Privacy Impact Assessment
for the

National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative

DHS/NPPD/PIA-017(a)

August 12, 2011

Contact Point
Shawn Graff
Director, National Infrastructure Coordinating Center
Office of Infrastructure Protection
National Protection and Programs Directorate
(703) 235-3074

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

Abstract

The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) National Infrastructure Coordinating Center (NICC) is publishing this PIA to reflect activities under its Suspicious Activity Reporting (SAR) Initiative. The NICC SAR Initiative serves as a mechanism by which a report involving suspicious behavior related to an observed encounter or reported activity is received and evaluated to determine its potential nexus to terrorism. NICC is conducting this PIA because SAR occasionally contain personally identifiable information (PII) and NICC will be collecting and contributing SAR data for reporting and evaluation proceedings. DHS is updating this PIA to clarify that Redacted NICC Patriot Reports are reports that have been scrubbed of any identifiable information to include business and PII.

Overview

The National Infrastructure Coordinating Center (NICC) is the coordinating center within the Office of Infrastructure Protection (IP). The mission of IP is to lead the national effort to mitigate the terrorism risk, and to strengthen the protection of and enhance the all-hazard resilience of the Nation's critical infrastructure. In an effort to further its mission, IP has implemented the NICC SAR Initiative. All SARs are centered on activities, meaning that an event or action has occurred that has triggered some degree of suspicion. Under the NICC SAR Initiative, all suspicious activities are reported via email or phone to the NICC. It is important to note that the NICC SAR Initiative does not replace the Emergency First Responder services provided by calling 911.

When the NICC receives a SAR with a potential nexus to terrorism from the Critical Infrastructure and Key Resources (CIKR) community or the general public, the SAR information is used to create a NICC Patriot Report and a corresponding Redacted NICC Patriot Report, which is maintained on WebEOC. (These reports are distinct from DHS National Operations Center (NOC) Patriot Reports, which are maintained separately and are covered by the DHS NOC Patriot Report PIA.) The draft of the NICC Patriot Report is initially submitted to the FBI Counter Terrorism Desk for review and if the FBI approves the report and generates a Guardian[1] number, the NICC Patriot Report and Redacted NICC Patriot Report are created for distribution. The Redacted NICC Patriot Report, which has been scrubbed of any identifiable information to include business information and PII, is posted to HSIN-CS, a secure, real-time collaboration tool that allows DHS and the its private sector partners to work together. The NICC Patriot Report is submitted via email to the DHS Intelligence and Analysis, FBI, DOJ and the DHS NOC. Additionally, NICC Patriot Reports that meet the Information Sharing Environment

[1] The FBI Guardian System has SORN coverage provided under 63 FR 8659 titled, "Department of Justice Federal Bureau of Investigation – 002 Central Records System (CRS) System of Records," published on January 25, 2007. The PIA for the FBI Guardian System is not published, as this is a National Security System.

Functional Standard are submitted to the Department of Justice's Bureau of Justice Assistance sponsored Nationwide SAR Initiative for inclusion in the Shared Space. [2]

The NICC Patriot Report that is sent to the FBI is submitted to the FBI Counter-terrorism division. There, the FBI will determine whether there is sufficient information and cause to issue a Guardian number. If the NICC Patriot Report does not provide sufficient information, FBI will contact the NICC for amplifying information and then determine whether or not to issue a Guardian number. In addition, the FBI will make a determination as to whether to also send the report to the e-Guardian unclassified database,[3] pursuant to the authority of the FBI. Whether or not a Guardian number is issued, the NICC will disseminate the report in accordance with the below description.

Unlike the Guardian number, every SAR is issued a DHS NOC number once it is submitted to the DHS NOC. Once the Guardian and DHS NOC numbers are received, they will be included into the NICC Patriot Report, and the NICC will then distribute these finalized NICC Patriot Reports to FBI, DHS NOC, and DHS Intelligence and Analysis. Additionally, the Redacted version of the Patriot Report is posted to HSIN-CS. With the advent of the Nationwide Suspicious Activity Reports Initiative (NSI), DHS NICC will begin inputting those NICC SARs that meet the Information Sharing Environment Functional Standard into the DHS ISE SAR Server.

