Privacy Impact Assessment
for the

National Operations Center Operations Counterterrorism Desk (NCOD) Database

DHS/OPS/PIA-009

July 30, 2012

<u>Point of Contact</u>
Ben Jacob

National Operations Center Counterterrorism Operations Desk (NCOD)
Office of Operations Coordination and Planning

202-282-8000

<u>Reviewing Official</u>
Mary Ellen Callahan
Chief Privacy Officer

Department of Homeland Security
202-343-1717

Abstract

The National Operations Center (NOC), within the Office of Operations Coordination and Planning (OPS), operates the NOC Counterterrorism Operations Desk (NCOD) and serves as the primary DHS point of contact to streamline counterterrorism Requests for Information (RFIs). The NCOD Database is a tracking tool used by NCOD Officers to track all counterterrorism related incoming and outgoing inquiries. OPS has conducted this Privacy Impact Assessment (PIA) because the NCOD Database contains personally identifiable information (PII).

Overview

OPS fulfills a unique response and facilitation role within the Department by serving as the bridge for sharing critical information between DHS Components, across the interagency community, and among homeland security partners. OPS planning activities provide a means of integrating government-wide activities in preparation for future incidents. Finally, OPS continuity activities allow for the continuation of essential government functions in the event of a catastrophic crisis.

In 2006, the National Operations Center (NOC) was created, and in its current capacity serves as the primary national-level hub for domestic situational awareness by fusing law enforcement, intelligence, emergency response, private sector, and open-source reporting. The unique mission of the NOC includes not only domestic situational awareness, but also the establishment and maintenance of a 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 all domestic situational awareness and facilitates information sharing and operational coordination with other federal, state, local, tribal, non-governmental operation centers, and the private sector.

National Counterterrorism Operations Desk (NCOD)

In fulfillment of the NOC's mission to fuse law enforcement, intelligence, emergency response, private sector, and open-source reporting, the NCOD was established within the NOC to serve as a single point of contact for all RFIs concerning counterterrorism from partner agencies. The NCOD serves as a single DHS point of contact, allows desk officers to provide unique reporting capabilities, and quickly responds to the requesting agency with results, and tracks the incoming and outgoing RFIs in the NCOD Database.

The NCOD allows the Department to provide twenty-four hour, 365 days a year support to DHS counterterrorism mission partners across the federal government. Counterterrorism RFIs are time sensitive and require an immediate response from NCOD Officers. The primary purposes of the NCOD are to:

- Coordinate appropriate DHS database checks;
- Streamline data exchange between DHS databases and other federal agency databases;
- Establish one location to track and direct incoming and outgoing RFIs;
- Operate as part of the NOC Watch;

- Serve as an extension of the DHS OPS CT Section;
- Provide communication to DHS Components for information clarification;
- Coordinate information collection and exchange;
- Lead and integrate DHS domains strategic-level, operations coordination and planning functions; and
- Ensure the incoming and outgoing RFIs are facilitated for a response to the responsible office in a timely manner.

NCOD RFIs

The NCOD receives and validates RFIs from other federal agencies. RFIs handled by the NCOD encompass all requests for information related to known or suspected terrorist (KST).

Prior to conducting any research, the NCOD officer must validate the RFI to ensure that the request falls into one of the three categories mentioned above and presents sufficient specificity. If the RFI meets this standard, NCOD officer will conduct the research and review the totality of information before responding to the RFI. The totality of information is evaluated based on the experience of the reviewer, requesting agency, facts, RFI context, and rational inferences that may be drawn from the information in the RFI. The validation process ensures that: (1) a RFI falls within the Department's authorities; (2) a RFI does not violate existing policies governing operational information sharing or the dissemination of controlled information;[1] (3) if the requestor is from within DHS he/she possesses a valid "need to know" and if the requestor is from outside that the request meets requirements of the Privacy Act. Requests not meeting the validation criteria will be returned to the requestor for additional clarification or justification. The results of the RFI, and the information subsequently logged into the NCOD Database tracking tool, which will record source system disclosures.

