Privacy Impact Assessment
for the

Field Activity Case Tracking System (FACTS)

DHS/USCG/PIA-029

August 2, 2019

Contact Point
Stephanie E. McClellen
FACTS Program Manager
Coast Guard Investigative Service
United States Coast Guard
(202) 372-3042

Reviewing Official
James Holzer
Acting Deputy Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Coast Guard Investigative Service (CGIS) uses a web-based electronic case records management system (RMS) known as the Field Activity Case Tracking System (FACTS) to capture, relate, and analyze information about the professional investigative activities of CGIS special agents. By intra-Coast Guard program management agreement, FACTS also supports the collection and management of the Coast Guard's Anti-Harassment and Hate Incident (AHHI) records, a function overseen by its Civil Rights Directorate (CRD). CGIS is publishing this Privacy Impact Assessment (PIA) because FACTS collects personally identifiable information (PII) from DHS personnel, employees of other federal agencies, and members of the public.

Overview

The United States Coast Guard (USCG) developed the Field Activity Case Tracking System (FACTS) records management system (RMS) to support the United States Coast Guard Investigative Service's (CGIS) role as the criminal investigative arm of the service. As the primary maritime law enforcement agency, the USCG is charged with enforcing U.S. laws and regulations on the high seas and waters over which the United States has jurisdiction. CGIS maintains a cadre of trained and experienced special agents who conduct criminal investigations into actual, alleged, or suspected felony-level violations of federal law and the Uniform Code of Military Justice (UCMJ).[1] CGIS special agents provide criminal investigative support to Coast Guard operational commanders in fulfilling maritime law enforcement missions, supporting homeland and national security objectives, and maintaining good order and discipline within the USCG. In addition to CGIS, the Coast Guard's Civil Rights Directorate (CRD) maintains Anti-Harassment and Hate Incident (AHHI) records in FACTS.

FACTS incorporates information previously stored in paper-based, geographically-dispersed, and locally-stored databases into a centralized, electronic database which records all CGIS law enforcement actions and investigations, including activities supporting background investigations of CGIS applicants, internal affairs investigations and administration, and investigations resulting from complaints to the Department of Homeland Security (DHS) Office of Inspector General (OIG), when referred to CGIS. The amount and type of information collected depends on the particular allegation of criminal activity, and collection of an individual's data is only initiated upon approval of the appropriate Special Agent-in-Charge (SAC) for the region in which a special agent is operating. The FACTS database is searchable by name, case number, Social Security number, or keyword, and includes records that date back to 1970. It also contains information on CGIS's other law enforcement activities (*i.e.*, Title 18 criminal investigations[2]),

[1] 10 U.S.C. § 47.
[2] For example, CGIS frequently investigates allegations that a subject made false statements in an official proceeding, which is a violation of 18 U.S.C. § 1001.

pollution enforcement activities, and marine casualty investigations, as well as personal and vessel information relevant to CGIS investigative and administrative activities. FACTS also contains information pertaining to a special agent's training to assist in case management. The FACTS RMS is only accessible by authorized special agents, legal counsel, a Major Cases team at the Coast Guard Intelligence Coordination Center (ICC), and administrative support personnel at Coast Guard Headquarters. Access by personnel other than those previously mentioned is only provided with the express, written authorization of a SAC.

Additionally, CRD personnel may also access the FACTS RMS to manage AHHI records. In accordance with Notice 915.002 of the Equal Employment Opportunity Commission's (EEOC)[3] minimum standards and guidelines for agencies' anti-harassment policies, DHS Directive 256-01[4] delegates and requires agencies to track, report, and address harassment in the workplace. Information contained within the AHHI database meets this requirement and includes records that date back to 2010. The AHHI records are searchable and retrievable by the name of the individual who files a complaint or report of harassment, the name of the alleged victim of harassment, and the name of the alleged harasser. Within the FACTS RMS, CRD's AHHI information is logically separated from CGIS investigation records. Neither organization's users have any capability to view or access the other's information.

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 authority for the collection of investigative information is provided by 5 U.S.C. § 301; 14 U.S.C. §§ 2, 88-89, 93(e), 95, 141, 143, 632, and 634; 19 U.S.C. § 1401; 33 U.S.C. § 1221; and Commandant Instruction Manuals (COMDTINST) M5830.1 (Administrative Investigations Manual) and M5527.1 (series) (Coast Guard Investigations Manual). The listed statutory authorities range from the ability to prescribe regulations for the conduct of employees to the requirement for the Coast Guard to enforce or assist in enforcing all applicable federal laws on, under, and over the high seas and waters subject to U.S. jurisdiction. In carrying out its broad law enforcement authority, the Coast Guard is authorized to make inquiries, examinations, inspections, searches, seizures, and arrests as well as engage in investigations or studies that may be of assistance to the performance of any of the duties or powers delegated to the Commandant. CGIS special agents are granted federal law enforcement authority in 14 U.S.C. § 95.

The authority for the investigation and collection of harassment and hate information is

[3] EEOC Notice 915.002, https://www.eeoc.gov/policy/docs/waiver.html.
[4] DHS Directive 256-01, Anti-Harassment Directive (April 25, 2013), https://www.dhs.gov/sites/default/files/publications/DHS%20Anti-Harassment%20Directive%20and%20Policy%20-%20MD%20256-01%20-%204.25.13_2.pdf.

provided by 6 U.S.C. § 345; 5 U.S.C. § 301; 44 U.S.C. § 3101; Section 803 of Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53); Executive Order 12958, as amended; and COMDTINST M5350.4 (series) (Coast Guard Civil Right Manual).

