Privacy Impact Assessment Update
for the

Incident Reporting Information System (IRIS)

DHS/USCG/PIA-023(a)

April 20, 2018

Contact Point
James Weaver
Interagency Coordination Division Chief
U.S. Coast Guard
(202) 372-2247

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) United States Coast Guard (USCG) operates the National Response Center's (NRC) Incident Reporting Information System (IRIS). The NRC uses IRIS to collect and disseminate information on pollution, oil, chemical, radiological, biological, and other unknown discharges into the environment, as well as related non-intelligence suspicious activity and security breach incidents, to federal, state, and local on-scene coordinators. The USCG is updating this Privacy Impact Assessment (PIA) to include the Incident Management Software System (IMSS), which supports all functional areas of Coast Guard Incident Management, Incident Action Plan (IAP) development, and incident preparedness activities.

Overview

The NRC was established in the 1970s under the National Oil and Hazardous Substances Pollution Contingency Plan (NCP) mandated by 40 CFR § 300.125(a). The regulation states: "The National Response Center (NRC), located at USCG Headquarters, is the national communications center, continuously manned for handling activities related to response actions. The NRC acts as the single point of contact for all pollution incident reporting, and as the [National Response Team (NRT)] communications center." The USCG does not own the NRC; however, 40 CFR § 300.125(b) requires that the USCG, along with other NRT agencies, is responsible for providing the necessary personnel, communications, facilities, and equipment for the NRC.

The primary function of the NRC is to serve as the sole federal point of contact for reporting all pollution, oil, chemical, radiological, biological, and other unknown discharges into the environment, as well as related non-intelligence suspicious activity and security breach incidents, to federal, state, local on-scene coordinators. In addition to gathering and distributing incident data to on-scene coordinators and serving as the communications center for the NRT (which consists of 16 federal agencies), the NRC also maintains agreements with a number of other federal, state, and local entities for additional notifications regarding incidents meeting pre-established notification criteria. Reports are made to the NRC telephonically or electronically (*e.g.*, fax, email) through a hotline staffed 24 hours a day, 7 days a week. NRC reports can originate from private citizens, government employees, industry members, and foreign entities that have a pollution incident with the potential of impacting the United States. There is no limit on who may call and make a report to the NRC.

IRIS is the primary tool that NRC watch-standers use to collect incident information related to pollution-related incidents and disseminate that information to federal, state, local on-scene coordinators. IMSS is the primary tool that NRC watch-standers use to collect the same type of information, but from USCG personnel, community organizations, and other federal agencies. Both IRIS and IMSS are used to manage incidents of all scales during all functional exercises, full-scale exercises, and incident responses, including small oil spills, natural disasters, and Incidents of National Significance (IONS), such as the Deepwater Horizon oil spill and Hurricane Katrina.

Once an Incident Command Post (ICP) has been established, the incident is managed via the National Incident Management System (NIMS) structure. NIMS is the organizational structure used by DHS to manage command and control, logistics, and personnel involved in an incident in which a command post has been established.

IMSS is an incident management tool that improves response operations and enhances information sharing by providing a Common Operating Picture and automating the major functional areas by providing details only of incident management for: people placement, work assignments, resource tracking, and the IAP operational cycle.[1] IMSS is the standard USCG enterprise-wide software system that has been identified by the Office of Contingency Preparedness and Exercise Policy as a key solution that resolves remedial actions gleaned from the internal review of the Deepwater Horizon response. It helps incident management teams expedite the creation of an IAP as well as fill out documentation used during incident command system (ICS) operations. There is only one IAP for each incident, and that IAP is developed at the incident level. IMSS can be used in any incident in which an IAP is required; however, it is highly recommended that it be used in every incident designated Type 1 or Type 2.[2] It also provides an electronic repository of incident documentation for post-incident archiving. IMSS does not use incident reports;[3] however, it generates IAPs for responders to use in the field to help with managing incidents. The IAPs include working objectives and strategies established to manage the response to an incident. For example, this may include the number of personnel and resources assigned or names of individuals who are in charge of certain operations (*e.g.*, who the Public Information Officer is for an incident). An IAP is created following the below timeline:

1. Initial incident notification occurs.
2. A USCG user creates the incident within IMSS.
3. Users who have been granted access to the system will generate individual IAP documents. The IAP documents include documenting the objectives, reflecting the tactics, and the resources necessary to manage the incident.
4. The IAP documents are then combined to create the final IAP.
5. The incident is closed.

[1] The Incident Action Plan (IAP) is a written plan that defines the incident objectives and reflects the tactics and resources necessary to manage an incident during an operational period.
[2] Events or incidents that are managed using ICS are assigned an incident Type, a number from 1 to 5, with Type 1 ranking the highest and most complex based on operational characteristics such as the number of resources used, the span of impacted locations, and personnel assigned.
[3] Within IRIS, incident reports differ from Incident Action Plans used for IMSS. Incident reports describe the details of an incident, and are submitted via fax, e-mail, or telephone to the National Response Center (NRC) to handle activities related to response actions. Although an IAP is similar regarding the details of an incident, the information is compiled and used as a plan of action for responders in the field to assist with managing the incident.

