as required by the Privacy Act of 1974.

Privacy Risk: There is a risk that data shared with other USCG mission partners may be used for a purpose other than that for which it was collected by the source system.

Mitigation: This risk is partially mitigated. The data analytics governance process reviews any proposed external sharing and specifies appropriate use and any further dissemination of the information in the approved information sharing agreement. However, the USCG does not have full visibility or control over other mission partners' use of the data short of the requirements agreed to in information sharing agreements.

Section 7.0 Redress

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

An individual may seek access to their records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens, lawful permanent residents, and covered citizens of designated foreign countries or regional economic organization under the Judicial Redress Act (JRA) are afforded access under the Privacy Act. Individuals not covered by the Privacy Act or Judicial Redress Act may still obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or FOIA request to view their record, they may submit requests electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form. Individuals may also submit requests to the USCG FOIA Officer by mail, facsimile, or email:

Commandant (CG-6P)
Attn: FOIA/PA Officer
U.S. Coast Guard
2703 Martin Luther King, Jr. Ave. SE STOP 7710
Washington, D.C. 20593-7710
Fax: (202) 372-8413
eFOIA@uscg.mil

To conform to the Privacy Act regulations set forth in 6 CFR Part 5, the individual must first verify their identity, including their full name, current address, and date and place of birth. The individual

must sign the request. The individual's signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. In addition, the individual should:

- explain why he or she believes the USCG would have the information being requested;
- specify when the individual believes the records would have been created; and
- if the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the USCG may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing an individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. However, USCG evaluates requests for access and redress on a case-by-case basis.

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

The correction procedure is the same as the procedure identified in Section 7.1 that allows individuals to access their information. U.S. citizens, lawful permanent residents, and covered persons from a covered country under the Judicial Redress Act are afforded amendment provisions, when applicable, through a Privacy Act request. While FOIA does not provide individuals with amendment provisions, USCG evaluates requests for redress on a case-by-case basis.

Depending on the source system, additional procedures that allow the subject individual to correct inaccurate or erroneous information may be provided, as described in applicable source system Privacy Impact Assessments and System of Records Notices.

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

This Privacy Impact Assessment, as well as the source systems' Privacy Impact Assessments, provide notice of the procedures for correcting information. USCG will review any information request on a case-by-case basis. Depending on the source system, notice may have been provided by applicable source system Privacy Impact Assessments and System of Records Notices. If the initial information collection occurred via a form, a Privacy Act Statement or privacy notice may have also provided notice.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to correct or access their information.

Mitigation: This risk is mitigated. Individuals may formally request to correct or access their information by making a Privacy Act or FOIA request, as identified in Sections 7.1 and 7.2. Depending on the source system, redress procedures may also have been provided through source Privacy Act Statements or applicable Privacy Impact Assessments and System of Records Notices.

Data within SURVEYOR may also be exempted from certain provisions of the Privacy Act regarding access and redress based on its source system System of Records Notice. Nonetheless, USCG will examine each separate request on a case-by-case basis, and may waive applicable exemptions in appropriate circumstances, or when it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.

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?

USCG has established a robust suite of controls, including data analytics governance controls and technical controls, for privacy assurance within SURVEYOR. Data analytics governance ensures that all proposed uses of data, publication of data views and analytic products, and potential sharing or dissemination of data or products are thoroughly reviewed for compliance with legal, policy, privacy, and ethical requirements. Technical controls provide for both attribute-based and role-based access control for data, data views, and analytic products, and for auditing user access and activities.

The Office of Privacy Management (CG-6P) will conduct a USCG Privacy Evaluation (CGPE) within one year of publication of this Privacy Impact Assessment. The Office of Privacy Management will share the results of the privacy evaluation with the DHS Privacy Office.

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

All SURVEYOR users are required to complete, at a minimum, USCG Federal Cyber Awareness Training and DHS Protected Personal Information Training, annually and prior to being granted access to the system. All SURVEYOR Administrators and those Operational Users and Analytic Users who may access Protected Health Information (PHI) are also required to complete Health Insurance Portability and Accountability Act (HIPAA) training. Analytic Users are also required to have earned the USCG Operations Research/Data Analytics special experience

indictor or demonstrated appropriate proficiency and experience in the responsible and ethical use of data. USCG tracks all privacy and security awareness training, special experience indicators, and other competencies to demonstrate compliance with training requirements.

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

User access is determined through the data analytics governance process and is limited to USCG employees and certain USCG contractors. User access may be considered for non-USCG personnel on a case-by-case basis.

