Privacy Impact Assessment
for the

Incident Reporting Information System (IRIS)

DHS/USCG/PIA-023

September 16, 2015

Contact Point

James Weaver
Interagency Coordination Division Chief
U.S. Coast Guard
202-372-2247

Reviewing Official

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Coast Guard (Coast Guard) operates the National Response Center's (NRC) Incident Reporting Information System (IRIS). IRIS is used by the NRC to collect and disseminate pollution, railroad, non-intelligence suspicious activity, and security breach incident related information to federal, state, and local on-scene coordinators. This Privacy Impact Assessment (PIA) is being conducted because IRIS maintains personally identifiable information (PII).

Overview

The National Response Center (NRC) is the federal government's national communications center, which is staffed 24 hours a day by U.S. Coast Guard officers and marine science technicians. The NRC is the sole federal point of contact for reporting all hazardous substances releases and oil spills. The NRC receives all reports of releases involving hazardous substances and oil that trigger federal notification requirements under several laws.

NRC was established in the 1970s under the National Oil and Hazardous Substances Pollution Contingency Plan ("National Contingency Plan").[1] The National Contingency Plan regulation mandates the NRC, located at USCG Headquarters, as the national, continuously-manned communications center for handling activities related to response actions. The NRC acts as the single point of contact for all pollution incident reporting,[2] and as the National Response Team [(NRT)] communications center.

NRC serves as the sole national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment that occur anywhere in the United States and its territories. Reports are made to the NRC telephonically through a manned 24/7 hotline. NRC reports can originate from private citizens, government employees, industry members, and foreign entities that have an oil spill with the potential of impacting the United States. There is no limit on who may call and make a report to the NRC.

In addition to gathering and distributing incident data to federal and state on-scene coordinators and serving as the communications center for the National Response Team (NRT) (which consists of fifteen federal agencies), the NRC also provides notification to those government entities with a need to know. For example, the National Transportation Safety Board (NTSB) will receive an NRC notification on events that involve a major rail accident. Reports to the NRC activate the National Contingency Plan[3] and the federal government's response

[1] 40 CFR §300.125(a)
[2] 33 CFR § 101.305.
[3] The National Oil and Hazardous Substances Pollution Contingency Plan, more commonly called the National Contingency Plan or NCP, is the federal government's blueprint for responding to both oil spills and hazardous substance releases. The NCP is the result of efforts to develop a national response capability and promote coordination among the hierarchy of responders and contingency plans. The first NCP was developed and published

capabilities. It is the responsibility of the NRC staff to notify the pre-designated On-Scene Coordinator[4] assigned to the area of the incident and to collect available information on the size and nature of the release, the facility or vessel involved, and the party(ies) responsible for the release. The NRC maintains reports of all releases and spills in a national database.

The NRC's role was expanded to include notification of suspicious activities and notification of breach of security in July of 2003.[5] Per the regulation, suspicious activities are those "activities that may result in a transportation security incident." Breach of security is defined as an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated. The U.S. Coast Guard requires regulated facilities and vessels to report suspicious activities and breach of security incidents to the NRC. The NRC relays these reports to the Federal Maritime Security Coordinator (FMSC) and appropriate security agencies. The FMSC or designated representative will follow up on the incident report and decide on the need for further action.

IRIS is the primary tool that NRC watch-standers[6] use to collect and disseminate incident information related to pollution, railroad, non-intelligence-related suspicious activity, and security breach incidents to federal and state On-Scene Coordinators. IRIS is supported through interagency funding and has been in existence since 1990. IRIS is hosted at USCG Headquarters and is sponsored by the Office of Environmental Response Policy (CG-MER).

Previously, IRIS received some incident reports through its public facing website; however, that capability has been disabled. Members of the public and local, federal and state agencies may only submit reports by facsimile (fax), electronic mail (e-mail), or telephone.

