Privacy Impact Assessment
for the

NOC Patriot Report Database

December 7, 2010

<u>Contact Point</u>
Ashley Tyler
Department of Homeland Security
Office of Operations and Coordination and Planning

<u>Reviewing Official</u>
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The National Operations Center (NOC) in the Office of Operations Coordination and Planning (OPS) operates the NOC Patriot Report Database. The NOC Patriot Report Database is a repository for reports generated to record and track suspicious activity that may implicate terrorism-related or criminal activity. OPS has conducted this privacy impact assessment (PIA) because the NOC Patriot Report Database may contain personally identifiable information (PII).

Overview

The NOC is the primary national-level hub for domestic situational awareness, common operational picture, information fusion, information sharing, communications, and coordination pertaining to the prevention of terrorist attacks and domestic incident management. The NOC is the primary conduit for the White House Situation Room and DHS Leadership for domestic situational awareness and facilitates information sharing and operational coordination with other federal, state, local, tribal, non-governmental operation centers and the private sector.

In fulfillment of its mission to provide domestic situational awareness of all threats and hazards, the NOC Fusion Desk utilizes the NOC Patriot Report Database to record and track suspicious activity that may implicate terrorism-related or criminal activity. The reports generated are called NOC Patriot Reports. The content of a NOC Patriot Report varies and may or may not contain PII. The NOC Fusion Desk officer writes a NOC Patriot Report when information received from federal, state, local, tribal, and territorial agencies and organizations, foreign governments and international organizations, domestic security and emergency management officials, private sector entities, or individuals, is determined (based on training, experience, and their individual knowledge of the subject at hand) to be credible and either possibly linked to terrorism and/or criminal behavior. When further corroboration of a report is needed, the desk officer may search publically available data, such as news organization websites or from commercial databases; or in the case of a private citizen report, the desk officer may reach out to the citizen's local authorities.

NOC Patriot Reports are distributed as soon as the information is deemed credible and accurately documented in the NOC Patriot Report Database. The Fusion Desk distributes all NOC Patriot Reports via email to a "standard" distribution list which includes all organizations that have a physical presence at the NOC; the FBI's 24/7 operations center Counter Terrorism Watch (CTW); a distribution list for all DHS I&A Representatives assigned to the individual fusion centers; state and local fusion centers; National Infrastructure Coordination Center (NICC); and Protective Security Advisors (PSA) Duty Desk (24/7 Center/reach back for PSA's in the field).

The level of effort required to produce a NOC Patriot Report varies on a report by report basis. The primary determining factor is the amount of information provided to the Fusion Desk and the amount of time it takes the desk officer to confirm certain information, gather supporting documents (maps, photos, police reports, etc.) and compile that information into a reportable format which may be easily read and understood by the target audience.

The NOC Patriot Report Database also serves as an archive of all NOC Patriot Reports processed by the NOC-HSIN (Homeland Security Information Network) and NOC Fusion Desks – these desk officers provide support to the NOC and its components within the HSIN network.

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?

Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)) requires the NOC "to provide situational awareness and establish a common operating picture for the entire federal government and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other manmade disaster; ensure that critical terrorism and disaster-related information reaches government decision-makers."

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

The current collection is covered by the DHS/IAIP-001 Homeland Security Operations Center Database SORN. As part of the biennial review of DHS SORNs, DHS has decided to update and rename this SORN to provide additional transparency. In conjunction with this PIA, DHS is publishing the DHS/OPS – 003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN.

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

Yes, Authority to Operate was granted on March 31, 2009, valid for three years.

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

OPS is working with NARA to develop a records retention schedule of no more than five (5) years.

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.

No specific form is being filled out by the public therefore PRA is not implicated.

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.

The NOC Patriot Report Database provides a thorough documentation of the events, incidents, or suspicious activities that are reported to the NOC Fusion Desk. SAR data may include the following elements as made available by the reporting source: description of the suspicious activity, a description of a possible threat, date-time and location of incident, reliability rating of informational source, validity rating of content, cross-referenced record number, if applicable, critical infrastructure indicators, names of reporting and/or responding agency personnel, and their respective contact information. An “additional comment” section provides a contextual narrative of the event and the as available: name, alias, height, weight, sex, build, race, complexion, eye color, hair color, hair style/length, ethnicity, distinguishing features and personal identifiers (e.g., drivers license, passport, Social Security number, etc.) of the person(s) engaged and/or connected to the suspicious activity.

The NOC Patriot Report Database covers the following categories of individuals:

- Federal, state, local, tribal, and territorial officials; foreign government and international officials; domestic security and emergency management officials; and private sector individuals who request assistance from, provide information to, are the subject of, or participate with the Department in activities related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters; and
- Individuals who provide information to the Department related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters, including Suspicious Activity Reports (SARs).