The majority of SURVEYOR users are operational users with 'view only' access to curated data views related to their official duties. Operational users have only limited access to the underlying raw data. Curated data views are accessible to operational users based on job functions and user roles within a user's command or program office. Access to information about individuals is limited to those operational users with a verified need-to-know the information to perform their official duties. The user access process for operational users includes validation by a supervisor that the user has a need-to-know the information at that access level and has met the minimum training requirements.

There is a small subset of analytic users in SURVEYOR who have access to both raw and curated data and analytic tools to perform advanced analytics in specific data domains. Analytic users work with datasets within those data domains relevant to their job function, which may be a single data domain or multiple data domains. Supervisors must validate that analytic users have met minimum training requirements and, if accessing personally identifiable information, a need-to-know. The analytic user must then obtain approval from any domain data steward to use and view the requested data.

There are a limited number of SURVEYOR Administrators who have access to the entire platform to perform system management and auditing functions. User activity in SURVEYOR is logged, user accounts are disabled after a period of inactivity; and access privileges are adjusted due to a loss of a verified need to know the information or change in job requirements, depending on the user role and level of access.

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?

The data analytics governance process includes applicable legal, policy, privacy, and ethical review and approval of information sharing agreements, Memoranda of Understanding/Agreement, and SURVEYOR system connections at the appropriate level for the

proposed sharing/connection.

If the data analytics governance process determines that a prospective data view, analytic product, or other analysis is a new use of information about an individual not covered in the source system System of Records Notice and/or Privacy Impact Assessment, then the appropriate privacy compliance documentation (e.g., Privacy Threshold Analysis, Privacy Impact Assessment, and/or System of Records Notice) will be completed by USCG.

Any new user access is determined through the data analytics governance process and is limited to USCG employees and certain USCG contractors. User access may be considered for non-USCG personnel on a case-by-case basis.

Contact Official

CAPT Brian Erickson
Chief Data Officer
Coast Guard Office of Data & Analytics
United States Coast Guard
SMB-COMDT-ODA@uscg.mil

Responsible Official

Kathleen L. Claffie
Privacy and FOIA Officer
United States Coast Guard
Kathleen.L.Claffie@uscg.mil

Approval Signature

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

_____

Mason C. Clutter
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX A: SURVEYOR Source Systems

Updated March 27, 2023

Source System Name	Privacy Impact Assessment[i]	System of Records Notice[ii]
Homeport	DHS/USCG/PIA-001 Homeport Internet Portal, June 19, 2017	DHS/USCG-060 Homeport, 79 FR 74747, December 16, 2014
GANGWAY Recruiting System	Forthcoming GANGWAY Recruiting System PIA DHS/USCG/PIA-024 Direct Access, November 9, 2016	DHS/USCG-014 Military Pay and Personnel, 76 FR 66933, October 28, 2011 DHS/USCG-027 Recruiting Files, 76 FR 49494, August 10, 2011
USCG Biometrics at Sea	DHS/USCG/PIA-002 USCG "Biometrics at Sea," December 6, 2016	DHS/USCG-031 USCG Law Enforcement (ULE), 81 FR 88697, December 8, 2016
Electronic Health Care Acquisition (eHRA) - MHS Genesis	Forthcoming eHRA PIA	DHS/USCG-011 Military Personnel Health Records, 73 FR 77773, December 19, 2008
USCG Law Enforcement Information Data Base (LEIDB)/Pathfinder	DHS/USCG/PIA-004 USCG Law Enforcement Information Data Base (LEIDB)/Pathfinder, March 31, 2008	DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder, 73 FR 56930, September 30, 2008
Financial Systems Modernization Solution (FSMS)	DHS/ALL/PIA-053 DHS Financial Management Systems, July 30, 2015	GSA/GOVT-003 Travel Charge Card Program System of Records, 69 FR 4517, January 30, 2004 DHS/ALL-007 Department of Homeland Security Accounts Payable System of Records, 73 FR 61880, October 17, 2008 DHS/ALL-008 Department of Homeland Security Accounts Receivable System of Records, 73 FR 61885, October 17, 2008

		DHS/ALL-010 Department of Homeland Security Asset Management Records, 73 FR 63181, October 23, 2008 DHS/ALL-019 Department of Homeland Security Payroll, Personnel and Time and Attendance Records, 73 FR 63172, October 23, 2008
Maritime Analytic Support System (MASS)	DHS/USCG/PIA-005 Maritime Analytic Support System (MASS), April 24, 2020	DHS/USCG-061 Maritime Analytic Support System (MASS), 85 FR 74742, November 23, 2020
Medical Readiness Reporting System (MRRS)	Forthcoming eHRA PIA	DHS/USCG-011 Military Personnel Health Records, 73 FR 77773, December 19, 2008
Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System (AIS)	DHS/USCG/PIA-006(b) Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System (AIS), April 28, 2015	DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305, June 25, 2009 DHS/USCG-029 Notice of Arrival and Departure System of Records, 82 FR 32715, July 17, 2017 DHS/USCG-061 Maritime Analytic Support System (MASS), 85 FR 74742, November 23, 2020
Abstract of Operations – Training Management Tool (AOPS-TMT)	N/A	DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, November 27, 2012 DHS/ALL-010 Asset Management Records System of Records, 80 FR 58280, September 28, 2015

		DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 FR 11780, March 16, 2018
National Pollution Funds Center – Pollution Response funding, Liability, and Compensation System (NPFC/PRFLACS)	DHS/USCG/PIA-007 National Pollution Funds Center – Pollution Response funding, Liability, and Compensation System (NPFC/PRFLACS), June 17, 2009	DHS/ALL-007 Department of Homeland Security Accounts Payable System of Records, 73 FR 61880, October 17, 2008 DHS/ALL-008 Department of Homeland Security Accounts Receivable System of Records, 73 FR 61885, October 17, 2008 DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, November 27, 2012
Coast Guard Military Human Resource Record (CGMHRR)	DHS/USCG/PIA-024 Direct Access, November 9, 2016	DHS/USCG-014 Military Pay and Personnel, 76 FR 66933, October 28, 2011 DHS/USCG-008 Courts-Martial and Military Justice Case Files System of Records, 84 FR 20383, May 9, 2019 DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, November 27, 2012,
Marine Information for Safety and Law Enforcement (MISLE)	DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE), September 3, 2009	DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305, June 25, 2009
Electronic Resource Proposal (eRP)	N/A	DHS/ALL-004 General Information Technology Access Account Records

		System (GITAARS), 77 FR 70792, November 27, 2012
Core Accounting Suite	DHS/USCG/PIA-009 Core Accounting Suite, September 18, 2009	DHS/ALL-007 Department of Homeland Security Accounts Payable System, 83 FR 65705, December 21, 2018 DHS/ALL-008 Department of Homeland Security Accounts Receivable System, 83 FR 65176, December 19, 2018 DHS/ALL-010 Department of Homeland Security Asset Management Records, 80 FR 58280, September 28, 2015
USCG Ship Arrival Notification System (SANS)	DHS/USCG/PIA-006(b) Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System (AIS), April 28, 2015	DHS/USCG-029 Notice of Arrival and Departure System of Records, 82 FR 32715, July 17, 2017
USCG Satellite Automated Identification System (SAIS)	Not a privacy sensitive system	Not a privacy sensitive system
USCG Nationwide Automated Identification System (NAIS)	Not a privacy sensitive system	Not a privacy sensitive system
Long Range Identification Tracking system (LRIT)	Not a privacy sensitive system	Not a privacy sensitive system
Boating Accident Report Database (BARD)	DHS/USCG/PIA-011 Boating Accident Report Database (BARD), November 12, 2009	DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305, June 25, 2009 Forthcoming Non-Law Enforcement Records SORN
Recruit Analysis and Tracking System	DHS/USCG/PIA-012 Recruit Analysis and Tracking System, November 30, 2009	DHS/USCG-027 Recruiting Files, 76 FR 49494, August 10, 2011

Academy Information System	DHS/USCG/PIA-013 Academy Information System, January 26, 2010	DHS/USCG-014 Military Pay and Personnel System, 76 FR 66933, October 28, 2011
Security and Safety Computer Network	DHS/USCG/PIA-014 Security and Safety Computer Network, June 6, 2010	DHS/ALL-010 Department of Homeland Security Asset Management Records, 80 FR 58280, September 28, 2015 DHS/ALL-023 Department of Homeland Security Personnel Security Management, 85 FR 64511, October 13, 2020 DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609, February 3, 2010
Merchant Mariner Licensing and Documentation System (MMLDS)	DHS/USCG/PIA-015 Merchant Mariner Licensing and Documentation System (MMLDS), March 1, 2011	DHS/USCG-030 Merchant Seamen's Records, 74 FR 30308, June 25, 2009
College Board Recruitment Plus (CBRP)	DHS/USCG/PIA-016 College Board Recruitment Plus (CBRP), April 1, 2011	DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656, November 25, 2008 DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792, November 27, 2012 DHS/USCG-027 Recruiting Files, 76 FR 49494, August 10, 2011
Coast Guard Business Intelligence (CGBI) (including the Enterprise Data Warehouse (EDW)	DHS/USCG/PIA-018 Coast Guard Business Intelligence (CGBI), April 17, 2012	DHS/USCG-013 Marine Information for Safety and Law Enforcement, 74 FR 30305, June 25, 2009