---

in 1968 in response to a massive oil spill from the oil tanker Torrey Canyon off the coast of England. More than 37 million gallons of crude oil spilled into the water, causing massive environmental damage. To avoid the problems faced by response officials involved in this incident, U.S. officials developed a coordinated approach to cope with potential spills in U.S. waters. The 1968 plan provided the first comprehensive system of accident reporting, spill containment and cleanup. The plan also established a response headquarters, a national reaction team and regional reaction teams (precursors to the current National Response Team and Regional Response Teams). Congress has broadened the scope of the NCP over the years. As required by the Clean Water Act of 1972, the NCP was revised to include a framework for responding to hazardous substance releases, as well as oil spills. Following the passage of Superfund legislation in 1980, the NCP was broadened to cover releases at hazardous waste sites requiring emergency removal actions. Over the years, additional revisions have been made to the NCP to keep pace with the enactment of legislation. The latest revisions to the NCP were finalized in 1994 to reflect the oil spill provisions of the Oil Pollution Act of 1990.

[4] On-Scene Coordinators (OSCs) are the federal officials responsible for monitoring or directing responses to all oil spills and hazardous substance releases reported to the federal government. OSCs coordinate all federal efforts with, and provides support and information to, local, state and regional response communities. An OSC is an agent of either EPA or the U.S. Coast Guard, depending on where the incident occurs. EPA's OSCs have primary responsibility for spills and releases to inland areas and waters. U.S. Coast Guard OSCs have responsibility for coastal waters and the Great Lakes.

[5] These terms are outlined in 33 CFR 101.305.

[6] "Watch-standers" are NRC employees that answer phones, speaking to the reporting party, and enter information into IRIS.

Incident Reports

Full incident reports with a Coast Guard connection, which may contain PII, are pulled via open database connectivity (ODBC) and stored on the USCG Marine Information for Safety and Law Enforcement (MISLE) system,[7] which is only available to authorized Coast Guard personnel via the Coast Guard intranet. On an hourly basis, MISLE ingests incident or oil spill information with a Coast Guard nexus from IRIS and includes:

- Date;
- Time;
- Location of spill;
- Type of spill (oil, gas, etc.);
- Name of reporting person; and
- Contact information of reporting person making report (email or telephone number)

This information is stored in MISLE as a "Notification" and described in the MISLE PIA.[8]

Incident reports derived from MISLE are manually reviewed and any personally identifiable information is identified and removed and the remaining data is then posted on the Coast Guard publicly available CG Maritime Information Exchange (CG MIX) website for public consumption.[9]

Full incident reports, including any PII from individuals who reported the incident, are also transmitted to the Department of Transportation (DOT) and U.S. Environmental Protection Agency (EPA) via hypertext transfer protocol secure (HTTPS) connections. DOT and EPA require real time transmission of NRC data for their first responders. This requirement is outlined in the Memorandum of Understandings (MoUs) established between NRC, DOT, and EPA.

The IRIS database (which is an Oracle database contained within IRIS) is the primary repository and is backed up to a disaster recovery site at USCG Operations Service Center (OSC) located in Martinsburg, WV.

---

[7] DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE) PIA (September 8, 2009).
[8] *See id.* page 6, "Notifications identify new incidents for action by field units. Notifications are communications to the Coast Guard, from external or internal sources, regarding events that will initiate Coast Guard actions. Examples include: radio calls from boaters in distress, phone reports of pollution incidents, and written reports of marine casualties."
[9] *See* the National Response Center public-facing website with reports dating back to 1990, *available at* http://www.nrc.uscg.mil/.

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 National Response Center (NRC) was established in the 1970s under the National Oil and Hazardous Substances Pollution Contingency Plan (NCP) and is cited in 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."

USCG does not own NRC; however, 40 CFR 300.125(b) requires "The Commandant, USCG, in conjunction with other National Response Team (NRT) agencies, shall provide the necessary personnel, communications, plotting facilities, and equipment for the NRC."