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

Several DHS-wide SORNs apply to this system's collection of information:

- DHS/ALL-020 Department of Homeland Security Internal Affairs[5] covers the collection and maintenance of records relating to investigations, including allegations of misconduct, conducted by DHS headquarters or its components, including USCG.
- DHS/ALL-023 Personnel Security Management[6] covers the collection and maintenance of records related to the processing of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position.
- DHS/ALL-029 Civil Rights and Civil Liberties Records[7] allows the Department's civil rights and civil liberties staff to maintain records to investigate complaints including: allegations that individuals acted under color of law or otherwise abused their authority; discrimination; profiling; violations of the confidentiality provisions of the Violence Against Women Act; conditions of detention; treatment; due process; and watch list issues.
- DHS/ALL-038 Insider Threat Program System of Records[8] covers the collection of information related to security investigations to facilitate counterintelligence and counterespionage responsibilities.
- DHS/ALL-003 Department of Homeland Security General Training Records[9] covers the collection and documentation related to training given to DHS employees, contractors, and others who are provided DHS training.
- DHS/ALL-004 General Information Technology Access Account Records System of

[5] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014), *available at* https://www.dhs.gov/privacy.
[6] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010), available at https://www.dhs.gov/privacy.
[7] *See* DHS/ALL-029 Civil Rights and Civil Liberties Records, 75 FR 39266 (July 8, 2010), *available at* https://www.dhs.gov/privacy.
[8] *See* DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (February 26, 2016), *available at* https://www.dhs.gov/privacy.
[9] *See* DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008), *available at* https://www.dhs.gov/privacy.

Records[10] covers the collection of user information for the purposes of providing authorized individuals access to the system. This SORN also covers the collection, review, and maintenance of any logs, audits, or other such security data regarding the use of the system.

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

The FACTS database system architecture operates on the previously approved Maritime Awareness Global Network (MAGNET) information technology platform.[11] MAGNET is an operational major application in the Coast Guard/DHS intelligence systems inventory. The Authority to Operate (ATO) was granted on March 23, 2016.

Records in the FACTS database system are safeguarded in accordance with the same rules and policies that apply to MAGNET, including all applicable DHS automated systems security and access policies. These strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

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

No, a National Archives and Records Administration (NARA)-approved records retention schedule has not yet been finalized. CGIS is working closely with the USCG Records Management Office and NARA to schedule the various categories of records contained in FACTS. At this time, CGIS follows existing records retention schedules noted in the SORNs described in Section 1.2. Each category of records will have its own records retention schedule in the finalized FACTS retention schedule. These categories include:

- Official investigative reports prepared by CGIS, DHS, Department of Defense (DoD), or other federal, state, local, tribal, or foreign law enforcement or investigative records.
- Biographic data, intelligence/counterintelligence debriefing reports, information concerning U.S. personnel who are missing, captured, or detained by a hostile entity. This information may be of criminal, counterintelligence, or general investigative interest.
- Preliminary Investigation Reports (PIR) document receipt of information that, in the initial

[10] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 November 27, 2012), available at https://www.dhs.gov/privacy.
[11] For more information about MAGNET, please *see* DHS/USCG/PIA-005 USCG Maritime Awareness Global Network, *available at* https://www.dhs.gov/privacy, and DHS/USCG-061 Maritime Awareness Global Network, 73 FR 28143 (May 15, 2008).

stages, indicates an incident occurred involving one or more criminal offense(s). However it was subsequently determined that no criminal offense occurred or that the incident and offense(s) did not fall within CGIS jurisdiction and/or responsibility to investigate.

- Polygraph data, which includes a listing of persons who submitted to polygraph examination by CGIS polygraph examiners. The data includes the examinee's name, results of the examination, and the identity of the examiner. This includes copies of examination records created in support of criminal investigations.
- Case Control and Management documents, which serve as the basis for recording, conducting, controlling, and guiding the investigative activity. Records identifying confidential sources and contacts with them.
- Forensic Laboratory Report Records reporting and documenting laboratory analysis of submitted evidence.
- Fingerprint Card Files and related correspondence obtained by CGIS law enforcement officials and submitted to CGIS Headquarters for forwarding to the Federal Bureau of Investigations (FBI) in support of criminal investigations.
- Personnel Security and Suitability Investigations (or inquiries) conducted by the U.S. Coast Guard or other DHS, DoD, federal, state, or local investigative agency. Records include personal history statements; fingerprint cards; personnel security questionnaire; medical/educational records, and waivers for release; requests for and national agency checks; local agency checks; military records, birth records; employment records; credit records and waivers for release; interviews of education, employment, and credit references; interviews of listed and developed character references; interviews of neighbors; and similar records.

AHHI Records

- Civil Rights Service Provider (CRSP) interview information related to an alleged harassment or hate incident.
- Command-initiated Administrative Investigation reports, which include copies of final, Command-approved reports, including the findings and outcomes that are uploaded. Records do not contain biometric data and are retained per the Administrative Investigations Manual. Electronic versions of records may be deleted after the expiration of the retention period for the individual record type or when no longer needed, whichever is later.