Personal information contained in IMSS is collected from system users and individuals involved in the incident, and typically includes business contact information, such as name, organization/component, unit, official phone numbers, official email address, and a secondary email address, which is used for password reset purposes.

IMSS user accounts and access are managed by USCG Regional and Sector administrators; with basic system users only having access to their own profile information. Once a need for database access has been determined, a username and password will be given to the user by the unit's user account manager or system administrator. Although USCG is the primary user group for IMSS, other federal, state, local, and tribal government users, as well as participating commercial entities and responsible parties involved in the incident, may be granted access, but only for the period of time that they are designated as participants in the incident command structure.

Once access is granted, the IMSS launch page is where users will log into their IAP database. Users will log into their unit-specified database with their username and password, which will have been given to them previously by the unit's user account manager or system administrator. After entering their username and password, they will be required to enter an authentication number that will be sent to the email address associated with the user account. They must enter this authentication code to complete their login.

It is the responsibility of the unit user account managers or system administrators to ensure that personnel who are granted access to the database are assigned the appropriate user role. Users may be granted access as "view only" approved/completed IAP documents (lowest level privilege assigned) up to the system administrator (highest privilege assigned). The roles that are assigned for each incident are in accordance with those described in the U.S. Coast Guard Incident Management Handbook,[4] which directly falls in line with NIMS requirements.

Reason for the PIA Update

While the functionality of the IRIS and IMSS systems is similar, the reason for this PIA update is to outline the differences between IRIS and IMSS, and identify any additional privacy risks with the information maintained by IMSS. Both systems collect very similar data to include similar types of personally identifiable information (PII). The major difference between the two systems is that the information is collected from a different population. IRIS collects information on incidents specifically from the general public, while IMSS collects incident information specifically from USCG personnel and other federal, state, local, and tribal government users, as well as participating commercial entities and responsible parties.

[4] COMDTPUB P3120.17B.

Privacy Impact Analysis

Authorities and Other Requirements

The USCG's collection of IRIS and IMSS information is in support of its missions as authorized by the National Oil and Hazardous Substances Pollution Contingency Plan, cited at 40 CFR § 300.125(a) and 40 CFR § 300.125(b), which requires the USCG to provide the necessary personnel, communications, facilities, and equipment for the NRC; the USCG Contingency Preparedness Planning Manual Volume IV: Incident Management and Crisis Response; and Commandant, United States Coast Guard Instruction (COMDTINST) M3010.24, which directs the use of IMSS during all functional exercises, full scale exercises, and incident responses when an IAP is developed.

USCG has completed the system security plan (SSP) for IMSS; however, the IMSS security software is and has always been hosted using Amazon Web Services (AWS), a Federal Risk and Authorization Management Program (FedRAMP)-compliant hosting location, in an environment that is exclusive to USCG use. The software application is entirely isolated from any other applications. The software product has been further modified to comply with all existing DHS and USCG information assurance requirements.

IMSS is a commercial-off-the-shelf (COTS), Software as a Service (SaaS) capability. The software provider contractor provides and manages the software through AWS and FedRAMP compliant hosting location, which delivers a standard approach to security assessment, authorization, and continuous monitoring for the Federal Government. The software provider contractor provides monthly scans as part of the contract service to the IMSS USCG Information System Security Officer (ISSO) and Security Controls Assessor (SCA). The ISSO and SCA validate the security scans, and perform continuous monitoring to ensure compliance with the implementation of security controls identified in the *Coast Guard Cyber Security Manual*, COMDTINST M5500.13, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37,[5] and NIST SP 800-53,[6] to include performing an annual security assessment.

The USCG Deputy Chief Information Security Officer (COMDT (CG-65)) has contracted with a software provider to provide the IMSS application. This helps ensure compliance with 40 CFR § 300.125(a) and 40 CFR § 300.125(b), the federally mandated policy for responding to both oil spills and hazardous substance releases, and COMDTINST M3010.24, the Presidential directive that requires the Coast Guard to be prepared to respond to and manage a natural disaster, act of terrorism, or other man-made disaster.

[5] *See* https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final.
[6] *See* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Similar to IRIS, the maintenance of information in IMSS is covered under the Marine Information for Safety and Law Enforcement (MISLE) System of Records Notice (SORN).[7]

Characterization of the Information

While IMSS and IRIS differ, the same information as outlined in the original IRIS PIA[8] is still collected through IMSS. However, whereas IRIS collects information from the general public, IMSS collects the same information from USCG personnel and other federal, state, local, and tribal government users, as well as participating commercial entities and responsible parties.

IMSS collects the following information from these users for account access:

- Contact name;
- Contact organization;
- Contact phone number;
- Contact email address;
- Contact secondary email (in case of password reset);
- City;
- State; and
- ZIP code.

The documentation loaded in to IMSS may contain similar types of PII as an IAP may contain the contact information of the preparer of the document or individuals associated with the incident. For example, a first responder's name may be in an IAP that is completed by the individual's supervisor.

