Privacy Impact Assessment
for the

National Operations Center Tracker and Senior Watch Officer Logs

February 3, 2011

Contact Point
Donald Triner
DHS National Operations Center
Office of Operations Coordination and Planning
202-282-8611

Reviewing Official
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 Tracker Log and the Senior Watch Officer (SWO) Log. The SWO Log is a synopsis of all significant information received and actions taken during a shift by the SWO. The NOC Tracker Log is a repository of all NOC responses to threats or incidents and significant activities that require a NOC tracking number. OPS has conducted this privacy impact assessment (PIA) because both the SWO Log and NOC Tracker Log may contain personally identifiable information (PII) associated with an administrative note or a watch desk Request for Information (RFI).

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.

The primary role of the SWO and the watch desks is to provide situational awareness and a common operating picture for the entire federal government, state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other man-made disaster; and ensure that critical terrorism and disaster-related information reaches government decision-makers. The NOC accomplishes this by keeping track of major events through both the SWO and NOC Tracker Logs and issuing situation reports, situation updates, and/or responding to requests for information (RFIs).

The SWO Log is a synopsis of all significant information received and actions taken by the SWO during the shift. The NOC Tracker Log provides further details on the items listed in the SWO Log; it is the underlying cumulative repository of responses to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters as well as RFIs that require a NOC tracking number. NOC numbers are assigned for the purpose of tying together the high volume of information, requests and responses for information and data collection relevant to discreet events and issues within the NOC. The NOC number makes that information easily accessible in an organized form should a future event benefit from previously gathered information. Examples of the types of issues that receive a NOC tracking number include, but are not limited to: Name Traces, Patriot Reports, RFIs, Committee on Foreign Investment in the U.S. (CFIUS) requests, CDC/HHS Data Request and the removal/addition to the "Do Not Board and or Lookout List" (DNB/LO). The SWO will also assign NOC numbers based on National/International events such as but not limited to; Special Event Assessment Rating (SEAR) Level 1-5 Special Event, natural disasters impacting critical infrastructure, suspicious activity or accidents that could become a matter of national interest and credible threat with a possible/actual terrorist nexus. The SWO will make the final determination of the events to be tracked using an NOC number based on the following Director's Criteria:

Phase 3 – Urgent

- An event so catastrophic that the federal government must assume the highest level of operational posturing and activity.
- A domestic event with a confirmed terrorist nexus.

Phase 2 - Concern

- An event meeting any of the four criteria outlined in Homeland Security Presidential Directive-5.

- Man-made events and natural disasters; chemical, biological, radiological, nuclear, explosive, and cyber events; floods, fires, and tsunamis; and other events causing loss of life and large scale evacuations (likely leading to a PDD) and requiring significant federal involvement.

- An event significantly impacting the U.S. critical infrastructure and industrial accidents occurring in densely populated areas.

- A credible threat with a possible/actual terrorist nexus and U.S. homeland security implications.

- A National Special Security Event (NSSE) or SEAR Level 1-5 Special Event whose public safety, threat, complexity, or other attributes require extensive Federal information sharing, interagency support, and incident management preparedness.

Phase 1 - Awareness

- Man-made events, natural disasters, and other events that state and local officials will manage with limited federal assistance.

- An event impacting critical infrastructure.

- Suspicious activity or accidents that could become a matter of interest at the national level.

- An event with a homeland security or safety nexus that the HSC, S1, and senior DHS officials may need to address.

- A NSSE or SEAR Level 1-5 Special Event whose public safety, threat, complexity, or other attributes require Federal information-sharing and involve federal operations coordination and planning activities.

Steady-State Phase

- Routine national and international events that may be of interest to DHS, usually handled at the local and state level, and requiring only DHS situational awareness, monitoring, and routine reporting.

Once a SWO decides that an event or incident should be of interest, a Tracker is directed to assign a NOC tracker number for the incident into the NOC Tracker Log. Upon creating incident titles and assigning NOC tracker numbers to incidents meeting criteria set forth by the watch, Trackers enter a synopsis and searchable text highlights. The Tracker then enters the timeline of events on an incident assigned a number into the NOC Tracking Log. All information concerning a specific tracked incident is then kept under the incidents tracker number. For example, all information pertaining to the Haitian earthquake (RFIs, situation

reports, etc.) is stored under the number assigned to the Haitian earthquake event. All supporting documents for an incident are scanned into electronic files for long term archive. The documents are scanned into a single PDF file and embedded in the NOC Tracker Log through either a copy/paste or drag/drop method. This ensures that all relevant information for a tracked incident is in a single location for ease of retrieval.