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.

Information collected and maintained in the FACTS RMS is in support of criminal and other types of Coast Guard investigations. As such, the information contained is exempt from the requirements of the PRA.

Information collected and maintained in the AHHI database is gathered from in-person or telephonic interviews. FACTS does not collect or store standardized information directly from members of the public within the AHHI reporting process.

Section 2.0 Characterization of the Information

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

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

CGIS maintains information on victims of crime, witnesses, or subjects under investigation for violations of the laws and regulations enforced by the Coast Guard, as well as background investigations for individuals applying to be CGIS special agents. This can include Coast Guard military and civilian employees, merchant mariner personnel, and civilians. The information that may be collected and stored includes any combination of the following:

- Unique Case ID (system generated);
- Case Type;
- Names;
- Dates of birth;
- Home addresses;
- Phone numbers;
- Phone call records;
- Social Security numbers;
- Marital status;
- Military Branch, Rank, and status;

- Employee identification numbers;
- Demographic information (*e.g.*, race, ethnicity);
- Physical characteristics;
- Biometric fingerprint data;
- Forensic reports of investigation;[12]
- Email addresses;
- IP addresses;
- Certificate/license numbers;
- Driver's license, State ID, and passport information;
- Photographic images;
- Civil or criminal history information;
- FBI case number;
- Transportation Worker Identification Credential (TWIC) number;
- Medical record information;
- Training records;
- Vessel/vehicle identifiers (*e.g.*, Hull Identification Number, Vehicle license plate number);
- Job performance evaluations; and
- Financial information.

FACTS also maintains information relating to allegations of abuses of civil rights, civil liberties, and racial, ethnic, and religious profiling by Coast Guard employees, as well as similar allegations relating to persons or entities under Coast Guard control (*i.e.*, contractors or programs). Basic information about complainants stored in FACTS includes, but is not limited to:

- Full name;
- Home and work mailing address;
- Home, cell, and work telephone and fax numbers;

[12] Forensic reports of investigation include those related to, for example, the collection of DNA following an alleged assault or sexual assault.

- Home and work email addresses;
- Name of representative filing a claim on behalf of a complainant, if applicable;
- Allegation occurrence date and time;
- Allegation facility name and location;
- Coast Guard organization referenced;
- Information on a complainant's national origin/race/color/religion/sex/marital status/political affiliation/sexual orientation, if relevant to the allegation; and
- Allegation details, primary and secondary issues, and primary and secondary basis.

Other information relating to allegations of abuses of civil rights, civil liberties, and racial, ethnic, and religious profiling by Coast Guard employees that may be collected on a limited, as-needed basis might include:

- Photographic facial images;
- Letters, memoranda, and other documents alleging abuses of civil rights, civil liberties, and profiling from complainants;
- Internal letters, memoranda, and other communications within DHS;
- Results of an investigation of allegations;
- Transcripts, interview notes, investigative notes; documentation concerning requests for additional information needed to complete the investigation;
- Medical records;
- Evidentiary documents and material, comments, and reports relating to the alleged abuses and to the resolution of the complaint; and
- Similar information regarding witnesses, persons involved in the alleged incident, or any other persons with relevant information regarding the alleged abuses.

The CRD component of the FACTS RMS does not collect or store Social Security numbers or any biometric data.

Information needed to obtain a user account in FACTS includes:

- Full name;
- Date of birth;
- Place of birth;

- Employee Identification (*e.g.*, EMPLID, DoD ID number);
- Duty status (active/reserve/civilian);
- Employee type (*e.g.*, analyst, agent, admin);
- Classification: (*e.g.*, Director, Deputy Director (DD), Special Agent in Charge (SAC), Assistant Special Agent in Charge (ASAC), Agent, Analyst);
- National Crime Information Center (NCIC) training certification date;
- Government email address; and
- CGIS Credential Number (agents only).

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

CGIS special agents collect information from a variety of internal and external sources during the course of investigative activities. CGIS Criminal and Administrative Investigations can be initiated in the following ways:

1) Commands are required by Commandant Instruction to report actual or suspected criminal violations to CGIS for investigation;

2) CGIS Special Agents, upon receipt of information that alleges criminal activity, may initiate investigations to determine validity of the information; and

3) CGIS Regional Offices may proactively initiate investigations based on trends or crime analyses. CGIS also routinely receives case referrals and information from DHS OIG concerning complaints that it receives about Coast Guard-related activities.

Agent Interviews, Observations, and Surveillance Activities:

Information is routinely collected from in-person interviews with victims, witnesses, and suspects. Interviews are comprised mostly of verbal statements, but often include the collection of other types of information (*e.g.*, photos, papers, recordings) that are provided to the CGIS special agent directly from the individual being interviewed. CGIS special agents may also conduct overt or undercover surveillance in the performance of their duties. Observations made during these activities are documented in FACTS, and any still or video imagery collected is uploaded into FACTS. Information is also collected from the lawful electronic surveillance of phone and computer devices.