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

DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE).[10]

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

USCG is developing a system security plan (SSP) for IRIS. IRIS is currently undergoing its first System Authorization, and will complete an SSP once the security authorization process is complete. IRIS's Federal Information Processing Standards (FIPS) 199 determination is classified as "moderate."

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

Yes, records are maintained in accordance with MISLE's NARA retention schedule NI-026-05-15.

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 contained within IRIS is not subject to the PRA.

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

Section 2.0 Characterization of the Information

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

IRIS maintains the following information from members of the public, private sector (industry members), and other state or federal government entities. Most callers who report incidents to the NRC are private sector or government officials who provide business contact information, however IRIS does capture some personal contact information if the reporting party is a concerned citizen.

Reporting parties:

- Reporting parties full name;
- Reporting parties company name;
- Reporting parties personal phone numbers (if member of the public);
- Reporting parties business phone numbers;
- Reporting parties personal address (if member of the public);
- Reporting parties business address;
- Reporting parties personal e-mail address (if member of the public);
- Reporting parties business e-mail address; and
- Reporting parties city/state/zip code.

The NRC also collects information about "suspected parties" who contributed to or caused the incident or spill. Oftentimes, the reporting party will not know the cause of the incident and in that case, suspected party information is marked as "unknown."

Suspected parties:

- Suspected responsible parties full name;
- Suspected responsible parties company name;
- Suspected responsible parties personal phone numbers;
- Suspected responsible parties business phone numbers;
- Suspected responsible parties personal address;
- Suspected responsible parties business address; and
- If a vehicle is involved in the incident report, a license plate number may be collected.

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

NRC obtains information from incident reporters (i.e., members of the public, industry members, or local, state, or federal government entity) via telephone, fax, or e-mail.

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

No.

2.4 Discuss how accuracy of the data is ensured.

NRC is the federal intake entity for all initial oil, chemical, radiological, biological and etiological reports. The data collected by NRC is initial information only. NRC then relays the incident information to the appropriate regulatory federal agency responsible for that particular incident. That appropriate responding federal agency will verify the accuracy and capture the information within its respective database. The NRC acts as the call center responsible for triggering the National Response System. Further information on the NRS can be found through the EPA at http://www2.epa.gov/emergency-response/national-response-system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information submitted by reporting parties may be inaccurate.

Mitigation: IRIS is used to support the NRC, which acts as a call center for oil and pollution spills. Necessarily, not all of the information stored in IRIS will be accurate, but instead will be based on whatever the reporting party shares with the NRC. Therefore, IRIS is used solely for information intake purposes but does is not used to make any determinations about suspected parties or individuals. IRIS is not used for investigatory purposes and does not make any operational decisions based on the suspected party information. If the suspected party information is inaccurate, the record will be clarified in MISLE as part of any subsequent investigation.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

NRC uses this data to provide government emergency responders with accurate and timely information. Federal responders are usually hours away from an incident and an on-scene

contact provides additional incident information and an up to date picture while responders are en route.

NRC is the federal intake entity for all for all oil, chemical, radiological, biological, and etiological discharges into the environment that occur anywhere in the United States and its territories. NRC also takes initial reports of suspicious activity or breaches of security at facilities regulated by USCG. The initial information collected by NRC is disseminated to the federal, state, and local government agencies within the area that are responsible for that particular event. The information collected by NRC is also used by first responders to investigate the incident.

NRC uses information similarly to a 911 dispatch center. NRC is the centralized national reporting hotline, making it easy to remember what number to call for pollution events. NRC collects the initial information, locates the agencies within a particular area that would respond to the event, and provides them with the necessary information to conduct a response.

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.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information maintained within IRIS may be used in a manner inconsistent with the original purpose for collection.

Mitigation: Incident reports are only made available to certain members of government agencies who have the need to know. These government members are also trained on the uses of PII and understand that a violation could lead to a loss of access to NRC information. USCG has incorporated data security procedures and requires all watch-standers to complete annual privacy and cyber awareness training. NRC conducts quarterly on the job training (OJT) that includes privacy awareness and reiterates the appropriate classification of 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.