Once an RFI is received and validated, the NCOD officer will log the fact of the request into the NCOD Database, to include contact information about the requestor. The NCOD officer will then conduct a series of checks against government unclassified Law Enforcement Sensitive (LES), Sensitive Security Information (SSI), and For Official Use Only (FOUO) systems to determine if DHS has any information regarding the subject of the RFI. Any positive results retrieved from DHS LES/SSI/FOUO databases will be summarized and redundant information removed. If conflicting information is received, the NCOD officer may reach back to DHS components, as owners of the source data, for information clarification. The final response to the request will also be maintained in the NCOD Database.

Resulting information will then be entered into a standard reporting form which is encrypted and sent back to the requesting agency via secure email. The encrypted forms are assigned a tracking number, which is stored in the NCOD Database. The forms are stored in a secure folder on a secure server at the NOC. The NCOD Database establishes one location to track and direct incoming and outgoing RFIs, thereby streamlining data exchange between DHS and other federal agencies. Information stored in the

[1] (FOUO) **Disclosure of Violence Against Women Act (VAWA), T, and U immigration information**. The NCOD shall not disclose to anyone (other than a sworn officer or employee of the Department, or component thereof, for legitimate Department, bureau, or agency purposes) any information which relates to an alien who is the beneficiary of an application for relief under 8 U.S.C. § 1101(a)(15)(T) [T classification], (U) [U classification], or 8 U.S.C. § 1229b(b)((2) [VAWA, i.e., battered spouse or child].

NCOD Database can be searched by any of the data fields collected as part of fulfilling the RFI such as: subject name, nationality, alien number, date processed, name of requesting agency. The NCOD officer would conduct such searches in response to an RFI to determine whether it previously provided the requested information. In addition, the NCOD will provide monthly organic database disclosures to components that require such disclosures.

NCOD Database

The NCOD database will maintain the agency contact information for the RFI, the RFI, and the response to the RFI. The response will include the relevant information from the government systems and indicating of source of the systems.

Categories of information contained in the NCOD database may include, but are not limited to, the following: name(s), date of birth, immigration status, gender, place of birth, country of citizenship, alien registration number, passport number, Social Security number, driver’s license number, any additional numbering system used by governments to identify individuals, warrant number, I-94 number, Student and Exchange Visitor Information System (SEVIS) number, visa number, cédula number (foreign government issued national identification card), Canadian social insurance number, Federal Aviation Administration (FAA) license number, mariner’s document, birth certificate number, naturalization certificate number, work permit number, residency permit number, immigration history, military identification number, license plate information, vehicle information, physical descriptions such as scars, marks and tattoos, occupation(s), employer(s), addresses, telephone numbers, email addresses, FBI Number, DHS Fingerprint Identification Number (DHS FIN), facial photographs, fingerprints, iris images, financial information, criminal history, NOC tracking number, requesting agency name, and travel information.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

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.” Additional legal authorities for OPS include: the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002); the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007) (codified in various sections of the U.S.C.); the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004) (codified in various sections of U.S.C.); the National Security Act of 1947, as amended; and 5 U.S.C. Section 301; and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*.

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

The NCOD Database's tracking functions and responses to RFIs are covered by the DHS/OPS–003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN. The component source data which is searched by the NCOD Officers is covered by the individual SORNs for the underlying government systems performing the original collection.

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

The NCOD Database will reside on the DHS unclassified network which has a security authorization. The Database will become operational upon signing of this PIA.

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

Yes. The records are covered under NARA/OPS records schedule N1-563-08-023 and have a five (5) year retention schedule.

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 information maintained by the NCOD is not covered by the Paperwork Reduction Act because no information is collected directly from the public.

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 NCOD Database does not collect information directly from the public. The NCOD Database tracks the RFIs coming into the NCOD, the responses being returned to the requesters, the requesting agency's contact information, and the tracking numbers assigned to the RFIs. These tracking numbers are linked back to the finished reports that are sent to the requesting agencies.

The NCOD officers perform searches and access information collected and maintained in DHS and other government systems, but only enter information into the NCOD Database that is related to the RFI being processed.

