Privacy Impact Assessment Update
for the

National Operations Center Identity Targeting and Analysis Section (ITAS) Database

DHS/OPS/PIA-009(a)

August 27, 2015

Contact Point
Marty Newingham
Identity Targeting and Analysis Section
Office of Operations Coordination and Planning (OPS)
Department of Homeland Security
(202) 282-8040

Reviewing Official
Karen L. Neuman
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 Identity Targeting and Analysis Section (ITAS) Database, formerly known as the NOC Counterterrorism Operations Desk (NCOD). OPS serves as the primary Department of Homeland Security (DHS) point of contact to streamline counterterrorism Requests for Information (RFIs). The ITAS Database is a tracking tool used to track all counterterrorism and fraudulent document-related incoming and outgoing inquiries. OPS, in partnership with the DHS Office of the Chief Information Officer (OCIO), Information Sharing Environment Office (ISEO), and its Homeland Security Information Network Program Office (HSIN), are updating the existing Privacy Impact Assessment (PIA) for NCOD to reflect the name change to ITAS and the shift of the database to the HSIN platform.

Overview

OPS fulfills a unique response and facilitation role within DHS by serving as the bridge for sharing critical information among DHS Components, across the interagency community, and among homeland security partners. OPS planning responsibilities 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, DHS established the NOC, and in its current capacity it 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. The NOC also facilitates information sharing and operational coordination with other federal, state, local, tribal, and non-governmental operation centers and the private sector.

Identity Targeting and Analysis Section (ITAS)

To fulfill the NOC's mission to fuse law enforcement, intelligence, emergency response, private sector, and open-source reporting, the NOC established ITAS to serve as a single point of contact for all RFIs from partner agencies concerning counterterrorism. The ITAS Database is a tracking tool used to track all counterterrorism and fraudulent document[1]-related incoming and

[1] The ITAS database's tracking functions and responses to RFIs are covered by the DHS/OPS–003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN. Pursuant to 6 U.S.C. § 121, 201, and

outgoing inquiries. ITAS allows desk officers to provide unique reporting capabilities, quickly responds to the requesting agency with results, and tracks the incoming and outgoing RFIs in the ITAS Database.

ITAS allows DHS 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 ITAS officers. The primary purposes of ITAS 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 Counterterrorism (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 that RFI responses are submitted to the responsible office in a timely manner.

The process for receiving, reviewing, responding, and storing RFIs has not changed since the original NCOD PIA.[2]

Reason for the PIA Update

The NOC maintains the ITAS Database on an internal OPS server. However, due to the size of the RFI files (many of which include pictures), the ITAS Database has created latency

504 (Homeland Security Act of 2002, as amended), the NOC is authorized to collect, plan, coordinate, and analyze all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from Federal, State, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals; and report, integrate, and fuse such information throughout DHS in order to share information, increase coordination, identify and assess the nature and scope of said information and understand risks in light of potential or actual vulnerabilities to the homeland; and help deter, detect, and prevent terrorist acts as well as to prepare for, respond to, and recover from all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters.

[2] For a detailed description of the ITAS RFI process, please see DHS/OPS/PIA-009 National Operations Center Operations Counterterrorism Desk (NCOD) Database, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_ops_ncod_07302012.pdf.

and storage management problems for the NOC server. Since the NOC server can no longer support the ITAS Database due to its size, the NOC decided to relocate the ITAS Database to the HSIN.

The NOC based the decision to relocate the ITAS Database on the following factors. HSIN is a secure, DHS-owned and operated platform for sharing Sensitive but Unclassified information with a valid security authorization. HSIN users submit to a rigorous, one-time identity proofing process during initial HSIN account registration; and HSIN requires two-factor authentication every time an individual accesses the platform.

In addition, HSIN is built on a SharePoint 2010 platform, which allows for a seamless integration of the existing Microsoft Access-based ITAS Database. Once the ITAS Database transfers to HSIN, ITAS officers will do a one-time login to HSIN to download the ITAS front-end user interface, which will allow them to access the ITAS Database within HSIN. Once the ITAS officer downloads the front-end Microsoft Access interface, he or she can log in via two security checkpoints. First, the ITAS officer must be logged into HSIN, having already passed through vetting by both HSIN and ITAS for a HSIN user account. Second, the ITAS officer must use a NOC-designated password that grants him or her access for his or her specific role. In addition to the HSIN security features the NOC passwords exist in the current system and will be carried over to the new one. The initial download of the database front-end and the additional need for HSIN log in are the only changes that ITAS officers will experience. The ITAS Database will still be viewed by the ITAS officers via the Microsoft Access front-end, and all existing database functionalities will remain in effect. HSIN's permission management system has been configured to prevent ITAS officers from accessing the database until this PIA is adjudicated. In accordance with the HSIN Terms of Service, records older than five (5) years will be removed from the HSIN ITAS Database.