USCG provides notice to reporting individuals by explaining the purpose of collecting the contact information during reporting phone calls. USCG provides notice through the publication of this PIA and DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE) SORN.[11]

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

When individuals call to report an incident, they are asked whether they would like to remain anonymous. They have the option to remain completely anonymous or to provide only partial information. NRC will still document the incident details without complete contact information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals are not provided with a Privacy Act Statement at the time of information collection.

Mitigation: This risk is fully mitigated. The NRC collects information telephonically, therefore reporting parties are not presenting with a Privacy Act Statement on a form. NRC mitigates this risk by explaining to the reporting party at the time of collection how their data is being used. Furthermore, USCG provides notice through the publication of this PIA and DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE) SORN.

Section 5.0 Data Retention by the project

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

The IRIS database contains all reports from its inception in 1990 to the present. The information contained within the database is used to fulfill Freedom of Information Act (FOIA) requests and provide information to agencies conducting environmental investigations.

Because of the nature of the data (and the fact that it is subject to FOIA requests), Coast

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

Guard information is retained per the legally mandated National Archives (NARA) approved schedule for the Marine Information for Safety and Law Enforcement (MISLE), N1-026-05015. Disposition is Permanent, with the exception of Notifications not associated with a Case or Activity (1.B): "Cut off at end of calendar year in which notification was received. Destroy/delete 5 years after cutoff."

Overall, the length of time this data is maintained (permanent) was deemed necessary by USCG attorneys, Program Managers, and NARA as subject data is needed long term as a record of USCG's business processes supporting Marine Safety, Maritime Security, Environmental Protection, Law Enforcement, Search and Rescue, and Bridge Administration activities needed for investigations, research, litigation et al.

EPA information is retained through NARA retention schedule N1-412-07-54. Department of Transportation information is retained through NARA retention schedule DAA-0571-2015-0007.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: IRIS maintains records from multiple agencies with multiple records retention schedules.

Mitigation: Records categorized for the U.S. Coast Guard pertaining to pollution incidents, non-intelligence related suspicious activity, and security breach incidents are stored in MISLE and are subject to MISLE's record retention schedule. IRIS transfers USCG records to MISLE for storage consistent with the applicable NARA schedule.

Records categorized for the EPA pertaining to pollution incidents are stored in EPA's system and are subject to its system's record retention schedule. Records categorized for the Department of Transportation pertaining to pollution incidents are stored in DOT's system and are subject to its system's record retention schedule. IRIS will ensure each NRC report contains either a USCG, EPA, or DOT agency. This will ensure the record is sent to the appropriate database for long term retention.

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.

Yes. NRC shares IRIS data with DOT and EPA. These agencies utilize the NRC as a communication center for pollution incidents that impact their regulatory responsibilities. As such, the NRC is obligated to send these agencies all information regarding the events that

impact their operation. Data is also scrubbed to remove sensitive data and PII then posted on the CG Maritime Information Exchange (CG MIX) website for public consumption (i.e. FOIA).

The NRC also shares incident reports with state and local governments. In many parts of the country, the local first responders are in a position to arrive on scene well before the responsible federal agencies. The NRC reports notify the local responders of an incident and initiate the response process. State and local agencies may request to be added to the NRC's distribution list through an application process. The entities can identify the specific location and type of report they wish to receive. This prevents excessive sharing of reports to agencies that do not have a need for the information.

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

External sharing is compatible with NRC's role as the national communications center continuously manned for handling activities related to response actions.

DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE) System of Records, Routine Use "I" permits DHS to share information to federal, state, and local environmental agencies, including, but not limited to, the EPA, to access historical data that may improve compliance with U.S. laws relating to environmental protection. Routine Use "O" allows sharing to federal, state, or local agencies with which the U.S. Coast Guard has a memorandum of understanding, memorandum of agreement, or inspection and certification agreement pertaining to marine safety, maritime security, maritime, law enforcement, and marine environmental protection activities.