External Databases:

CGIS special agents are authorized to use information on a limited basis received from the

NCIC,[13] and to collect information from other federal agencies in accordance with applicable laws and policies. These agencies/systems include FBI NCIC/Nlets;[14] U.S. Navy Law Enforcement Data Exchange (D-DEx),[15] the DoD Defense Manpower Data Center (DMDC) Defense Enrollment Eligibility Reporting System (DEERS),[16] and the Department of Justice (DOJ) Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center.[17] CGIS special agents or support personnel manually enter information into FACTS; there is no automatic transfer of data from these external databases to FACTS. Additionally, CGIS special agents may also collect information from various state law enforcement databases when necessary to support investigative efforts. CGIS requests this information from other agencies pursuant to section (b)(7) of the Privacy Act, which allows for agencies to share information with U.S. law enforcement entities for law enforcement purposes.

Internal Databases:

CGIS special agents collect information from the U.S. Coast Guard's Direct Access (DA) employee database.[18] CGIS also obtains information from Coast Guard Business Intelligence (CGBI)[19] and Coast Guard Marine Information for Safety and Law Enforcement (MISLE).[20] CGIS special agents also collect information from U.S. Customs and Border Protection's (CBP) TECS (not an acronym) system,[21] and manually enters that information into FACTS. CGIS requests this information from its DHS partners pursuant to section (b)(1) of the Privacy Act, which allows for the agency to share information with its own employees who have a need to know the information in order to perform their official duties.

---

[13] The National Crime Information Center (NCIC) is an FBI-owned system that assists law enforcement in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists. Additional information on NCIC is available at https://www.fbi.gov/services/cjis/ncic.

[14] The National Law Enforcement Telecommunications System (Nlets) is the International Justice and Public Safety Information Sharing Network: a state-of-the-art secure information sharing system for state and local law enforcement agencies. It provides electronic messaging to allow information exchange between state, local, and federal agencies and support services to justice-related programs. The network is operated by Nlets, a non-profit corporation owned and operation by the states and funded solely by fees for service. See http://www.nlets.org/.

[15] The U.S. Navy Law Enforcement Data Exchange (D-DEx) is designed to enhance information sharing between local, state, and federal law enforcement in areas of strategic importance to the Department of the Navy. For more information, please *see* http://www.ncis.navy.mil/PI/LEIE/Pages/default.aspx.

[16] The Defense Enrollment Eligibility Reporting System (DEERS) is a computerized database for U.S. Service members, retirees, dependents, DoD-active contractors, and others worldwide who are entitled to Public Key Infrastructure and TRICARE eligibility. Please *see* the Privacy Impact Assessment, *available at* https://www.dmdc.osd.mil/appj/dwp/documents.jsp.

[17] *See* Addendum to Memorandum of Understanding Between US DOJ OCDETF Fusion Center and USCG dated September 6, 2018.

[18] *See* DHS/USCG/PIA-024 Direct Access, *available at* https://www.dhs.gov/privacy.

[19] *See* DHS/USCG/PIA-018 Coast Guard Business Intelligence (CGBI), *available at* https://www.dhs.gov/privacy.

[20] *See* DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE), *available at* https://www.dhs.gov/privacy.

[21] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* https://www.dhs.gov/privacy.

Civil Rights Division:

Civil Rights Service Providers (CRSP), who are Coast Guard personnel assigned to CRD, collect data from in-person or telephonic interviews with the reporting party and any witnesses. Interviews are comprised of verbal statements provided to the CRSP directly from the individual. CRSPs may also review and upload an Administrative Investigation conducted and provided by the Command where the alleged incident took place. CRSPs do not collect any biometric data, nor do they obtain or share any information from any external sources.

Social Media:

CGIS special agents may collect social media as part of criminal investigations and law enforcement intelligence operations in accordance with COMDTINST 5520.5 (series) and COMDTINST M5527.1 (series). CGIS special agents communicating online with witnesses, subjects, or victims must disclose their affiliation as USCG law enforcement when Coast Guard policy would require such disclosure if the communication were taking place in person or over the telephone. CGIS special agents may communicate online under a non-identifying name or fictitious identity if the Coast Guard would authorize such communications in the physical world. For purposes of CGIS undercover guidelines, each discrete conversation online constitutes a separate undercover activity or contact, but such a conversation may comprise more than one transmission between the special agent and another person (*e.g.*, online chat rooms). CGIS policy requires significant documentation, planning, review, and approval for undercover activities, pursuant to COMDTINST M5527.1 (series).

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

Yes. FACTS may include commercially available and public information that is relevant to a particular investigation. Some FACTS users access commercial or public sources, such as CLEAR, as part of their official duties, and may manually incorporate this information into reports or records within FACTS. However, FACTS does not give a user the capability to query these other sources of information directly. Incorporation of any commercial or public information is at the sole discretion of the individual user based on its relevance to the ongoing investigation and is not the result of an automated collection process. CGIS special agents routinely use data from commercial sources and publicly available data to both verify and enhance existing case information contained in FACTS.

CGIS special agents may also directly or indirectly (via a commercial data provider) access public information on the Internet, including social media websites, during investigations and incorporate that information into case documents. In the case of undercover operations, information

may be collected that is not publicly available but can only be viewed by those who have connected or "friended" the individual on social media sites, or who have otherwise been given special access to a restricted site. These instances are limited to agents who are engaged in authorized undercover operations during the course of a criminal investigation.

CRD does not use or import any commercial information sources or publicly available data into the AHHI component of FACTS.