As official records, SWO and NOC Log entries are never changed after either Log is closed out for a particular shift or when there has been a turnover of watch personnel. If updated or corrected information becomes available, a new Log entry is made, citing the initial entry and providing the updated/corrected information. Watch relief does not occur until all Log entries from the watch being relieved are completed. While it is the responsibility of the off-going watch to complete their Logs, the incoming SWO will not accept turnover until he/she has read and understood all entries and acknowledges them to be complete. The daily log is closed at 2400 local time. All outstanding actionable entries are carried over and annotated at the beginning of the new log entry.

The NOC receives and makes RFIs on a regular basis. They are primarily used to gather information to help make a decision on what the next step should be in a given situation. The vast majority of RFIs processed by the NOC do not contain PII (e.g., the Department of State might send an RFI asking, "What is the potential number of CBP officers that are being prepared to depart to Port au Prince, Haiti with the main mission of processing Haitian children adoptions?" OPS would task the CBP desk to answer the Department of State, and the RFI would be stored in the "Haitian Earthquake" event folder). Occasionally, the NOC receives and answers an RFI that either contains or asks for a response that may contain PII. (e.g., LAPD might send an RFI stating, "Please run a name trace on a foreign national acting suspiciously at the Rose Bowl Parade.") The information entered into the SWO and NOC Tracker Log from a "name trace" RFI may contain some or all of the following information: name, address, phone number, medical information, physical location, SSN, DOB, Alien registration number (A-number), vehicle license plate number, and passport number.

This PIA describes the system, functions, data safeguards, and data integrity features of the SWO and NOC Tracker Logs.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The SWO Log is a synopsis, in the form of a Word document, that records all significant information received and actions taken by the SWO during the shift. While it is the responsibility of the SWO, maintenance of the SWO Log may be delegated to other personnel on watch.

The NOC Tracker Log is the underlying cumulative repository of responses to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters as well as requests for information (RFIs) that require a NOC tracking number. It contains a copy of all documents and information that is requested, shared, and/or researched between all NOC Watch Officer Desks. One duty of the SWO is to decide what incidents/events are of interest to the NOC. Once a SWO decides that an event or incident should be of interest, a Tracker is directed to assign a NOC

tracker number for the incident into the NOC Tracker Log. The information entered into the SWO and NOC Tracker Logs from a "name trace" RFI may contain some or all of the following information: name, address, phone number, medical information, physical location, SSN, DOB, A-number, vehicle license plate number, and passport number.

1.2 What are the sources of the information in the system?

The sources of information are:

- Private individuals submitting tips either directly to the NOC or through law enforcement officials;
- Suspicious activity reports (SARs) from law enforcement, governmental agency, or private sector security officials;
- Law enforcement bulletins and reports from federal, state, county, local, and/or tribal law enforcement;
- Reports compiled from open source information; and
- Contents of and answers to RFIs.

1.3 Why is the information being collected, used, disseminated, or maintained?

The NOC collects and maintains information in order to provide key domestic security agencies with the information necessary to coordinate their prevention, mitigation, response, and recovery activities. DHS uses the SWO and NOC Tracker Logs as a check to insure that there is no duplication of effort between watch desks. Using the "Haitian Earthquake" example given in the overview, if FEMA, the Red Cross, or DOD made the same RFI the next day, the answer would come back immediately from the Tracker.

1.4 How is the information collected?

Information is generally collected from private individuals submitting tips either directly to the NOC or through law enforcement officials. Incoming calls are recorded, and the caller is on notice via announcement at the outset of the call that the call may be monitored. All paper documents for a tracked incident are scanned into electronic files for long term archive. The documents are scanned into a single PDF file and embedded in the NOC Tracker Log through either a copy/paste or drag/drop method. This ensures that all relevant information for an incident is in a single location for ease of retrieval. Information and documents are indexed by incident number. The NOC Tracker Log's synopsis is searchable; however, the embedded documents are not.

1.5 How will the information be checked for accuracy?

The SWO reviews all information collected and decides what incidents/events are credible and of interest to the NOC. In order to determine if reported information has a possible nexus to terrorism or criminal activity, the SWO and Trackers have the necessary training, experience, and

individual knowledge of the subject at hand to properly vet information for credibility and accuracy.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

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."

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: There is a privacy risk that PII in the system may be accessed or altered by unauthorized individuals for criminal or other unauthorized purposes.

Mitigation: All users are authenticated prior to gaining access to 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. The privacy risk is also minimized by the log's architecture. The SWO and NOC Tracker Logs maintain PII in a single location or data repository. This structure reduces the risk to the data by minimizing its proliferation in multiple locations and systems, each of which would need to employ physical or technological security measures to prevent a breach.

Privacy Risk: There is a privacy risk that PII in a SAR may be inaccurate.