NCOD will respond to RFIs that encompass requests for information related to KSTs. All NCOD searches and name checks must have a nexus to either terrorism or national security. Persons included in the NCOD reports in response to RFIs may include: individuals known or suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and /or terrorist activities,[2]; individuals who are the subjects of law enforcement investigations into violations of U.S. laws, as well as other laws and regulations within DHS' jurisdiction, including investigations led by other domestic agencies where DHS is providing support and assistance; fugitives with outstanding Federal or State warrants. Information may be returned from any/all of the DHS component unclassified Law Enforcement Sensitive (LES), Sensitive Security Information (SSI) and For Official Use Only (FOUO) databases. Any positive results retrieved from DHS LES/SSI/FOUO databases will be summarized and redundant information removed.

Categories of information collected may include, but are not limited to, the following: name(s); date of birth; immigration status; gender; place of birth; country of citizenship; ; alien registration number; passport number; Social Security number; driver's license number; any additional numbering system used by governments to identify individuals; warrant number; I-94 number; Student and Exchange Visitor Information System (SEVIS) number; visa number; cédula number (government issued national identification card); Canadian social insurance number; Federal Aviation Administration (FAA) license number; mariner's document; birth certificate number; naturalization certificate number; work permit number; residency permit number; military identification number; license plate information; vehicle information; physical descriptions such as scars, marks and tattoos; occupation(s); employer(s); addresses; telephone numbers; email addresses; FBI case number; DHS Fingerprint Identification Number (DHS FIN); facial photographs; fingerprints; iris images; financial information; and travel information.

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

The NCOD Database does not collect information directly from individuals, but rather accesses information collected, generated, and stored by and in other source systems. Information is collected from these systems via manual search the NCOD officer. The search results are then manually entered into the reporting form, which is stored on a secure server at the NOC. The reporting form is issued a tracking number which is stored in the NCOD Database. .

The data used to populate the NCOD reporting form is retrieved from the following source systems, detailed further in the Appendix: ENFORCE (ICE's Enforcement Case Tracking System), IDENT (US-VISIT's Automated Biometric Identification System), ADIS (Arrival/Departure Information System), APIS (Advance Passenger Information System), ATS-P/N/L (Automated Targeting System Passenger/Inbound Cargo), CCD (Department of State's Consolidated Consular Database), CIS (USCIS' Central Index System), CLAIMS 3 and 4 (USCIS' Computer-Linked Application Information Management System), RAPS (Refugee, Asylum, and Parole System), SEVIS (Student Exchange Visitor Information System), IAFIS/JABS (FBI's Integrated Agency Fingerprint Identification System/Joint

[2] Id (defining "suspected terrorist").

Agency Booking System), CPIC (Canadian Police Information Centre), NSEERS (National Security Entry/Exit Registration System), TECS , and Person Centric Query Service (PCQS).

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 NCOD Officers do not rely on commercial or publicly available data when fulfilling RFIs.

2.4 Discuss how accuracy of the data is ensured.

Because NCOD does not collect information directly from the public or any other primary source, it relies on the system(s) performing the original collection to provide accurate data. NCOD Officers will use a variety of data sources available through the source systems to verify and correlate the available information to the greatest extent possible. During an RFI, any positive results retrieved from DHS LES/SSI/FOUO databases will be summarized and redundant information removed. If conflicting information is received, the NCOD officer may reach back to DHS components, as owners of the source data, for information clarification.

In order to determine if reported information has a possible nexus to terrorism, NCOD Officers have extensive training and experience with the application of counterterrorism laws, regulations, and policies to properly vet information for credibility and accuracy. NCOD officers, based on education, training, and experience consider the originating requesting agency's counterterrorism mission and evaluate the nature, scope, timeliness, and context of the information that generated the requestor's RFI.

2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

In addition to the risks accumulated by the underlying systems which NCOD Officers access the following risks related to NCOD's collection of data have been identified:

<u>Privacy Risk</u>: Because NCOD compiles data from multiple systems, the collection of the information may not be consistent with the original program's purpose.

<u>Mitigation</u>: NCOD Officers access information from border security and immigration benefit systems that share purposes compatible with its counterterrorism mission. Prior to responding to an RFI, NCOD Officers, in conjunction with OPS/CT to determine if the RFI is "suitable for support." To be assessed suitable for support, (1) the RFI must be made in furtherance of a lawful governmental function, and (2) reasonable belief must exist that the request relates to a known or suspected terrorist or Homeland security threat. If the RFI is not suitable for support, consistent with NCOD's counterterrorism mission, it will not be fulfilled.