2.4 Discuss how accuracy of the data is ensured.

CGIS special agents receive special training and qualifications to ensure that they input the data correctly into the system. They, along with the supervisors who review the investigative data, have primary responsibility for ensuring that it is accurate. Data used to draft a Report of Investigation (ROI), receives methodical law enforcement scrutiny, as well as a legal sufficiency review by an attorney, prior to any consideration for using the data and subsequent ROI in any adverse action against an individual. For example, CGIS special agents are required to undergo extensive FACTS RMS training to ensure data accuracy. They complete multiple biannual and annual records management and privacy awareness training modules for access to other databases as required by Department of Justice's (DOJ) Criminal Justice Information Services (CJIS) in addition to Coast Guard and DHS-mandated training requirements. Furthermore, the centralized FACTS database provides each CGIS special agent with the ability to compare data sets for related investigations and ensure that the most accurate information is available to all other special agents. This facilitates a more consistent, efficient, and effective investigative process. Cases involving the same person or organization with multiple violations can be combined, resulting in all information pertaining to a given subject being linked within FACTS for ease of access.

For CRD, CRSPs manually input data obtained during their investigations as well as input data from any Administrative Investigation provided by the unit Commander, if applicable. The CRSP, along with the supervisor who reviews the data, has primary responsibility for ensuring that it is accurate. CRSPs complete multiple biannual and annual records management and privacy awareness training modules per Coast Guard and DHS-mandated training requirements.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information in FACTS will not be accurate, complete, or timely.

Mitigation: This risk is partially mitigated. The immediate availability of new and updated records in FACTS for purposes of investigation deconfliction, ensures that all users have the most complete information available at any given time. FACTS users are instructed to verify their own data prior to input and to contact other users to resolve any discrepancies they identify when viewing

information already in the system. Users are trained to validate all commercial or publicly available data against authoritative sources, such as other federal records, before considering that information to be credible. Because some information includes statements made by individuals who have been interviewed by an agent, some content may be factually inaccurate. Special agent and supervisory review, as well as the legal sufficiency review if system data is used for any adverse action against an individual, provides a check and balance to the potential risk of inaccurate data.

Privacy Risk: Because data is entered in an as necessary, *ad hoc* basis, there is a risk that FACTS may contain more information than is necessary to meet the needs of a given investigation.

Mitigation: This risk is partially mitigated. Information input into FACTS is curated by trained investigators. They collect, retain, and input information that appears to have probative value at the time that it is collected. It is normal in the investigatory process that information considered probative at one point in time may later be determined to be irrelevant to a case. However, it is also possible that information considered probative in a case may ultimately be exculpatory in either the immediate case or a linked case. Supervisory and legal review helps to ensure that the data in the system is consistent with the purpose of the program.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

CGIS special agents and support personnel use the information in FACTS to document and inform the agency's criminal investigative activities, and to support criminal prosecutions arising from those investigations. Subject records and ROIs are also used to draw connections between subjects and cases and inform decisions about subsequent case activities. Biographic data about individuals is used for case and identity deconfliction purposes. For example, "case deconfliction" is when a given record is used to ensure a case agent knows that there is pre-existing identity information and possibly already an investigation on an individual for whom they are creating a subject record, whereas "identity deconfliction" involves using the system to ensure one individual does not have multiple subject records.

External law enforcement agencies use FACTS data in support of their investigations or agency missions, as described more fully in Section 6.0. External agencies may receive this information as a result of routine use disclosures, as provided for in section (b)(3) of the Privacy Act, which provides that information may be disclosed for routine uses, as defined in the applicable System of Record Notice. Coast Guard's Security Center (SECCEN) also has access to FACTS data that it uses to determine Coast Guard employees' eligibility for security clearances.

The AHHI component of FACTS is used as a repository of information related to harassment and hate incidents within the Coast Guard. It contains information gathered by CRSPs

during the course of an investigation and may also contain any findings and outcomes from a Command-initiated Administrative Investigation. The data stored within AHHI is searchable by the name of the individual who files a complaint or report of harassment, the name of the alleged victim of harassment, and the name of the alleged harasser. The database can be searched to ensure those being recommended for awards or promotions are not linked to a substantial finding of harassment or hate incident. The information within the database is for internal Coast Guard use only and is not shared externally.

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

No. FACTS does not conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

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

No other DHS components or external agencies have assigned roles and responsibilities within FACTS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to, or inappropriate use or disclosure of, information contained in FACTS. The significance of this risk is enhanced due to the system's law enforcement purpose and the nature of the information about individuals that is contained in the system.

Mitigation: This risk is mitigated through user training, strict access controls to FACTS, operational oversight, and information security controls.

Training and access controls: Annual Coast Guard, DHS, and FACTS training requirements related to privacy and records management are in place. CGIS special agents also receive additional training regarding the special rules for handling criminal justice information in accordance with CJIS and NCIC requirements. Initial access to the system is only provided after a request by the special agent's SAC, and access is tailored to limit an individual to the lowest level of privileges necessary to perform his or her job-related responsibilities. Finally, when determined appropriate by record owners and their supervisors, the originators of cases or records in FACTS may limit the access by other FACTS users to that information, with the caveat that a user may not limit his or her supervisor's access to information.