Mitigation: The referral of a SAR to a particular law enforcement entity remains associated with the originating entity to permit anyone accessing that information to contact the investigative agency for updates on any related investigative activity. If an individual thought for any reason that inaccurate information about them was in the NOC Tracker Log, he or she may contact the NOC to have it corrected.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

SWOs and watch desk officers utilize the SWO and NOC Tracker Logs to provide key domestic security agencies with the information necessary to coordinate prevention, mitigation, response, and recovery activities. The logs are used as a check to insure that there is no duplication

of effort between watch desks. Information for a tracked event is shared with agencies with a proven need to know and is tailored to contain only information that is required by the requesting or receiving agency as it relates to their official duties. The watch desks may communicate requests to submitting entities in support of the NOC mission of receipt, validation, protection, and dissemination of information. If a report contains PII, the PII is considered part of the submission, and therefore, afforded the same protection as the rest of the data. After an incident is closed, the information in the log can be used in after action and "lessons learned" studies/reports.

2.2 What types of tools are used to analyze data and what type of data may be produced?

None.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Publicly available open source data may be included in the SWO and NOC Tracker Logs. As part of the effort of the NOC to determine whether or not information is credible, NOC desk officers may query publicly available data, including web sites as well as commercial data sources. For example, if a report about an explosion in Times Square is received, the NOC may check CNN or CNN.com to see if there is any substantiating information being reported.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

With the collection of this information, there is a risk of misuse or unauthorized access to PII. To mitigate this risk, all information is stored on secure servers and accessible only to the Senior Watch standers, and the personnel manning the tracker desk, who have received the requisite training regarding the proper use and handling of PII. The Tracker desk is located in a Sensitive Compartmented Information Facility.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The SWO and NOC Tracker Logs contain steady state, Phase 1, Phase 2 and Phase 3 records. Phase 1 and steady state (normal day-to-day) records are kept for five years and destroyed. All Phase 2 and 3 event files are transferred to the National Archives five years after the event or case is closed for permanent retention in the National Archives. All files that have a nexus to an event are kept in the folder for that event. (i.e., all RFI's, media reports, etc. that deal with the Haitian earthquake, are kept in one common folder called "Haitian earthquake.")

Phase 2 events are significant events whose size, scope, and/or complexity require federal information-sharing, coordination, and/or resource assistance and whose attributes do not rise to the level of a major event. Such events require a coordinated federal response in which more than one DHS agency will become substantially engaged, significantly impacting U.S. critical infrastructure and industrial accidents occurring in a densely populated area, indicating a possible terrorist nexus, man made events and natural disasters; chemical, biological, radiological, nuclear, and explosive events; floods, fires, tsunamis, and other events causing loss of life and large scale evacuations and requiring significant federal involvement.

A Phase 3 event is a major event that occurs or is about to occur. Major events are those events possessing the attributes of an Incident of National Significance, an event with a confirmed nexus to terrorism or a situation involving a potential impending terrorist attack and most likely causing the Homeland Security Advisory System level to rise above yellow nationally or selectively in a location in the 55 U.S. states and territories. An example of a Phase 3 event is Hurricane Katrina or a terrorist group detonating a nuclear device in an American city.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, NARA has approved the retention schedule (NARA schedule N1-563-08-2).

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated

Although there is always risk inherent in retaining PII for any length of time, the data retention periods for SWO and NOC Tracker Logs are limited to 5 years and are based on case type identified in the NARA retention schedules, consistent with the concept of retaining PII only for as long as necessary to support the agency's mission.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information may be shared with U.S. Secret Service; Immigration and Customs Enforcement; Federal Protective Service; Federal Air Marshals; Transportation Security Administration; Customs and Border Protection; U.S. Coast Guard; Federal Emergency Management Agency, National Protection and Programs Directorate, and the Office of Intelligence and Analysis.

The SWO and NOC Tracker Log information that DHS shares with internal organizations is tailored to contain only information that is required on a need to know basis by the requesting or receiving agency.

4.2 How is the information transmitted or disclosed?

Information is shared only through secure interconnected networks and/or the NOC tracker desk officer.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The main risk associated with internal sharing is unauthorized access to, or disclosure of, PII. To mitigate this risk, sharing of the information is limited to those DHS officials, employees, and contractors of DHS who have a need for the record in performance of their duties. DHS Employees may be subject to discipline and administrative action for unauthorized disclosure of this information. Privacy protections include strict access controls, including passwords and real-time auditing that tracks access to electronic information.

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.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The White House Situation Room and NOC watch desk parent organizations are provided access to information as it relates to their official duties. Watch desks parent organizations include but are not limited to: Central Intelligence Agency; Defense Intelligence Agency; National Security Agency; National Geospatial-Intelligence Agency; Federal Bureau of Investigation; Department of Interior; Drug Enforcement Administration; Alcohol, Tobacco, Firearms and Explosives; Virginia State Police; Fairfax County Police; New York, Boston, and Los Angeles police departments. All information for a tracked event is shared with organizations with a proven need to know.