<u>Privacy Risk</u>: Since NCOD relies upon DHS-owned and other federal agency data instead of collecting directly from individuals, there is a risk that the data in NCOD will become inaccurate.

<u>Mitigation</u>: Information responding to RFIs that include information about individuals are stored in the NCOD Database and includes the source of the data that provided the response. Due to the time sensitive nature of counterterrorism inquiries, the NCOD Officers must rely on the most accurate, up-to-date information available. Therefore, they conduct a new search of the source data systems for each RFI. They do not rely on previously reported information contained in final reports previously. This ensures that the new report rely on the most accurate and timely information available in the source systems.

Privacy Risk: Because NCOD compiles data from multiple systems, users will access information from several systems that previously was not accessible in a single system. The information compiled is not necessarily indicative of illegal activity.

Mitigation: Responses to an RFI may only contain information that appropriate responses to the request. The supervisory will review the response prior to sending the response back to a requester to ensure that the analysis and conclusions of the product or response are germane to the purpose for which the product or response was intended.

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.

Information collected and maintained by the NCOD Database is used to facilitate and track incoming and outgoing RFIs from counterterrorism mission partners and to track the subsequent response reports from the NCOD. Tracking numbers are assigned by date to assist NCOD Officers in determining which RFIs have already been answered, and to determine a workflow priority. The tracking numbers also link the finished reports that are saved on the secure shared drive with their corresponding RFI.

Underlying source information from the different government databases is used by the NCOD Officers to draft and compile their final reports back to the requesting partner agency. Each RFI requires a new source database search by the NCOD Officer, to ensure that the information contained in the final report is the most accurate, relevant, and timely. The information compiled into reports may include any encounter data (such as border crossing or immigration benefit application), or biometric and biographic data on the record subject of the RFI.

The NCOD Database is critical tool for the NCOD Officers to streamline data exchange between DHS databases and other federal agency databases. The NCOD Database establishes one location to track and direct incoming and outgoing. RFIs, and allows the NCOD Officers to lead and integrate DHS domains strategic-level, operations coordination, and planning functions (e.g., database searching, all domain awareness, assessments, information sharing, situational awareness, common operating picture, contingency planning, etc.). The NCOD officer would search the NCOD Database in response to an RFI to determine whether it previously provided the requested information. In addition, the NCOD will provide monthly organic database disclosures to components that require such disclosures.

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.

NCOD does not utilize pattern-based search technologies. All searches are done manually.

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

No, only NCOD Officers physically located in the NOC are granted access to the NCOD Database.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that the final reports may be submitted to partner agencies about individuals who do not have a sufficient nexus to terrorism.

Mitigation: Consistent with NCOD's counterterrorism mission, it may only respond to RFIs for counterterrorism-related purposes. All RFIs must be determined "suitable for support." To be assessed suitable for support, (1) the RFI must be made in furtherance of a lawful governmental function, and (2) reasonable belief must exist that the RFI relates to a known or suspected terrorist or Homeland security threat. The NCOD will only release information in reports back to requesting agencies that have a reasonable belief that the RFI relates to a KST.

Privacy Risk: There is a privacy risk of misuse or unauthorized access to the information. Authorized users of NCOD could utilize their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation: To mitigate this risk, access to data in the NCOD 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. Unauthorized use of the NCOD Database may result in the suspension of a user's access depending upon the nature and scope of the unauthorized use. Further, the NCOD is located in a Sensitive Compartmented Information Facility (SCIF).

It is the policy of the U.S. government that employees and contractors have no privacy expectations associated with the use of any DHS network, system, or application. This policy is in full effect for NCOD. Audit trails are created throughout the process and are reviewed if a problem or concern arises regarding the use or misuse of the information. When a user goes through the log-in process, he must acknowledge the consent to monitoring or he cannot use the system.

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.