Operational oversight and information security controls: FACTS has robust auditing

features to help identify and support accountability for user misconduct. The audit logs capture user activity, which includes, but is not limited to, uploading records or data; extracting information from the system; resolving entities within the system, queries, and searches; and viewing investigative records. Supervisors have access to these audit logs and may take disciplinary action for violations of Coast Guard and CGIS policies regarding the system when necessary.

Additionally, FACTS users have the ability to place "alerts" on their cases and receive an email notification in their FACTS inbox when another individual has queried that record, document, or case in the system; the search criteria he or she used; and whether the information was displayed. However, there is an exception to this notification requirement when a supervisor queries a record. This allows the record owner to monitor when other users access specific records and inquire as to why another user has conducted a particular query or viewed a record. This can reveal misconduct on the part of the users who may be inappropriately browsing the system, and serves as a deterrent, as users know it is likely that inappropriate activity will be challenged or reported. When used, query notifications bring transparency to the system that may also reduce duplication of effort. Users are trained to report suspected misuse of FACTS or misconduct associated with FACTS use to supervisors. Finally, FACTS data may be shared electronically or via paper with agencies outside of the Coast Guard in accordance with formalized agreements or pursuant to *ad hoc* requests that conform to the requirements of the Privacy Act. This helps to ensure the sharing is supported by legal authorities and is consistent with the purposes for which the information was collected.

Privacy Risk: For AHHI information, there is a risk of unauthorized access to or inappropriate use or disclosure of information contained in FACTS.

Mitigation: This risk is mitigated by user training, strict access controls to FACTS, operational oversight, and information security controls. Additionally, AHHI records are logically separated from CGIS investigative records, and users do not have accessibility to view or access other's information.

Section 4.0 Notice

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

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

Notice of the existence, contents, and uses of FACTS is provided by the publication of this

PIA and by the following SORNs: DHS/ALL-020 Internal Affairs;[22] DHS/ALL-029 Civil Rights and Civil Liberties Records;[23] and DHS/ALL-038 Insider Threat Program.[24] Because FACTS is a law enforcement system that collects and maintains sensitive information related to criminal investigations, it is not always feasible or advisable to provide notice to individuals at the time their information is input into the system. When CGIS special agents interact with individuals in connection with an investigation, however, those individuals are generally aware that their information will be recorded and stored. CGIS special agents take biographical information from the individuals with whom they interact and write it in field notes in plain view of those individuals. CGIS special agents also inform victims and witnesses that the information they provide will be recorded and stored.

CRSPs use AHHI to collect and maintain information related to investigations conducted by individual units. When investigators interview individuals, they are generally aware that their information will be recorded and stored.

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

Because FACTS is a law enforcement database, it includes information collected from individuals through lawful searches and other non-consensual means. Individuals may decline to provide information, and the consequences of failing to provide some information may include the Coast Guard's decision to pursue administrative or criminal penalties based on other existing information. In some circumstances, a decision not to provide information by some individuals, specifically potential victims, may prevent continued investigation into allegations of criminal activity.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is risk that interviewees may not realize that they have the option to consent or decline to participate in the interview.

Mitigation: This risk is mitigated. Individuals interviewed are provided with their rights advisement via Miranda warnings or rights warnings pursuant to the Uniform Code of Military Justice indicating that their participation in the interview is voluntary. Furthermore, USCG provides notice through the publication of this PIA and associated SORNs.

Privacy Risk: There is a risk that individuals may not be aware their information is

[22] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014), *available at* https://www.dhs.gov/privacy.
[23] *See* DHS/ALL-029 Civil Rights and Civil Liberties Records, 75 FR 39266 (July 8, 2010), *available at* https://www.dhs.gov/privacy.
[24] *See* DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (February 26, 2016), *available at* https://www.dhs.gov/privacy.

contained within FACTS or understand how the Coast Guard uses the information collected about them.

Mitigation: This risk is partially mitigated. Individuals who are questioned directly by CGIS special agents have notice by virtue of the encounter that CGIS is conducting a particular investigation. Although there is a potential risk that a language barrier may cause misunderstanding when CGIS encounters an individual, attempts are made to communicated with individuals in their native language or through an interpreter.

There is also a countervailing risk when individuals are notified that information is being collected about them by CGIS for law enforcement purposes because notification may be the proximate cause of attempting to compromise an investigation, especially if the individual decides to flee, destroy, or conceal evidence, as a result of this notice. This risk directly affects the ability of CGIS to perform its mission. Furthermore, release of information about the existence of an investigation could pose officer safety issues for law enforcement personnel. In such cases, CGIS may intentionally withhold notification to the individual until he or she is arrested or indicted.

In addition to the notice described above, some service providers who are required to provide subscriber information to CGIS pursuant to a subpoena will, in certain instances, inform subscribers that they have provided information to CGIS.

Public notice that informs the public how CGIS uses the information it collects in investigations is provided through this PIA and the associated SORNs.

Privacy Risk: For CRD, there is a risk that individuals may not be aware their information may be contained within FACTS or understand how the Coast Guard uses the information collected about them.

Mitigation: This risk is partially mitigated. Individuals who are questioned directly by command-appointed investigators are given notice by the investigator or by virtue of the encounter that the unit is conducting a particular investigation.