Non-law enforcement and non-governmental users are never afforded access to the personal information contained in the SWO and NOC Tracker Logs.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

All sharing will be compatible with the original collection and covered by the routine uses in DHS/OPS-002 National Operations Center Tracker and Senior Watch Officer Logs System of Records, published in the Federal Register at XXX.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

If PII is shared, the information is sent over NIPERNet, SIPRNet or JWICS. Information is generally transmitted manually or disclosed verbally to external organizations on an ad hoc basis pursuant to a routine use defined in the DHS/OPS-002 SORN or in response to a written request under section (b)(7) of the Privacy Act (which is maintained as part of the file). External organizations do not have direct access to the logs, meaning that external organizations do not have access through individual user accounts. External organizations secure SWO and NOC Tracker Log information in accordance to the terms of information sharing agreements which include provisions for appropriate and adequate safeguarding of sensitive information.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

There is a potential risk of SWO and NOC Tracker Log information being leaked, misused, or lost by the agencies with which DHS shares information. The log information that DHS shares with an external entity is tailored to contain only information that is required by the requesting or receiving agency and is shared pursuant to and consistent with the routine uses enumerated in DHS/OPS-002.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. Notice is provided through this PIA and through the DHS/OPS-002 National Operations Center Tracker and Senior Watch Officer Logs SORN.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. When an individual is submitting information to the NOC over the phone, he/she is notified via announcement at the outset of the call that the call may be monitored, and at that time the caller has the right to decline providing the information. As an example, an caller contacts the NOC with a report of suspicious activity, the caller may request that the NOC collect the information without capturing his or her identifying information. However, in instances where PII is provided as part of the suspicious report, the individual is unlikely to have knowledge that his/her information has been submitted to the system.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No, the individuals will not be able to consent to particular uses of the information after providing the information to the NOC.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Individuals will be provided notice through the DHS/OPS-002 SORN and through this PIA. Given that in some instances personal information will be collected without the knowledge of the individual, the SWO and NOC Tracker Logs are accessible only to those personnel with appropriate clearance and a verifiable need to know the information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to 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 SWO and NOC Tracker Logs (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.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If an individual believes that he or she has suffered an adverse consequence that is related to the SWO and NOC Tracker Logs, 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 SWO and NOC Tracker Logs regarding a particular incident, activity, transaction, or occurrence. That correspondence will be directed to the DHS NOC Watch Floor, and a member of the watch will research the SWO and NOC Tracker Logs 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 are individuals notified of the procedures for correcting their information?

Mechanisms for correcting information are set forth above as well as in DHS/OPS-002 SORN.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Information in the SWO and NOC Tracker Logs is often, by definition, raw suspicious activity information. Having verified and accurate information is the ultimate goal of the law enforcement, intelligence community, and other governmental officials using the NOC. The redress indicated in 7.2, above, will help to ensure that the information is accurate. NOC watch desk officers will ensure the integrity of the SWO and NOC Tracker Log information based upon information provided by individuals, as well as any updates received from law enforcement and other government authorities.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The risk that an individual may not be afforded adequate opportunity to correct information is mitigated by allowing individuals to request access or amendment of their records at any time by either submitting a FOIA or a PA request as outlined above.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

SWO's, Assistant Senior Watch Officers and Trackers are employees of DHS who have access to the SWO and NOC Tracker Logs. No other users have access to the SWO and NOC Tracker Logs and, therefore, no other users can access the PII or related information.

8.2 Will Department contractors have access to the system?

No.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All NOC system users are required to complete annual training in privacy awareness. If an individual does not take training, he/she loses access to all computer systems containing PII.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. NOC SWO and Tracker Logs reside on the HSDN and NIPRNET LANs. ATO was granted on August 24, 2010.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Systematic network and system monitoring is in place to detect intrusions. Role-based security is used to prevent unauthorized use of the information, including improper printing or editing of data.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Data on the system is secured in accordance with applicable federal standards, including systematic network and system monitoring in place to detect intrusions. Security controls are in place to protect the confidentiality, availability, and integrity of the data, including role-based access controls that enforce a strict need to know policy. Each user is given a unique login name and password and audit trails are maintained and monitored to track user access and detect any unauthorized use.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The SWO Log is a word document that records all significant information received and actions taken during a shift. The NOC Tracker Log is the underlying cumulative repository of all NOC responses to threats or incidents and significant activities that require a NOC tracking number.

9.2 What stage of development is the system in and what project development lifecycle was used?

It has been in use since 2003.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security