Uses of Information

IMSS uses information similar to the way IRIS uses the information it collects. USCG and other federal, state, local, or community users input incident information into IMSS and then use the information to manage the incident. IMSS can manage incidents of all scales from small oil spills and natural disasters to incidents of national significance, like the Deepwater Horizon oil spill. The system provides a Common Operating Picture and automates the major functional areas of incident management: personnel, resource tracking, and the IAP operational cycle. The system provides an electronic repository of incident documentation for post-incident archiving.

[7] DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305 (June 25, 2009).
[8] *See* DHS/USCG/PIA-023 Incident Reporting Information System (IRIS) (September 16, 2015), *available at* https://www.dhs.gov/privacy.

Notice

Because a different population is the source of the information, additional measures are required to provide adequate notice. A Privacy Act Statement will be placed on the IMSS login screen for users.

Privacy Risk: There is risk that individuals may not be aware that IMSS is collecting their data and for what purpose.

Mitigation: This risk is mitigated. The USCG will provide a Privacy Act Statement on the login screen that explains to the user that his or her information is collected and that submission of the data is voluntary. Also, the USCG provides notice of IMSS through the publication of this PIA and through the DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE) System of Records Notice (SORN).[9]

Privacy Risk: There is risk that individuals (such as first responders) may not be aware that USCG is collecting their information because their supervisor is the one who inputs the information into IMSS via an IAP.

Mitigation: Generally this risk is unmitigated. These individuals would be working in an official capacity as federal, state, local, or tribal government personnel, or as a participating commercial entity or responsible party employee when this information is collected. However, individuals that are involved in managing and responding to these types of incidents will know of USCG's involvement as the lead organization.

Additionally, this PIA provides general notice of this collection.

Data Retention by the Project

The information in IMSS is retained in accordance with National Archives and Records Administration (NARA) retention schedule NI-026-05-15, which is the same retention schedule as IRIS information. This retention schedule states: "Disposition is Permanent, with the exception of Notifications not associated with a Case or Activity." Those records not associated with a case or activity have a cut-off date at end of calendar year in which notification was received. Those records should then be destroyed/deleted five years after the cut off. It is the responsibility of the IMSS system owner and Information System Security Officer (ISSO) to ensure that the records are destroyed/deleted.

Privacy Risk: There is a risk that USCG may retain records containing PII in IMSS for longer than is necessary and allowable by the retention schedules.

Mitigation: This risk is mitigated. ISSOs and system owners ensure that records are destroyed and deleted in accordance with the records schedule. These individuals conduct yearly evaluations to determine which information/incidents should be purged from the system.

[9] DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305 (June 25, 2009).

Information Sharing

The information sharing discussion in the IRIS PIA generally applies to IMSS, with minor exceptions. Unlike IRIS, IMSS does not share incident information and PII with the Department of Transportation (DOT) or Environmental Protection Agency (EPA). However, IMSS does share information with other federal, state, local, and tribal government users, as well as participating commercial entities and responsible parties involved in an incident.

Individual Access, Redress, and Correction

Individuals seeking access, redress, or correction to their data may submit a Privacy Act request. Individuals, regardless of citizenship status, may also request access to their records under the Freedom of Information Act (FOIA). Individuals may submit these requests to EFOIA@uscg.mil, or in writing to:

Department of Homeland Security
United States Coast Guard Headquarters
Commandant (CG-611)
2703 Martin Luther King Jr. Ave. SE
Washington, D.C. 20593-0001

In addition, because individual users present their information directly through IMSS, they are able to access their data through their system profile at any time. Through this access, users can correct erroneous information about themselves.

Privacy Risk: There is a risk that an individual associated with an incident (*e.g.*, a first responder) will not know that his or her information is maintained in IMSS and will not be aware of the redress procedures to access and correct his or her information.

Mitigation: This risk is partially mitigated through the publication of this PIA. Individuals involved in incidents are likely to encounter USCG or other personnel who collect their information over the course of an incident response. While they might not receive information at the time of collection regarding redress and access procedures, this PIA (and other published privacy documentation, including previous PIAs and the relevant SORN) provide instructions related to accessing information through Privacy Act and FOIA processes.

Auditing and Accountability

IMSS audit logs are reviewed on a bi-weekly basis to detect anomalies.

All IMSS personnel are required to annually complete the DHS privacy training regarding safe handling and protection of PII, which includes the mandated *DHS: Protecting Personal Information, DHS Record and Federal Cyber Awareness Challenge Training.* Training is also provided by the software provider for all users of the system.

The primary user group for this software system is the USCG. During an incident, the USCG may grant account access to other federal, state, local, and tribal government users, as well as participating commercial entities and responsible parties involved in the incident, only for the period of time that they are designated as participants in the incident command structure. Access to incident information is strictly controlled within the software system by user access levels. The software system is designed with controls to manage the access level of users based on their role and attributes, to prevent unauthorized access to more sensitive data.

Responsible Official

LCDR Jeffrey Olk
Project Manager (CG-7612)
United States Coast Guard

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security