The NCOD does not directly collect information from individuals, and therefore does not have the opportunity to provide notice of such collection. The NCOD receives information collected in other databases, some of which is collected directly from individuals. This PIA serves as public notice of the existence, contents, and uses of the NCOD Database. Notice of collection by the underlying government systems performing the original collection is described in the individual PIAs and SORNs for those systems. Individuals are provided notice via Privacy Act Statements at the original points of collection, as well as the published Systems of Records Notices for the underlying systems, which state that their information may be shared with law enforcement entities. As part of this PIA process, DHS reviewed the applicable SORNs to ensure that the uses were appropriate given the notice provided. Direct notice to the individual at the time of the RFI search would undermine the law enforcement mission.

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

The NCOD does not collect information directly from individuals. As such, there are no opportunities for NCOD to seek consent to uses or for individuals to decline to provide information or opt out of the project. NCOD relies on the underlying systems from which it draws information to provide opportunities to individuals from which this information is collected. Additionally, many of the government systems from which NCOD draws information are law enforcement systems that collect information that individuals are required to provide by statutory mandate, therefore these individuals do not have an opportunity to decline to provide the required information, opt out, or to consent to uses.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: NCOD does not collect information directly from the public, so individuals do not have notice that their information may be used by NCOD.

Mitigation: Public notice is provided through this PIA and the corresponding SORN, DHS/OPS-003. In addition, individuals are notified at the point of collection of the original data that their information may be shared for law enforcement purposes. Notice is not provided by NCOD at the point of collection from the underlying source systems since the information is used for a law enforcement or counterterrorism purpose, and providing notice to record subjects may compromise pending investigations.

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.

The records are retained under NARA/OPS records schedule N1-563-08-023 and have a seven (7) year retention schedule. However, OPS is working with NARA to modify the records retention schedule to 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 risk of retaining information longer than is necessary for any specific RFI or research project.

Mitigation: In order to reduce the risk of maintaining information that is no longer accurate, NCOD is reducing the length of time it is retaining information from 7 years to 5 years. Although there is always risk inherent in retaining PII for any length of time, the data retention period for the NCOD 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 governments, 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.

Yes, the primary mission of the NCOD is the serve as the primary point of contact for other agency counterterrorism partners to file RFIs with DHS. The NCOD shares the results of these RFIs with the requesting agencies. Results of the RFIs are shared in the form of final, encrypted reports that are sent via secure email from the NCOD to the requesting agency. These reports are used by the requesting agencies in the furtherance of law enforcement investigations pertaining to terrorism.

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

The sharing of PII outside of the Department is compatible with the original collections listed in the System of Records Notices of the underlying systems. Generally, information is shared for law enforcement, intelligence, and/or national security purposes and with contractors working for the federal government to accomplish agency functions related to the system of records.

Routine uses of DHS/OPS-003 SORN allows OPS to share information with federal, state, or local agency, or other appropriate entities or individuals, through established liaison channels for counterintelligence or antiterrorism purposes.

This sharing is conducted pursuant to routine use "I" of the DHS/OPS-003 SORN, which states that DHS may share information with "a federal, state, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence" and routine use "K" of the DHS/OPS-003 SORN, "To federal and foreign government intelligence or counterterrorism agencies or state, local, tribal or territorial components where the information is or may be terrorism-related information and such use is to assist in anti-terrorism efforts."

6.3 Does the project place limitations on re-dissemination?

NCOD Officers will utilize the processes and procedures already established within DHS and OPS with regard to dissemination of data and information internally within DHS and external to the Department. Users will follow the Third Agency Rule, which mandates that prior to sharing information or data to a third agency (not involved in the original sharing agreement) the agency that intends to share will acquire consent from the agency that provided the data or information. Only individuals with a need to know will be able to gain access to the final encrypted reports produced by the NCOD Officer. Only members of the NCOD have access to the NCOD Database and the final reports on the secure shared drive.

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

An electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom it is disclosed is kept in the Database. Underlying source databases are responsible for tracking disclosures from their own systems, but the NCOD Database does keep a record of all databases that were queried in response to an RFI. The organic database owners audit their systems. The NCOD Database will contain the source databases used to respond to RFIs. A record of the database that was queried would be contained in the NCOD Database. The NCOD Database can be audited.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: When the NOC distributes an NCOD 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.