Within the NICC SAR Initiative, information reported is collected by authorized "Watch Standers." The NICC Watch Stander staff analyze all information in a manner that attempts to clarify and validate any reported facts as to its impact on Critical Infrastructure. NICC Watch Standers complete Personally Identifiable Information (PII), Protected Critical Infrastructure Information (PCII), and Chemical-Terrorism Vulnerability Information (CVI) training before becoming Watch-qualified. All Watch Standers are scheduled to complete necessary vetting training and must also maintain an active "secret" security clearance or higher. All reported information is collected from a variety of sources including Critical Infrastructure Stakeholders or the general public via email, fax or phone to NICC Watch Standers as it relates to suspicious activities, events or incidents. Information collected will include all suspicious activities that are observed, reported, and recorded in WebEOC and through the HSIN-CS portal. Information collected of the events, incidents, or suspicious activities reported can include contact information from the person that is reporting the suspicious activity, such as name, address, home phone, or work phone. This information is used to gather additional information about the activity witnessed.

[2] See DHS/ALL/PIA-032 DHS Information Sharing Environment Suspicious Activity Reporting Initiative.
[3] http://foia.fbi.gov/eguardian_threat.htm

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 Homeland Security Act of 2002 as codified within the United States Code at 6 U.S.C. § 321d(b)(1), Section 515 provides DHS with authority to collect the information. Additionally, specific legal authority for IP to operate is provided by under 6 USC § 121(d)(1), Directorate for Information Analysis and Infrastructure Protection.

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

Department of Homeland Security system of records titled, "Department of Homeland Security National Protection and Programs Directorate – 001 National Infrastructure Coordinating Center Records System of Records," published on November 15, 2010.

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

A system security plan has been completed with the Authority to Operate for the LENS systems, which was issued on September 9, 2009 and is valid for two years, as well as the Authority to Operate for the HSIN system, which was issued on March 31, 2009 and is valid for three years.

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

The NICC is working with the NPPD and DHS Records Officer to develop a NARA approved retention schedule, and DHS plans to propose a retention schedule of five years for SARs unless the record becomes part of an ongoing law enforcement investigation.

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.

The NICC SAR Initiative collects information through non-standardized email and phone reporting. Therefore, there are no PRA implications for this system.

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 NICC collects all reported information received via email or phone to NICC Watch Standers as it relates to suspicious activities, events or incidents.

SAR data may include, but is not limited to, 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 "Amplifying Information" section, based on the information provided by the submitter, provides a contextual narrative of the event and 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., driver's license number, passport, Social Security number, etc.) of the person(s) engaged and/or connected to the suspicious activity.

The NICC SAR Initiative 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 are the subject of information sent 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 is 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.

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

SARs are collected by the NICC through National Response Center (NRC) emails, NICC emails, HSIN-CS sector portals, fax and phone calls from CIKR community members witnessing suspicious activities. It is also possible private individuals and state local and local government officials to include law enforcement may submit information. As background, the primary function of the NRC is to serve as the sole national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment anywhere in the United States and its territories. In addition to gathering and distributing spill data for Federal On-Scene Coordinators and serving as the communications and operations center for the National Response Team, the NRC maintains agreements with a variety of federal entities to make additional notifications regarding incidents meeting established trigger criteria. The NRC also takes Terrorist/Suspicious Activity Reports and Maritime Security Breach Reports.

Reports are received by the NRC through their 800 number, online reporting tool and email. The NICC receives NRC reports as an email that is directly ingested into WebEOC. Additionally, PII is included in the NRC reports received by the NICC.

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 system does not use commercial or publically available data.

2.4 Discuss how accuracy of the data is ensured.

SAR data is collected and recorded "as is" by the NICC. Any action taken or based on any SAR data must be properly vetted and researched through appropriate channels (i.e., DHS NOC, FBI, etc.) once it has been disseminated by the NICC. The NICC does not vet SAR information, nor does the NICC cross reference or check information that has been received by the DHS NOC.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more PII than is needed for further analysis of the reporting will be collected and retained.

Mitigation: All information that is collected at the time of the reporting will be used to determine whether a potential SAR event is occurring. Thus, this privacy risk is inherent in the type of activity that is occurring under the NICC SAR Initiative. As further dissemination and analysis takes place after the NICC Patriot Report is generated with the information received, this privacy risk may be mitigated by the use of the additional PII to determine whether a viable SAR has been received.

