Privacy Impact Assessment Update
for the

DHS/ALL/PIA-061-1(e) HSIN R3 User Accounts

HSIN Exchange Flash Alerts

April 24, 2017

Contact Point
James Lanoue
HSIN Program Management Office
Office of the Chief Information Officer
(202) 343-4224

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Office of Chief Information Officer (OCIO) maintains the Homeland Security Information Network (HSIN). HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector, and other non-governmental stakeholders involved in identifying and preventing terrorism, as well as undertaking incident management activities. This Privacy Impact Assessment (PIA) Update documents how OCIO has established information sharing relationships through a new centralized application called HSIN Exchange to provide authorized individuals access to: (1) securely create, send, and receive requests for information (RFI); and (2) "opt-in" to receive messages and emergency notifications called Flash Alerts, thereby streamlining these communications. This PIA Update also documents that OCIO now maintains HSIN; it was previously maintained by the Office of Operations Coordination and Planning, now known as the Office of Operations Coordination (OPS).

Overview

HSIN is a user-driven, web-based, information sharing platform that connects all homeland security mission partners within a wide spectrum of homeland security mission areas. DHS mission partners rely on HSIN as a trusted environment that supports DHS missions by: (1) providing timely and accurate information related to detecting, preventing, responding to, and recovering from terrorist attacks and natural disasters; (2) providing timely and accurate information regarding vulnerabilities and threats, managing incidents to mitigate risks, and reducing post-incident loss of life and property; (3) providing near real-time collaboration and incident management; (4) facilitating information exchange for emergency management response and recovery operations; (5) connecting disparate information users in a dynamic and diverse information exchange environment; (6) providing authorized individuals access to securely create, send, and receive RFIs; and (7) providing authorized individuals the ability to "opt-in" to send and receive emergency notifications called Flash Alerts.

HSIN contains personally identifiable information (PII) about the homeland security enterprise HSIN users. This PIA covers the user information required for access to the HSIN community. HSIN also contains PII about members of the public who are subjects of documents, reports, or bulletins contained in the HSIN collaboration spaces.[1]

Reason for the PIA Update

DHS is updating this PIA because HSIN has built a new application, HSIN Exchange,

[1] For a detailed description of the content and information available on HSIN and the associated privacy risks, please *see* DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces on the Sensitive But Unclassified Network PIA (July 25, 2012), *available at* https://www.dhs.gov/privacy.

which allows a more collaborative and efficient process of communicating with large sets of users. HSIN Exchange allows authorized users the ability to create, send, and receive emergency notifications called Flash Alerts. Additionally, HSIN is now maintained by OCIO; it was previously maintained by OPS.

HSIN Exchange for Requests for Information (RFI)

Every day, homeland security partners across the country receive and manage dozens of RFIs by email. With the introduction of HSIN Exchange, there is a secure and standardized way to submit, respond, and easily track these requests, as well as provide automatic reports for key performance indicators. HSIN Exchange enables more efficient response times, provides tracking capabilities in a secure environment, and reduces duplication of systems and effort. As a centralized RFI management system, this new feature also enables analysts to easily pick up and continue work from one shift to the next.

All HSIN Exchange users must first be granted HSIN access through the protocols described in earlier PIAs.[2] The only information HSIN Exchange uses from HSIN to allow new users is the individual's full name.[3] For a user to access HSIN Exchange, an access request is made on behalf of the individual to the group administrator who is the assigned individual overseeing access requests. Once the request is received, the group administrator verifies the individual has a valid HSIN account. Next, the group administrator creates a HSIN Exchange account and links it to the individual's HSIN account.

Within HSIN Exchange users are organized into stakeholder sets, and within stakeholder sets, groups.[4] HSIN Exchange enables stakeholder sets to define how many groups comprise the stakeholder set, as well as what information should be captured and shared in their RFI form. At the group level, groups are able to define access criteria and how their group(s) will interact with other stakeholder sets and other groups. Groups are also able to define unique contact information about their group, which is available in a group directory for all groups participating in HSIN Exchange to access. At the user level, individuals are able to update their own contact information relevant to their role in HSIN Exchange to receive notifications, separate from that in their HSIN profile. Therefore, the information updated in HSIN Exchange remains in that application and is not associated with an individual's HSIN profile.