Section 5.0 Data Retention by the Project

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

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

FACTS records are currently being treated as permanent records until an applicable records retention schedule is approved. CGIS is working with the USCG Records Management Office and NARA to schedule the various categories of records contained in FACTS. At this time, CGIS follows existing records retention schedules noted in the SORNs described in Section 1.2. Each category of records that FACTS maintains will have its own records retention schedule in the

finalized FACTS retention schedule.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: This risk is not mitigated. A NARA-approved records retention schedule has not yet been finalized. FACTS records currently follow existing records retention schedules noted in the SORNs described in Section 1.2. This risk will remain until an applicable records retention schedule is approved by the USCG Records Management Office.

Section 6.0 Information Sharing

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

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

Consistent with federal law and DHS policy, information and investigative records from FACTS are shared outside of DHS with other agencies that demonstrate a need to know the information for the performance of their missions, and provide a request detailing such. Information is shared pursuant to formal agreements or through sharing between CGIS personnel and other agency personnel by other means, including, for example, between law enforcement officials assigned to a joint investigation or with prosecuting agencies. FACTS data will be shared if doing so will further law enforcement efforts conducted by CGIS or its law enforcement partners, and disclosure is consistent with applicable law and agency policies.

FACTS information is also shared with federal, state, tribal, local, and foreign law enforcement agencies, as well as relevant law enforcement fusion centers, FBI Joint Terrorism Task Forces (JTTF), and international criminal enforcement organizations such as INTERPOL. All external sharing of FACTS information will be documented using applicable disclosure procedures per DHS policy and applicable statute. Currently, this sharing is conducted manually by CGIS personnel and not via system-to-system connections. However, future iterations of FACTS are intended to provide automated access to other law enforcement databases such as the Law Enforcement Defense Data Exchange (D-DEx), Law Enforcement Information Exchange (LInX), and the DOJ Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center information portal.

CGIS also discloses limited information from FACTS to obtain information from sources

such as witnesses, recipients of subpoenas, and sources of commercial and public data. Information is disclosed in these situations where personnel conducting investigations believe that the parties to whom they are making the disclosure have relevant information. CGIS personnel disclose only the information necessary to receive the information they need.

AHHI data is not shared outside of DHS.

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

The sharing with law enforcement agencies outside of DHS is compatible with the original purpose for collection, namely to conduct criminal law enforcement investigations and other enforcement activities or administrative actions, to uphold and enforce the law, and to ensure public safety. All external sharing falls within the scope of applicable law, including the published routine uses in the DHS/ALL-020 Internal Affairs[25] and DHS/ALL-038 Insider Threat Program[26] SORNs.

AHHI records are not shared externally. AHHI records are logically separated from CGIS investigative records and users do not have accessibility to view or access other's information.

6.3 Does the project place limitations on re-dissemination?

Federal agencies that receive FACTS information are subject to the requirements of the Privacy Act and, as such, may not re-disclose information without prior authorization from CGIS. Additionally, FACTS information is shared with other agencies pursuant to information sharing agreements, and those agreements include provisions for appropriate and adequate safeguarding of sensitive information. Commercial data providers with whom CGIS shares limited information contained in its queries to their systems are prohibited under terms of their contracts from re-disseminating information related to CGIS queries. Such commercial providers are also required to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information, and notify CGIS if they become aware of any breach of security of interconnected systems or potential or confirmed unauthorized use or disclosure of personal information.

AHHI records are not shared externally. Therefore, there is no external dissemination of AHHI records.

[25] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014), *available at* https://www.dhs.gov/privacy.
[26] *See* DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (February 26, 2016), *available at* https://www.dhs.gov/privacy.

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

FACTS users are required to complete and retain a paper memorandum documenting an external disclosure. In future releases, FACTS users will be able to complete this form electronically from within the system and store it in the FACTS case file.

AHHI records are not shared externally. Therefore, there are no records maintained of disclosures outside of the department.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data will be shared with external parties lacking a need to know, and that external sharing will not be properly recorded as required by the Privacy Act.

Mitigation: This risk is mitigated. FACTS users are required by law and policy to share information with only those external partners who have a demonstrated law enforcement, intelligence, or national security need to know. This requirement is in keeping with the law enforcement purpose of the FACTS system. As noted above, CGIS special agents are also required to complete a paper memorandum when making external disclosures. Supervisors routinely review their subordinates' case files and inspect these memoranda as part of their review. This risk is also mitigated by the fact that only CGIS-authorized users have direct user access to the system.

There is no privacy risk for AHHI records, as they are not shared externally.

Section 7.0 Redress

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

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

Individuals seeking information of and access to any of the records covered by this PIA may submit a request in writing to the Coast Guard FOIA Officer by mail, facsimile, or email:

Commandant (CG-611)
Attn: FOIA/PA Officer
U.S. Coast Guard
2703 Martin Luther King, Jr. Ave. SE
Washington, D.C. 20593-7710
(202) 372-8413
eFOIA@uscg.mil

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 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. During the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity.

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

Individuals seeking to correct records contained in the system of records listed above in Section 1.2, or seeking to contest their content, may submit a request in writing to the Coast Guard via mail, facsimile, or email:

Commandant (CG-611)
Attn: FOIA/PA Officer
U.S. Coast Guard
2703 Martin Luther King, Jr. Ave. SE
Washington, D.C. 20593-7710
(202) 372-8413
eFOIA@uscg.mil

All or some of the requested information may be exempt from correction pursuant to the Privacy Act to prevent harm to law enforcement investigations or interests. Providing 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. Access to these records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension. However, USCG evaluates requests for correction and redress on a case-by-case basis. During the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity."