		DHS/USCG-027 Recruiting Files, 76 FR 49494, August 10, 2011 DHS/USCG-029 Notice of Arrival and Departure System of Records, 82 FR 32715, July 17, 2017 DHS/USCG-030 Merchant Seaman's Records, 74 FR 30308, June 25, 2009 DHS/USCG-060 Homeport, 79 FR 74747, December 16, 2014 DHS/ALL-002 DHS Mailing and Other Lists, 73 FR 71659, November 25, 2008 DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records, 80 FR 58283, September 28, 2015
Transportation Worker Identification Credential (TWIC) Reader Requirements for USCG	DHS/USCG/PIA-019 Transportation Worker Identification Credential (TWIC) Reader Requirements for USCG, March 25, 2013	DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862, August 11, 2014
Interagency Operations Center (IOC) Watchkeeper	DHS/USCG/PIA-020 Interagency Operations Center (IOC) Watchkeeper, January 4, 2013	DHS/USCG-029 Notice of Arrival and Departure, System of Records, 82 FR 32715, July 17, 2017 DHS/CBP-006 Automated Targeting System, System of Records, 77 FR 30297, May 22, 2012
Rescue 21	DHS/USCG/PIA-021 Rescue 21, July 29, 2015	DHS/USCG-013 Marine Information for Safety and

		Law Enforcement (MISLE), 74 FR 30305, June 25, 2009
Coast Guard Maritime Information eXchange (CG-MIX)	DHS/USCG/PIA-022 Coast Guard Maritime Information eXchange, July 30, 2015	DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305, June 25, 2009
Incident Reporting Information System (IRIS)	DHS/USCG/PIA-023 Incident Reporting Information System (IRIS), April 20, 2018	DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305, June 25, 2009
Direct Access (DA)	DHS/USCG/PIA-024 Direct Access, November 9, 2016	DHS/USCG-014 Military Pay and Personnel, 76 FR 66933, October 28, 2011
Other HR Systems • FedHR • Monster • WebTA	DHS/USCG/PIA-024 Direct Access, November 9, 2016 DHS/ALL/PIA-043 Office of the Chief Human Capital Officer Talent Acquisition, September 11, 2020	DHS/USCG-014 Military Pay and Personnel, 76 FR 66933, October 28, 2011 OPM/GOVT-1 General Personnel Records, 77 FR 73694, December 11, 2012, as modified by 80 FR 74815, November 30, 2015,) OPM/GOVT-5 Recruiting, Examining, and Placement Records, 79 FR 16834, March 26, 2014, as modified by 80 FR 74815, November 30, 2015 OPM/GOVT-6 Personnel Research and Test Validation Records, 71 FR 35354, June 19, 2006, as modified by 80 FR 74815, November 30, 2015 OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records, 71 FR 35356, June 19, 2006, as modified by 80 FR 74815, November 30, 2015

		DHS/ALL-023 Department of Homeland Security Personnel Security Management, 85 FR 64511, October 13, 2020 DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records, 80 FR 58283, September 28, 2015
Asset Logistics Management Information System (ALMIS)	DHS/USCG/PIA-025 Asset Logistics Management Information System (ALMIS), January 29, 2018	DHS/ALL-004 General Information Technology Access Account Records, 77 FR 70792, November 27, 2012 DHS/USCG-032 Asset Logistics Management Information System (ALMIS) System of Records, 83 FR 19087, May 1, 2018
USCG Research and Development Center (RDC) Small Unmanned Aircraft Systems (sUAS) Program	DHS/USCG/PIA-026 USCG Research and Development Center (RDC) Small Unmanned Aircraft Systems (sUAS) Program, February 22, 2018	N/A
DHS/USCG/PIA-030 U.S. Coast Guard Counter-Unmanned Aircraft Systems Pilot	DHS/USCG/PIA-030 U.S. Coast Guard Counter-Unmanned Aircraft Systems Pilot, October 28, 2019	N/A

Sources of Enrichment Data	Privacy Impact Assessment	System of Records Notice
DoD Defense Repository Form Common Enterprise Data (DRCED known as Advanced Analytics (ADVANA)) • Jupiter (U.S. Navy) • Blade (U.S. Air Force (USAF) - Logistics)	DoD DRCED (ADVANA) PIA, May 27, 2020	DUSDC 01, Defense Repository for Common Enterprise Data (DRCED), 85 FR 15150, March 17, 2020[10]
Unified Data Library (UDL)		
Enterprise Logging Ingest & Cyber Situational Awareness (ELICSAR) - USAF		

[i] Privacy Impact Assessments are *available at* https://www.dhs.gov/privacy-impact-assessments.

[ii] System of Records Notices are *available at* https://www.dhs.gov/system-records-notices-sorns.

[10] *Available at* https://www.federalregister.gov/documents/2020/03/17/2020-05504/privacy-act-of-1974-system-of-records.