Users are able to set up two notifications to prompt them to open HSIN Exchange when RFIs are sent, received, or updated: (1) pop-up windows in active browser sessions of HSIN

[2] For more information about how HSIN users are registered, please *see* DHS/ALL/PIA-061-1 HSIN R3 User Accounts and the subsequent updates, *available at* https://www.dhs.gov/privacy.

[3] HSIN Exchange exists as a separate, stand-alone application from HSIN. Information provided by users within HSIN Exchange remains within the application.

[4] A group is a Fusion Center or federal, state, or local organization that handles RFIs. A stakeholder set is a collection of groups. For example, all Fusions Centers would be one stakeholder set.

Exchange; and (2) email notifications. In order to set up these notifications, a user inputs his or her own contact information PII. This PII is inputted because the only information that HSIN Exchange received from HSIN is the individual's full name.

Information included in RFIs uploaded into HSIN Exchange may contain PII. It is the responsibility of the authorized user(s) to manage that PII. The inclusion of PII on HSIN Exchange is covered by the HSIN 3.0 Shared Spaces on the Sensitive But Unclassified Network PIA.[5] Once an RFI is distributed, HSIN Exchange allows originators and responders to clarify the requests and ask for additional information. All RFI recipients are able to submit multiple responses if required. Only the originator can see all responses. Respondents can only see their organizations response(s), not any other organizations' responses. Responses include structured data (e.g., expiration date, case number, date submitted), a text description, and attachments. Responders can attach standard office documents (e.g., Word, Excel), image files (e.g., JPEG, PNG), and geospatial files (e.g., KML).

HSIN Exchange for Flash Alerts

HSIN Exchange also allows authorized users the ability to create, send, and receive emergency notifications called Flash Alerts. Flash Alerts are notifications that HSIN Exchange users can receive via text message to their mobile phones. In order to receive Flash Alerts, individual users must "opt-in" within the HSIN Exchange platform. Users must input additional contact information PII, to include which groups they want to receive Flash Alerts from and what mobile phone number should receive the Flash Alerts.

The goal of the Flash Alerts notifications is to remove the burden of maintaining contact information for other groups in an emergency situation and to assist operators working during quickly-evolving events. When an incident (e.g., terrorist attack, earthquake) occurs that requires a Flash Alert to be sent to a certain group or combination of groups (e.g., Fusion Centers in a region of the United States), Flash Alerts leverages the contact information provided in HSIN Exchange to inform individual users across many different groups or a while stakeholder set that the incident has occurred.

Because HSIN Exchange allows users to update and maintain their contact information relevant to their role, and groups are able to maintain up-to-date membership for users who should have access to their center's operational information, leveraging this up-to-date information will create enormous efficiencies for users in times of emergency. Through Flash Alerts, groups are alerted quickly at an individual level that an incident requiring their attention has occurred.

[5] *See* DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces on the Sensitive But Unclassified Network PIA (July 25, 2012), *available at* https://www.dhs.gov/privacy.

HSIN moved under OCIO Management

HSIN was moved from OPS to OCIO management in 2015 in order to provide more comprehensive IT oversight and management. From 2010 to 2015, day-to-day operations were managed by OCIO while OPS controlled the budget. In 2015, the budget responsibilities were transferred from OPS to OCIO. No technical implications or data transfers occurred when HSIN was transferred from OPS to OCIO management.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

Authorities have not changed from the original PIA. The collection of information from individuals to access HSIN and use its capabilities is covered by several different system of records notices (SORN).

- DHS/ALL-004 General Information Technology Access Account Record System (GITAARS)[6] covers the collection of information from users to allow them to access or interact with HSIN.
- DHS/ALL-037 E-Authentication Records Systems of Records[7] covers the collection and maintenance of information associated with enrolling, issuing, and maintaining credentials (e.g., online account) for individuals seeking electronic access to HSIN.
- DHS/ALL-002 DHS Mailing and Other Lists Systems[8] is maintained for the purpose of disclosing informational or responses to those who request it or for other purposes for which contact lists may be created. This covers the information collected to enable Flash Alerts for individuals.