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 NICC utilizes the information obtained in the SAR Initiative to report information related to terrorism-related threats and other criminal activities. This action enables law enforcement and intelligence analysts the opportunity to evaluate suspicious activity before an incident, providing another tool to combat terrorism. The NICC uses this information as a mechanism to share suspicious behavior reports relating to an observed encounter or reported activity with appropriate federal entities to evaluate its potential nexus to terrorism. It is important to note that the NICC SAR Initiative does not replace the Emergency First Responder services provided by calling 911.

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.

The NICC does not conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly prior to submitting a SAR in a NICC Patriot Report.

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

Information may be shared internally within DHS to those who demonstrate a need-to-know in the performance of their official duties. PII should only be shared

internally where the information received was for a purpose required by statue, executive order, or regulation (all other PII received will be managed in accordance with the requirements for this PIA).

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that SAR reports containing PII in connection with a report will be disseminated through the NICC Patriot Report and the PII will be transmitted to other components within the system with the potential to lead to unauthorized use of the PII.

Mitigation: This privacy risk is mitigated by the fact that both a Redacted and an Un-Redacted NICC Patriot Report are generated once a SAR is received. The Redacted NICC Patriot Report, which has been scrubbed of any identifiable information including business information and PII, is distributed by posting to HSIN-CS. The Un-Redacted NICC Patriot Report is disseminated internally to DHS and, externally to FBI and DOJ.

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.

This PIA serves as notice of the NICC SAR initiative. Notice of the initial collection of SAR data is provided through the DHS SORN titled, "Department of Homeland Security National Protection and Programs Directorate – 001 National Infrastructure Coordinating Center Records System of Records," published on November 15, 2010.

The NICC SAR Initiative is a voluntary submission of unsolicited information from the reporting individual to the NICC. The reporting individual may call or email the NICC of their own volition to submit SAR information, where it is collected for inclusion in a NICC Patriot Report.

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

Individuals who are the subject of a SAR are not provided the opportunity to consent to the use of their information. With SAR data, frequently the individual who is the subject of the SAR may not be aware that his information has been submitted to DHS.

For information about the individual submitting a SAR, the individual is given the opportunity to decline to provide their own information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware of the information collection that is occurring under the SAR program.

Mitigation: During law enforcement and intelligence activities, such notice may be counter-productive or simply impossible in the context of certain operations and investigations. Formal notice of this initiative is provided by this PIA. In addition, the SORN cited above provides notice that NICC within DHS collects and uses SAR data for their mission needs.

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.

SARs collected through the HSIN-CS or the LENS portal will be retained for a period of five years. HSIN-CS users will be required to change the status of their submissions from active to inactive if an incident is determined to have no nexus to terrorism.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that records containing PII collected under the SAR Initiative will be deemed to not qualify as suspicious activities after further investigation and analysis but will be retained in the system.

Mitigation: This privacy risk will be mitigated by the records retention schedules that are in place for the SAR Initiative. Given that most of the contained data reported is not PII, but is more focused on the nation's CIKR operational status, contemporary knowledge of incident and recovery planning indicate long periods of historical data is required to make good decisions on current events.

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.

When a SAR is submitted, the NICC will create a NICC Patriot Report and a corresponding Redacted NICC Patriot Report. The NICC will then disseminate the NICC Patriot Reports according to the appropriate protocols and as necessary (e.g., to FBI and DOJ.) NICC Patriot Reports that meet the Information Sharing Environment Functional Standard are submitted to the Nationwide SAR Initiative for inclusion in the Shared Space.

The NICC Watch uploads Redacted Patriot Reports, which have been scrubbed of any identifiable information including business information and PII, to HSIN-CS where Critical Infrastructure Stakeholders with access to HSIN-CS main page can access them.

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

The dissemination of NICC Patriot Reports will allow the NICC to collect and distribute infrastructure information related to all threats and all hazards, law enforcement activities, acts of terrorism, and other information collected or received.

Consistent with DHS's information sharing mission, information contained in the DHS/NPPD – 001 NICC Records System of Records may be shared with other DHS components, as well as appropriate agencies and entities. This sharing will only take place after DHS determines that the receiving component or agency has a verifiable need-to-know the information to carry out national security, law enforcement, immigration,

intelligence, or other functions consistent with Routine Use I set forth in this system of records notice.

6.3 Does the project place limitations on re-dissemination?

Yes. All NICC Patriot Reports contain the following statement at the bottom of the page:

> Third Agency dissemination of this report is prohibited without prior DHS approval. Please address requests for further distribution, questions, or comments to the NICC via telephone 202-282-9201 or email NICC@dhs.gov.