Data Transfer

DHS will save the existing ITAS Database that operates on the NOC's servers in the ITAS shared drive to serve as an archive on the DHS unclassified network. OPS is conducting this PIA update to ensure the ITAS Database relocation is conducted in a privacy protective manner. To migrate the ITAS Database, HSIN's Service Operations Team was granted access to the NOC server on which the ITAS Database is currently stored. The HSIN Service Operations Team will perform a data migration from the existing server to HSIN's secure servers by replicating database files that are then migrated. Once the migration is complete, these files will exist on both HSIN and the archive on the aforementioned ITAS shared drive on the DHS unclassified network. The archive will be retained consistent with the ITAS records disposition schedule and shall be destroyed after 5 years.

Privacy Compliance Review

The DHS Privacy Office conducted a Privacy Compliance Review (PCR) of the NCOD in June 2013. Recognizing that the NOC ITAS (formerly NCOD) has many robust privacy protections in place, the Privacy Office provided recommendations to help guide the NOC in further development of best practices to protect privacy and to promote compliance with the original NCOD PIA. This PIA update will address the status of those recommendations.

Privacy Impact Analysis

Authorities and Other Requirements

There is no update to the authorities for the NOC to operate ITAS. The ITAS Database's tracking functions and responses to RFIs remain covered by the DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN.[3] The Component source data that is searched by the ITAS officers is covered by the individual SORNs for the underlying government systems performing the original collection.

Regarding security authorization, the ITAS Database will now reside on the HSIN network which has its own system security plan and security authorization. The HSIN Authority to Operate (ATO) expires on July 27, 2018.

Characterization of the Information

In response to the recommendations in the NCOD PCR from 2013, the NOC made several adjustments to the information collected by ITAS.

1. *Document Verification*

During the PCR, the Privacy Office observed that the documentation for some RFIs does not clearly demonstrate how the RFIs satisfy OPS requirements.[4] In some cases, this was because the RFI record did not reflect additional information provided by the requesters by phone or a classified cable. The documentation for each RFI should be sufficient to explain why the RFI merited the reason code assigned. When the details of the request warrant further documentation, analysts should document in the written record any telephone conversations or amplifying information provided to help determine whether the validation criteria were met. In the case of supplemental documentation, such as classified cables, the analyst could incorporate

[3] DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, 75 FR 69689, (November 15, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-11-15/html/2010-28566.htm.
[4] DHS/OPS/PIA-009 National Operations Center Operations Counterterrorism Desk (NCOD) Database, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_ops_ncod_07302012.pdf

this information into the record by reference when the classification of the subject, agency, and source allow.

2. Tracking

Given that NCOD analysts assigned the reason code “Other” more than any other reason code, the Privacy Office recommended that the NCOD implement one of the following options. First, the NCOD could demote the “Other” reason code to be a sub-category of one of the other three reason codes. This would require that an analyst first assign one of the three reason codes corresponding to Criterion 1, 2, or 3 before providing additional information under “Other.” Alternatively, the NCOD could eliminate the “Other” reason code and have a comment box for analysts to insert additional information under Criterion 1, 2, or 3. This would ensure that every RFI meets one of the three validation criteria, and that the NCOD codes and tracks the RFIs accordingly.

Following the PCR, OPS has since found that the “Other” code resulted overwhelmingly in requests for individuals who obtained fraudulent identification documents. With this PIA update, the NOC will add a new RFI Reason for “fraudulent identity documents” and will remove the “Other” option to minimize free text submissions and streamline reporting. This will eliminate the need for the sub-RFI Reason free text field currently used as clarification for the “Other” RFI Reason. Although not specifically counterterrorism-related, the NOC has broad authority to expand its information collection to include this new data element.[5]

No new privacy risks have been identified from the addition of these privacy-enhancing data fields.