6.3 Does the project place limitations on re-dissemination?

Entities (i.e. MISLE, DOT, & EPA) with which NRC shares IRIS information are not allowed to - re-disseminate data that is sensitive or contains PII. Some limited re-sharing or re-dissemination of non-sensitive and non-PII scrubbed data may be posted on CGMIX for open government and FOIA disclosure purposes.

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

NRC maintains written correspondence with any agency (federal, state, or local) that requests NRC information. That correspondence is in the form of a signed application detailing the type of information requested. NRC's system, IRIS, tracks each transmission of this data. Each NRC report is stamped with the name of the agency that received the information and how that agency received the information.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the NRC may disseminate USCG information externally inconsistent with the Privacy Act and DHS/USCG-013 MISLE SORN.

Mitigation: All external sharing is compatible with NRC's role as the national communications center continuously manned for handling activities related to response actions. NRC watch-standers are trained to only disseminate information to on-scene responders and agencies that have a need to know to accomplish the NRC mission. NRC has signed agreements with DOT and EPA regarding the data provided by IRIS. Employees of those agencies who are privy to that data are trained on uses and restrictions and are aware of the consequences of misuse. NRC maintains a written agreement with each agency (federal, state, and local) that requests NRC information. That agreement explains the expectations for the proper handling of NRC information, which includes PII.

Section 7.0 Redress

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

Individuals seeking access to their data may submit a Privacy Act request in writing to USCG, Commandant (CG-611), 2703 Martin Luther King Jr Avenue SE STOP 7710, Attn: Freedom of Information Act (FOIA) Coordinator, Washington, DC 20593-7710. Individuals may also submit a request to EFOIA@uscg.mil.

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

Individuals may seek to correct their information through a Privacy Act request as cited in Section 7.1 above.

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

Individuals are provided notification of the procedures to correct their information through this PIA and DHS/USCG-013 Marine Information for Safety and Law Enforcement SORN. [12]

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

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals who are reported as suspected parties to the NRC will not be aware which federal agency is storing their records, and therefore, will not be able to correct or amend their records.

Mitigation: Depending on the type of incident reported, USCG, EPA, or DOT are responsible for investigating and adjudicating the incident. IRIS serves as the intake point for incidents. If the incident is related to a USCG incident, individuals may be able to obtain access, correct, or amend their record by following the procedures cited above. However, FOIA/Privacy Act exemptions may preclude this action.

Individuals are encouraged to contact the NRC 1-800-424-8802 or NRC@uscg.mil for clarity. If an individual wishes to correct or amend records that are not USCG records, the NRC will assist in directing individuals to the proper agency.

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?

NRC has signed agreements with DOT and EPA regarding the data provided by IRIS. The Information System Security Officer (ISSO) conducts audits on system logs to ensure IRIS has not been compromised by USCG users. The header of each NRC report states "***GOVERNMENT USE ONLY*** Information released to a third party shall comply with any applicable federal and state Freedom of Information and Privacy Laws." The NRC uses news alerts to monitor information released to media and ensure that information falls in line with the Privacy Act requirements.

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

All NRC watch-standers are required to complete DHS privacy and cyber awareness training annually.

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 NRC members, database administrators, and persons with the need to know (with accompanying authorization) within USCG, DOT, EPA, and local, state, and federal agencies (involved in response) are able to view full records. Members of the public may access non-

sensitive and non-PII information proactively disclosed to the public via the Coast Guard's public-facing FOIA disclosure system, CGMIX.

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?

Current IRIS information sharing MOUs have been reviewed by the program manager, system owner, counsel, and authorizing official. IRIS is undergoing System Authorization and all new or revised MOUs will also be sent to the USCG Privacy Officer for review.

Responsible Officials

James Weaver
Interagency Coordination Division Chief
U.S. Coast Guard
Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security