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

The NICC distributes SAR through email to a select group of recipient within the federal government. All emails from the NICC Watch are retained in the DHS email system in accordance with DHS retention policy.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that SAR containing PII outside the scope of the initial reporting will be disseminated outside the Department.

Mitigation: This privacy risk is mitigated by the fact that both a Redacted and an Un-Redacted NICC Patriot Report are generated by the NICC once a SAR is received. The Redacted NICC Patriot Report, which has been scrubbed of identifiable information including business information and PII, is disseminated to the larger authorized and pre-approved group with a need-to-know. The Un-Redacted NICC Patriot Report is disseminated to other agencies with investigative responsibilities pursuant to strict protocols and with a prohibition on further dissemination. NICC Watch Standers are required to take initial and recurring training to ensure proficiency with all NICC products and processes. Additionally, peer and leadership review is required for all product creation and dissemination.

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 information in the NICC SAR Initiative, DHS may not always permit the individual to gain access to or request amendment of his or her record.

The procedures for submitting FOIA requests are available in 6 C.F.R. Part 5. Please write to "FOIA, U.S. Department of Homeland Security, National Programs and Protection Directorate, Attn: FOIA Officer, Washington, D.C. 20528." You may also make informal inquiries to NPPD.FOIA@dhs.gov.

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

Given the nature and function of the NICC SAR Initiative, there are no procedures in place for the subject individual to correct inaccurate or erroneous information at the time of collection. If additional information is received relating to a particular incident, the re-submission process allows for the correction of inaccurate or additional information that may have been reported at the onset of the reporting.

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

If an individual feels that the information maintained in the SAR system is inaccurate, there will be two methods available to provide accurate information to the NICC. The DHS FOIA process (see Question 7.1) allows access to records. All communications received, regardless of method, will be entered into and remain on record within the SAR system pursuant to its general record retention schedule and will be subject to audit.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A major privacy risk relating to redress is that an individual may not be afforded adequate opportunity to correct information.

Mitigation: This privacy risk is mitigated by providing individuals the opportunity to submit any information they deem relevant to the SAR system. If an individual believes that he or she has suffered an adverse consequence related to the SAR system, 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 SAR system regarding a particular incident, activity, transaction, or occurrence.

The development of the SAR system and the processes governing its use include detailed consideration of the impact of erroneous data on individuals. Information in the SAR system is, by definition, raw information. The SAR system is simply a pool of un-vetted, reported "as is" information that is maintained in a manner making it accessible to appropriate official entities for further investigation and analysis predicated upon reasonable suspicion of a terrorism nexus.

Having verified and accurate information is the ultimate goal of the NICC, as well as all law enforcement, intelligence community, and other governmental officials using the system. The redress process referred to in Question 7.2, above, will help to ensure that the information is accurate. NICC Watch Standers will ensure the integrity of the SAR information based upon information provided by individuals, as well as any updates received from law enforcement and other government authorities.

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?

The NICC SAR Initiative serves as a mechanism by which a report involving suspicious behavior relating to an observed encounter or reported activity is received and evaluated to determine its potential nexus to terrorism. Once the information is collected, a NICC Patriot Report is created and transmitted to the FBI for further analysis and dissemination. Given its role, the NICC SAR Initiative does not analyze the submissions received. Rather, the transmission to the FBI allows for auditing of the information to be completed at the next level. Thus, the NICC SAR Initiative solely serves as a repository

for the collection of information and no auditing mechanisms are in place to verify the information collection at this stage.

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

All DHS employees are required to take annual computer security training, which includes privacy training on appropriate uses of sensitive data and proper security measures. In addition, all Watch Standers must complete PII, PCII and CVI training before becoming Watch-qualified to access the data.

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

Access to records in maintained through password protections and tiered access to the information that is contained within the system. In addition, all Watch Standers must complete PII, PCII and CVI training before becoming Watch qualified to access the data. Further, all Watch Standers are scheduled to complete vetting training, and must maintain an active "Secret" security clearance or higher. Also, authentication and role-based user access requirements ensure that users can only access or change information that is appropriate for their official duties.

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

Shawn Graff
Director, National Infrastructure Coordinating Center
Office of Infrastructure Protection
National Protection and Programs Directorate

Approval Signature

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security