Uses of the Information

The backend source data for the ITAS Database will reside on HSIN, but the user experience will not change. ITAS officers will continue to use information collected and maintained by the ITAS Database to facilitate and track incoming and outgoing RFIs from counterterrorism mission partners and to track the subsequent response reports from ITAS. Tracking numbers are assigned by date to assist ITAS officers in determining which RFIs have

[5] Pursuant to 6 U.S.C. § 121, 201, and 504 (Homeland Security Act of 2002, as amended), the NOC is authorized to collect, plan, coordinate, and analyze all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from Federal, State, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals; and report, integrate, and fuse such information throughout DHS in order to share information, increase coordination, identify and assess the nature and scope of said information and understand risks in light of potential or actual vulnerabilities to the homeland; and help deter, detect, and prevent terrorist acts as well as to prepare for, respond to, and recover from all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters.

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.

Privacy Risk: There is a privacy risk of misuse or unauthorized access to the ITAS Database since it will now reside outside of the NOC internal server.

Mitigation: To mitigate this risk, DHS limits access to the ITAS Database through both ITAS role-based permission controls and HSIN security and access management procedures. ITAS community leadership will have the ability to develop Membership Groups containing specific individuals. Sections of the ITAS COI on HSIN will be accessible exclusively to specified Membership Groups through HSIN's access control and permission group settings. ITAS Database users must be added to Membership Groups individually. In the event that a user does not require access and has been incorrectly added to a Membership Group roster, ITAS leadership will remove the user from the Membership Group roster.

The ITAS Database is contained to a closed membership sub-site under the Federal Operations, NOC COI. Users with access to the NOC COI will be able to see the ITAS database site listed in the "Site Contents," but unable to access the ITAS COI unless they have been granted access by ITAS. Only users with HSIN accounts vetted by ITAS can access the ITAS COI and the ITAS database.

Once ITAS officers have access to the ITAS COI, they must then pass through two security checkpoints to log in to the database. First, the ITAS officer must be logged into HSIN, having already passed through vetting by both HSIN and ITAS to access the database. Second, the ITAS officer must use a NOC designated password that grants him or her access for his or her specific role. The NOC passwords exist in the current system and will be carried over to the new one in addition to the HSIN security features.

Privacy Risk: There is a privacy risk of inaccurate or untimely data because there will be two copies of the ITAS Database following the migration to HSIN.

Mitigation: The HSIN Service Operations Team will perform a data migration from the existing server to HSIN's secure servers by replicating database files that are then migrated. Once the migration is complete, these files will exist on both HSIN and the archive on the aforementioned ITAS shared drive on the DHS unclassified network for 30 days. During this time, ITAS will evaluate the functionality of ITAS Database on HSIN. If, after 30 days, OPS is satisfied with the ITAS Database's functionality on HSIN, OPS will delete the ITAS Database from their shared drive.

Notice

ITAS is not collecting any new information, or using information for a different purpose. Therefore, no additional notice is needed.

Data Retention by the project

The records are retained under NARA/OPS records schedule N1-563-08-023 and have a five (5) year retention schedule. This five-year retention schedule is based on the operational needs of the Department.

The risk that OPS was retaining information longer than necessary, which was described in the previous PIA is no longer valid. The HSIN platform does not retain information beyond a period of five (5) years from the date of upload. The mitigation described for the risk in the previous PIA is already standard practice.

To reduce the risk of maintaining information that is no longer accurate, ITAS reduced length of time it retains 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 ITAS 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.

Information Sharing

There are no updates pertaining to the internal or external sharing of information from the original PIA.

Redress

There are no updates to the redress procedures described in the original PIA.

Auditing and Accountability

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.

HSIN security settings include strict access controls, including passwords and administrative tools that track access-levels to electronic information. Authentication and role-based user access requirements ensure that users only access or change information that is appropriate for their official duties. HSIN accounts require that all users process through a one-time, rigorous identity proofing process during account creation, and subsequent validation into the specific COI by a trusted vetting official, as chosen by NOC ITAS leadership. HSIN's two-factor authentication control provides increased security for user accounts. Additionally, the user must be logged into HSIN to access the information, thus being a trusted member of the HSIN ITAS COI. In turn, this requires the user to abide by HSIN's information sharing practices as stated in the HSIN Terms of Service.

Responsible Official

Marty Newingham
Chief, Identity Targeting and Analysis Section
Office of Operations Coordination
Department of Homeland Security

Approval Signature

Original signed PIA on file with the DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security