Contact information collected from the person calling in the report NOC Patriot Reports not required and is completely voluntary. Such information may include: name, address, home phone, or work phone. This information may be used to help further substantiate a report. For example, if a private individual reports suspicious activity near a nuclear power plant, local law enforcement authorities might be contacted to confirm that there is indeed suspicious activity. In this case, the information received from local law enforcement would also be entered into the NOC Patriot Report Database and would include the name, title, and contact information of the official.

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

Information is collected from private individuals submitting tips or observations of suspicious activity to the NOC Fusion Desk and when warranted, information from local authorities that corroborates or disproves a report. Information received from private citizens in strictly voluntary and initiated by the caller. While the NOC may receive SAR data from other sources, that other SAR data is not incorporated in the NOC Patriot Report Database.

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

The NOC Patriot Report Database may have information from commercial sources or publicly available data. As part of the effort of the Fusion Desk officers to determine whether or not the information is credible, the Fusion Desk officers may query publicly available data, including websites as well as commercial data sources. For example, if someone calls the Fusion Desk to report an explosion in Times Square, the desk officer may check CNN or CNN.com to see if there is any substantiating information being reported.

2.4 Discuss how accuracy of the data is ensured.

In order to determine if reported information has a possible nexus to terrorism or criminal activity, Fusion Desk officers have the necessary training, experience, and individual knowledge of the subject at hand to properly vet information for credibility and accuracy. Additionally, Fusion Desk officers will look both at internal DHS databases as well as commercial databases and publicly available data to corroborate information provided through the NOC Patriot Report process.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more PII than is necessary may be collected.

Mitigation: This privacy risk is minimized by the strict controls imposed and training mandated to ensure Fusion Desk Officers understand what is appropriate use and collection of sensitive PII. Further, any information provided by the caller information is summarized and input into a call log report that is only shared upon a verified need to know bases. In order to become an authorized user, a Fusion Desk officer must have successfully completed privacy training and hold appropriate security clearances (at a minimum “secret”). Finally, an officer must have a “need to know” for the information in the performance of their official duties.

Privacy Risk: There is a privacy risk that inaccurate information will be attributed to the individual as part of the corroboration process.

Mitigation: Information from/about the reporting individual is used only to help verify the event they are reporting. If an individual believes for any reason that inaccurate information about them was in the database, they can contact the fusion desk to have it corrected.

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.

The NOC utilizes the NOC Patriot Report Database to collect, report, analyze, and fuse information related to terrorism-related or criminal-related threats and activities collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals. Those Patriot Reports that meet the ISE-SAR Functional Standard Version 1.5 will be entered into the DHS ISE-SAR Server.

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, only Fusion Desk officers are afforded access to the database.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of misuse or unauthorized access to the information.

Mitigation: To mitigate this risk, access to data in the NOC Patriot Report Database is controlled through passwords and restrictive rules. Authentication and role-based user access requirements ensure that users can only access or change information that is appropriate for their official duties. Background checks are conducted on users to ensure they are suitable for authorized access to the logs. The effectiveness of authentication and security protections are verified through audits of system operation and usage. Further, the NOC is located in a Sensitive Compartmented Information Facility.

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 is provided through this PIA and through the publication of DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN.

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

When an individual is submitting information to the NOC over the phone, he/she has the right to decline providing personal information. As an example, an anonymous caller contacts a law enforcement agency with a report of suspicious activity. The information may be submitted to the NOC without capturing the caller's identifying information. However, in instances where PII is provided as part of the suspicious report, (e.g., the description of a person/persons acting suspiciously) the individual(s) being described is unlikely to have knowledge that his/her information has been submitted to the system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a possibility of individuals not being aware of the collection of information.

Mitigation: Notice of the collection of information is provided via this PIA and the DHS/OPS-003 SORN mitigating this risk.

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.

OPS is working with NARA to develop a records retention schedule of no longer than five (5) years. This five-year retention schedule is based on the operational needs of the Department.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a possibility of retaining information longer than is necessary.

Mitigation: Although there is always risk inherent in retaining PII for any length of time, the data retention period for the NOC Patriot Report Database is based on case type identified in the NARA retention schedule and is consistent with the concept of retaining PII only for as long as necessary to support the agency's mission.

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.

The Fusion Desk distributes all NOC Patriot Reports via email to a "standard" distribution list which includes the following: DHS components with an operational or law enforcement mission, FBI CTW, a distribution list for all DHS I&A Representatives assigned to the individual fusion centers, state and local fusion centers, NICC, and PSA Duty Desk. There is the possibility of a report being disseminated to other entities from agencies on the NOC distribution list, however, it would be strictly on a "need to know" basis to be determined by the agency that receives it from the NOC. The sharing of NOC Patriot Reports through a standard distribution list to notify appropriate entities of possible terrorism-related or criminal activity is compatible with the routine uses listed in the SORN.