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

Individuals are provided notification about the procedures for correcting their information through this PIA and DHS/ALL-020 Internal Affairs, DHS/ALL-023 Personnel Security Management, DHS/ALL-029 Civil Rights and Civil Liberties Records, and DHS/ALL-038 Insider

Threat Program SORNs. The Coast Guard also provides general notice on its public-facing website about the procedures for submitting FOIA and Privacy Act requests. No individual notification of procedures for correcting FACTS records is currently provided; however, FACTS contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. However, the USCG will review requests on a case-by-case basis. Notification to individuals that they are or have been the target of a law enforcement investigation could undermine the law enforcement mission of the Coast Guard.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to access, correct, and amend records about themselves given the law enforcement and investigatory nature of FACTS.

Mitigation: This risk cannot be fully mitigated. Because FACTS contains data maintained for law enforcement purposes, individuals' rights to be notified of the existence or non-existence of data about them, and to direct how that data may be used by CGIS, are lawfully limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools would no longer be useful. Permitting individuals to direct the agency's use of their information will similarly interfere with the intended law enforcement use of the system. The publication of this PIA and associated SORNs provides general notice about CGIS, CRD, and the Coast Guard's collection of information and the uses of that information. Nevertheless, CGIS maintains an interest in ensuring its information is accurate and will review correction requests and make any changes it deems appropriate. CGIS may grant individuals an opportunity to access or correct their records within the system on a case-by-case basis consistent with law enforcement necessity.

Section 8.0 Auditing and Accountability

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

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

CGIS ensures that FACTS information is used in accordance with the stated practices in this PIA through access controls, auditing procedures, and supervisory or legal review. FACTS maintains internal audit and change logs detailing which records are accessed, viewed, and edited by each specific user. Audit logs are accessible by supervisors, system administrators, and support personnel. Externally, CGIS ROIs are compiled using the information from FACTS and are only provided to the requesting authority or command and the appropriate legal office with an official need to know to review the ROI for proper disciplinary or administrative action in accordance with

existing agency requirements. ROIs are only provided to the previously mentioned authorities for the period of time necessary for the completion of any action deemed appropriate by the proper authority. Upon completion of that purpose, the ROI must either be returned directly to the issuing CGIS office or destroyed locally, as required by the memo provided to the requestor when the requested records are provided.

CRD ensures that AHHI information is used in accordance with the stated practices in this PIA through access controls, auditing procedures, and supervisory or legal review. AHHI maintains internal audit and change logs detailing which records are accessed, viewed, and edited by each specific user. Audit logs are accessible by system administrators and vendor support personnel. Any AHHI ROIs are only provided to the authority or command who initiated the investigation or the appropriate legal office with an official need to know.

The Coast Guard Privacy Office (CG-6P) will conduct a USCG Privacy Evaluation (CGPE) within one year of publication of this PIA. Coast Guard Privacy will share the results of the CGPE with the DHS Privacy Office.

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

CGIS special agents and CRSPs receive annual DHS and Coast Guard-mandated privacy and security training to carry out their investigative responsibilities and apply that training to the protection of the information they have collected and store within FACTS. Completion of the most recent training is factored into the decision to give users access to the system, and only CGIS special agents who receive approval from their SAC are granted access to the system. All CGIS special agents with access to the system receive additional privacy and records management training from other sources, including CBP (due to access to TECS).

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

Only CGIS special agents and support personnel, CRD, legal, and intelligence personnel whose official duties necessitate access to FACTS data will be granted access. CGIS senior-level management (*i.e.*, regional SACs) approve the assignment of user accounts and role-based permissions. Access roles are assigned by a supervisor based on the user's job responsibilities. User accounts and role-based permissions are set up and maintained by CGIS FACTS Administrators. Access roles are reviewed regularly to ensure that users have the appropriate level of access. Individuals who no longer require access are removed from the access list.

CRD ensures that only administrators oversee and approve the assignment of user accounts and update role-based permissions for AHHI. Access roles are assigned by CRD administrators

based on the user's job responsibilities and area of responsibility. Access roles are reviewed regularly to ensure that users have the appropriate level of access. Individuals who no longer require access are removed from the access list.

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?

Any information-sharing agreements, to the extent they are required, will be reviewed by the program's Information Systems Security Officer, CGIS Legal Counsel, the Office of Information and Intelligence Law (CG-LII), the Coast Guard Privacy Office (CG-6P), and the Program Manager. Any memoranda of understanding (MOU) will clearly articulate who will be accessing the information and how it will be used. Any new or revised MOU is sent to the USCG Privacy Officer (CG-6P) for review.

AHHI records are not shared externally and are logically separated from CGIS investigative records and users do not have accessibility to view or access other's information.

Responsible Officials

Stephanie E. McClellen
FACTS Program Manager
Coast Guard Investigative Service
United States Coast Guard

Kathleen L. Claffie
Chief, Privacy Program (CG-6P)
U.S. Coast Guard
(202) 475-3515

Approval Signature

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

_____

James Holzer
Acting Deputy Chief Privacy Officer
Department of Homeland Security