NCOD Reports will be shared with the requesting organization. No external organizations have direct access to the NCOD 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.

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 NCOD 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 with non-exempt records. Instructions for filing a FOIA or PA request are available at http://www.dhs.gov/foia.

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 NCOD 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 NCOD Database regarding a particular incident, activity, transaction, or occurrence. That correspondence will be directed to the NOC, and a member of the watch will research the NCOD 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 75 Fed. Reg. 69689 (November 15, 2010).

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: 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information,* January 6, 2005. 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, OPS Privacy Officer, OPS counsel and then sent to the DHS Office of the General Counsel and Chief Privacy Officer for formal review.

Responsible Officials

Don Triner

Department of Homeland Security

Approval Signature

____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Source Databases for NCOD Queries:

ENFORCE (Enforcement Case Tracking System). ENFORCE is an Immigration and Customs Enforcement (ICE) system that was created to identify and track aliens who were repeatedly apprehended attempting to enter the United States illegally. The system is also used to identify apprehended aliens who are suspected of criminal activity, have outstanding arrest warrants, or who have been previously deported. ENFORCE is linked to the FBI fingerprint database through Integrated Automated Fingerprint Identification System and is currently available to CBP and ICE personnel in the field. (SORN DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274, PIA DHS/ICE/PIA-015 Enforcement Integrated Database (EID) January 14, 2010 *(PDF, 29 pages – 420.65 KB)*

IDENT (US-VISIT's Automated Biometric Identification System). United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Secondary Inspection Tool (SIT). IDENT was created as a biometric identification system to enhance security for citizens and visitors while facilitating travel and trade across the U.S. borders. In many cases, US-VISIT begins overseas at U.S. consular offices where visitors' biometrics, digital fingerprints, and photographs are collected and checked against a database of known criminals and suspected terrorists. When the visitor applies for admission at a U.S. port of entry, the same biometrics are collected to match the person applying for admission with the individual who received the visa at the consular office. The biometrics are again checked against a database of criminals and suspected terrorists. US-VISIT technology is in place at all air, sea, and major land ports of entry. US-VISIT currently applies to all persons other than U.S. citizens and Lawful Permanent Residents, with limited exemptions. (SORN DHS/USVISIT-0012 - DHS Automated Biometric Identification System (IDENT) June 5, 2007, 72 FR 31080, PIA DHS/NPPD/USVISIT/PIA-002 US VISIT, IDENT, July 31, 2006 *(PDF, 16 pages – 236 KB)*

ADIS (Arrival/Departure Information System). ADIS was introduced as a new automated system, which captures Form I-94 arrival and departure data electronically at ports of entry and uploads this information into TECS. The stored data includes names, dates of birth, destination address, visa category, and flight information. This data assists the CBP officer in facilitating the inspection process, and is extremely useful in determining any future admissibility issues. This database is available to TECS users. (SORN DHS/USVISIT-001 - Arrival and Departure Information System (ADIS) August 22, 2007, 72 FR 47057, PIA DHS/NPPD/USVISIT/PIA-005(a) Arrival and Departure System (ADIS)APIS (Advance Passenger Information System). APIS was established to enable commercial airline and vessel operators to provide passenger manifests to CBP prior to a conveyance's arrival in the United States. APIS enhances border security in that all manifest data is screened against the IBIS databases to identify mala fide passengers and crew members before their arrival at a port of entry. APIS data is currently available to CBP personnel at air and sea ports of entry. (SORN DHS/CBP-005 - Advance

Passenger Information System (APIS) November 18, 2008, 73 FR 68435, Final Rule for Privacy Act Exemptions November 18, 2008 73 FR 68291, PIA DHS/CBP/PIA-001(e) Advanced Passenger Information System (APIS) Update National Counter Terrorism Center (NCTC), June 23, 2011(*PDF, 7 pages – 183.57KB*))