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

Routine uses of DHS/OPS-003 allows DHS to share information with federal, state, or local agency, or other appropriate entities or individuals, through established liaison channels for counterintelligence or antiterrorism purposes. The sharing of NOC Patriot Reports through a standard distribution list to notify appropriate entities of possible terrorism-related or criminal activity is compatible with this routine use.

6.3 Does the project place limitations on re-dissemination?

External organizations secure NOC Patriot Reports in accordance to the terms of information sharing agreements which include provisions for appropriate and adequate safeguarding of sensitive information and restrictions on re-dissemination.

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

NOC Patriot Reports are only disseminated by email and only to authorized entities. A copy of the email and all the recipients is kept in the sent box of the Fusion desk as an audit trail.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a potential risk of NOC Patriot Reports being leaked, misused, or lost by the agencies with which DHS shares information.

Mitigation: The distribution list of external entities who receive the NOC Patriot Reports is narrowly tailored to only include those agencies that have a need to know. No external organizations have direct access to the NOC Patriot Report Database, meaning external entities do not have access through individual user accounts. Finally, all sharing is consistent with the routine uses enumerated in DHS/OPS-003.

Privacy Risk: There is a potential risk of NOC Patriot Reports being further disseminated by receiving agencies.

Mitigation: When the NOC distributes a NOC Patriot Report it clearly labels this information as law enforcement sensitive. Receiving agency personnel have been trained on proper use of law enforcement sensitive information and understand that they may only provide the information to those who have a need to know.

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 access to any record containing information that is part of a DHS system of records, or seeking to contest the accuracy of its content, may submit a Freedom of Information Act (FOIA) or Privacy Act (PA) request to DHS. Given the nature of some of the information in the NOC Patriot Report Database (sensitive law enforcement or intelligence information), DHS may not always permit the individual to gain access to or request amendment of his or her record. However, requests processed under the PA will also be processed under FOIA; requesters will always be given the benefit of the statute with the more liberal release requirements. The FOIA does not grant an absolute right to examine government documents; the FOIA establishes the right to request records and to receive a response to the request. Instructions for filing a FOIA or PA request are available at http://www.dhs.gov/xfoia/editorial_0316.shtm.

The FOIA/PA request must contain the following information: Full Name, current address, date and place of birth, telephone number, and email address (optional). Privacy Act requesters must either provide a notarized and signed request or sign the request pursuant to penalty of perjury, 28 U.S.C. §1746. Please refer to the DHS FOIA website for more information.

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

If an individual believes that he or she has suffered an adverse consequence that is related to the NOC Patriot Report Database, that individual will be able to provide any information that they deem relevant with a request that it be included within any record maintained in the NOC Patriot Report Database regarding a particular incident, activity, transaction, or occurrence. That correspondence will be directed to the NOC Fusion Desk, and a member of the watch will research the NOC Patriot Report Database to ascertain whether any record correlates to the information provided. If there is correlative information, the watch officer will enter the information provided into that record and indicate it as First-Party Amplifying information.

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

Mechanisms for correcting information are set forth above as well as in DHS/OPS-003 SORN.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: The privacy risk is that an individual may not be afforded adequate opportunity to correct information.

Mitigation: To mitigate this risk, individuals are afforded opportunity to request access or amendment of their records by either submitting a FOIA or a PA request as outlined above.

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?

Privacy protections include strict access controls, including passwords and real-time auditing that tracks access to electronic information. Authentication and role-based user access requirements ensure that users only can access or change information that is appropriate for their official duties. Background checks are conducted on users to ensure they are suitable for authorized access to the logs. The effectiveness of authentication and security protections are verified through audits of system operation and usage. DHS Employees may be subject to discipline and administrative action for unauthorized disclosure of this information.

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

All DHS employees and contractors are required to follow DHS Management Directive (MD) Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, May 11, 2004. This guidance controls the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information. All employees and contractors are required to follow Rules of Behavior contained in the DHS Sensitive Systems Handbook. Additionally, all DHS employees are required to take annual computer security training, which includes privacy training on appropriate use of sensitive data and proper security measures.

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

Privacy protections include strict access controls, including passwords and real-time auditing that tracks access to electronic information. Authentication and role-based user access requirements ensure that users only can access or change information that is appropriate for their official duties. Background checks are conducted on users to ensure they are suitable for authorized access to the logs. The effectiveness of authentication and security protections are verified through audits of system operation and usage. DHS Employees may be subject to discipline and administrative action for unauthorized disclosure of this information.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All MOUs are reviewed by the program manager, component Privacy Officer, and counsel and then sent to DHS for formal review.

Responsible Officials

Ashley Tyler, Program Manager

Department of Homeland Security

Office of Operations Coordination and Planning

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security