ATS-P/N/L (Automated Targeting System Passenger/Inbound Cargo). The ATS is a computer-based system used to target high-risk passengers and cargo shipments. The system combines information from APIS, Limited Passenger Name Record (PNR), I-94 data, visa information, border crossing history, secondary referral comments, refusal comments, suspect and violator indices (SAVI), and/or cargo shipping history and runs these elements against a set of criteria developed by subject matter experts to identify potential high-risk targets, trends, and patterns. The system is available at all CBP ports of entry. (SORN DHS/CBP-006 - Automated Targeting System August 6, 2007, 72 FR 43650 , Final Rule for Privacy Act Exemptions February 3, 2010 75 FR 5487, Response to Public Comments *(PDF, 23 pages - 590 KB)*, PIA DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012 *(PDF, 40 pages - 22.97 MB)*

CIS (Central Index System). CIS is a computerized indexing system that contains personal identification data such as the A-File number, name, date and place of birth, date and port of entry, as well as the location of each official hard copy paper file known as the individual's "A-file." The data may also contain naturalization information including certificate number, date of naturalization, and court of naturalization. CIS is available to CBP, ICE, and USCIS officers. (SORN DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records June 13, 2011, 76 FR 34233, PIA DHS/USCIS/PIA-009 USCIS Central Index System, June 22, 2007, *(PDF, 23 pages - 240 KB)*

CLAIMS 3 and 4 (Computer-Linked Application Information Management System). CLAIMS was created by the Immigration and Naturalization Service (INS) as an application processing and storage database that includes biographic information on individuals who have filed applications for benefits under the INA and those who have submitted fee payments with such applications or petitions. It also includes biographic information on individuals who have paid fees for access to records under the Freedom of Information/Privacy Acts (FOIA/PA). Records in the system may also include such information as the date documents were filed or received, application or petition status, location of a record, FOIA/PA or other control number when applicable, and fee receipt data. At the ports of entry, CBP has access to CLAIMS through TECS for viewing records. (SORNs DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records June 13, 2011, 76 FR 34233 ,DHS-USCIS-003 – Biometric Storage System April 6, 2007 72 FR 17172 ,DHS-USCIS-007 - Benefits Information System September 29, 2008 73 FR 56596 ,DHS-USCIS-011 – E-Verify Program System of Records May 9, 2011 76 FR 26738, PIA DHS/USCIS/PIA-010(e) Person Centric Query Service Supporting Immigration Status Verifiers of the USCIS Enterprise Service Directorate/Verification Division Update June 8, 2011 *(PDF, 9 pages – 191KB)*

Consolidated Consular Database (CCD). CCD is a Department of State (DOS) web-based database, which feeds the Automated Targeting System-Passenger that is linked to the Consular Lookout and Support System. CCD contains electronic immigrant and nonimmigrant visa application and U.S. passport information and U.S. passport, including biometric and biographic details. (PIA Consular Consolidated Database (CCD) Privacy Impact Assessment (PIA) March 22, 2010 http://www.state.gov/documents/organization/93772.pdf)

DHS Pattern and Information Collection Sharing System, (DPICS2). DPICS2 is a toolset that assists ICE law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations that are indicative of violations of the customs and immigration laws as well as possible terrorist threats and plots. (SORN ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service December 15, 2011, PIA DHS/ICE/PIA-004(a) ICE Pattern Analysis and Information Collection (ICEPIC) Update, October 26, 2011 *(PDF, 14 pages - 241 KB)*

ICE Intelligence Fusion System (IFS). IFS is a large data repository that provides search and analysis capabilities to DHS personnel responsible for enforcing or administering the customs, immigration, and other laws within the DHS mission. (SORN DHS/ICE-006 - ICE Intelligence Records System (IIRS) March 1, 2010, 75 FR 9233, PIA DHS/ICE-PIA-007 Law Enforcement Intelligence Fusion System (IFS) November 17, 2008 (*PDF, 20 Pages - 203 KB*)

RAPS (Refugee, Asylum, and Parole System). This system was designed to automate the tracking of asylum applicants, control refugee and asylum applications, and make the adjudication process more efficient. USCIS administers this system; currently, it is not accessible by CBP at the ports of entry. (SORN DHS/USCIS/PIA-027(a) Refugees, Asylum, and Parole System and the Asylum Pre-Screening System Update National Counter Terrorism Center (NCTC), June 30, 2011 *(PDF, 6 pages - 156 KB)*, PIA DHS/USCIS-010 - Asylum Information and Pre-Screening January 5, 2010 75 FR 409)

SEVIS (Student Exchange Visitor Information System). SEVIS is an automated database where foreign student information is warehoused. CBP, ICE, and USCIS officers can verify student history, attendance records, and current student status. SEVIS is available to NCOD Officers through TECS access. (SORN DHS/ICE001 - Student and Exchange Visitor Information System January 5, 2010, 75 FR 412, PIA DHS/ICE/PIA-001(a) Student and Exchange Visitor Information System (SEVIS) Update National Counter Terrorism Center (NCTC), June 23, 2011 (*PDF, 6 pages - 167 KB*)IAFIS/JABS – (Integrated Agency Fingerprint Identification System / Joint Agency Booking System). IAFIS/JABS is an FBI owned, automated fingerprint identification system used throughout CBP at ports of entry, Border Patrol stations, and ICE units which interface with ENFORCE and the FBI fingerprint analysis system. Response by the FBI is available every day and at all hours with associated information on criminal histories, arrest records and outstanding warrants. This system is designed to provide a coherent, unified approach to biometric identification of criminal violators and applicants for benefits. (PIA The *Joint Automated Booking System* (JABS) http://www.justice.gov/jmd/pia/jabs_privacy_impact_assessment_jan2102.pdf)

CPIC (Canadian Police Information Centre). CPIC is a Canadian database containing arrest records and criminal histories on Canadian violators. This system is available to CBP and ICE officers though an interface with TECS. (PIA http://www.cpic-cipc.ca/English/cpicpia.cfm)

Historical data associated with the NSEERS (National Security Entry/Exit Registration System) Program. NSEERS is a registration system for nationals of certain countries who arrive at or depart from a port of entry, or who are in the United States legally on a long-term basis, e.g., a student who is a national of a special interest country. Aliens from countries whose registration is mandated have their fingerprints and photographs taken digitally and comprehensive biographical data is captured. Failure to properly register may be grounds for a refusal of admission on subsequent visits to the United States. NSEERS violators normally have lookout records entered in TECS to alert CBP, USCIS, and ICE personnel regarding the alien's noncompliance. (SORN DHS/CBP-005 - Advance Passenger Information System (APIS) November 18, 2008, 73 FR 68435, Final Rule for Privacy Act Exemptions November 18, 2008 73 FR 68291, PIA DHS/CBP/PIA-001(e) Advanced Passenger Information System (APIS) Update National Counter Terrorism Center (NCTC), June 23, 2011(*PDF, 7 pages – 183.57KB*))

CBP TECS – TECS is a computerized information system designed to identify individuals and businesses is violation of federal laws. It is also a communications system permitting message transmittal between Treasury, and other national, state and local law enforcement agencies. (SORN DHS/CBP-011 - U.S. Customs and Border Protection TECS December 19, 2008 73 FR 77778 ,Final Rule for Privacy Act Exemptions August 31, 2009 74 FR 45072, PIA DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing December 22, 2010 *(PDF, 28 pages – 330 KB)*

USCIS Person Centric Query Service (PCQS).The PCQS System provides users with the ability to search multiple systems for persons from a centralized location. Users can perform searches by Name with Date of Birth, Alien Number, Receipt Number, Social Security Number (SSN), I-94 Number, SEVIS ID, Visa Control Number, Card Serial Number, Encounter ID, Enumerator, TECS Record ID, and Naturalization Citizenship Certificate Number. Only systems that support a particular type of search will be available when that type of search is selected. Systems that do not support the chosen search type will be grayed out. When searching against multiple sources, users have the ability to see the data returned from each source and perform comparisons. (SORNs DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records June 13, 2011, 76 FR 34233 ,DHS-USCIS-003 – Biometric Storage System April 6, 2007 72 FR 17172 ,DHS-USCIS-007 - Benefits Information System September 29, 2008 73 FR 56596 ,DHS-USCIS-011 – E-Verify Program System of Records May 9, 2011 76 FR 26738, PIA DHS/USCIS/PIA-010(e) Person Centric Query Service Supporting Immigration Status Verifiers of the USCIS Enterprise Service Directorate/Verification Division Update June 8, 2011 *(PDF, 9 pages – 191KB)*