Characterization of the Information

HSIN Exchange uses the following information to facilitate the sending and receiving of RFIs and Flash Alerts for DHS employees, contractors, and employees of other participating federal, state, local, and international agencies:

A) Individual User Information Collected:

- User Name

[6] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[7] *See* DHS/All-037 E-Authentication System of Records, 79 FR 46857 (August 11, 2014).
[8] *See* DHS/ALL-002 DHS Mailing and Other Lists System, 73 FR 71659 (November 25, 2008).

- Title
- Group Associations
- Primary Email Address
- Alternate Email Address
- Classified Email Address
- Office Phone Number
- Mobile Phone Number
- Home Phone Number
- Fax Number

B) Group Information Supplied by Group Administrator:

- Group Name
- Acronym or Short Name
- Location (U.S. State/Territory)
- Time Zone
- Hours
- Originating Agency Identifier (ORI)
- Group Website URL
- Group Email Address(es)
- Group Phone Number
- Group Fax Number
- Group Emergency Contact Name
- Group Emergency Contact Email
- Group Emergency Contact Phone Number
- Group Emergency Contact Fax

The information for access to HSIN Exchange and to receive Flash Alerts is collected directly from DHS employees, contractors, and employees of other participating federal, state, local, and international agencies. All users initially input information into HSIN themselves during the registration process. Once an individual's HSIN Exchange access is created, the individual inputs the information listed above to be added to the correct group distribution lists to create, send, or receive RFIs and Flash Alerts.

HSIN assumes the initial accuracy of the PII provided by DHS employees, contractors, and employees of other participating federal, state, local, and international agencies and their supporting agency or component through input/import. After the initial input of PII, individual HSIN Exchange users are responsible for updating their own PII to ensure its accuracy. Group administrators within HSIN Exchange are responsible for removing users that leave the organization or group. The information collected as part of this initiative is governed and protected in the same fashion as the other attributes within HSIN.

Privacy Risk: There is a privacy risk that individual users may upload more PII than is necessary to receive Flash Alerts. Specifically, some users may opt to use both their personal and business mobile phones to receive the notifications.

Mitigation: This risk is partially mitigated. Although the collection of this information is covered under the previously listed SORNs, it is recommended that an individual user submits his or her business mobile phone number as the primary method to receive Flash Alerts. However, requiring individual users to only use business mobile phone as a means to receive Flash Alerts may preclude some users and inhibit the ability of HSIN to perform its mission.

Within the HSIN Exchange platform, a disclaimer will be uploaded on the page individuals opt-in to receive Flash Alerts indicating business mobile phone numbers should be the primary method of communication, when applicable.

Uses of the Information

HSIN Exchange uses the information listed above to provide individual's access to HSIN Exchange in order to create, send, or receive RFIs and Flash Alerts. In order to enhance communication and information sharing about an RFI, the contact information of the individual user submitting the RFI displays for recipients to see. This information includes the individual's name, title, and designated email addresses and phone numbers. RFI originators and responders have the ability to communicate back and forth within the context of the RFI. When individuals communicate within the RFI on the HSIN Exchange platform, their first name, last name, and group affiliation will be displayed.

HSIN Exchange tracks actions associated with each RFI with a date and time stamp, as well as the first name, last name, and group affiliation of the individual who performed the action. These actions include submitting, responding to, modifying, or ending an RFI. A group's actions or "history" are only visible internally. Additionally, group administrators are able to see reports of their group's actions within the system for key performance metrics by individual user, such as total RFIs submitted, conversation totals within an RFI, average conversation totals/day, submissions/day, and closures/day.

Flash Alerts use the contact information provided by individual users who have opted-in to facilitate the distribution of emergency notifications and users are notified through text message.[9] Users are expected to acknowledge the alerts in their next active session of HSIN Exchange. HSIN Exchange allows for reporting on how many users received an alert and how many users acknowledged the alert.

Privacy Risk: There is a privacy risk that individual users may upload and transmit PII in Flash Alerts to other participating groups/users who receive them via text message on their mobile phones.

Mitigation: This privacy risk is mitigated through several steps. Prior to using the Flash Alerts capability, all HSIN Exchange users will be required to take mandatory HSIN PII Training regarding the use of PII and will receive a certification once the training is completed. In addition, there will be an implementation rollout plan conducted via the Learning Management System (LMS)[10] in which specific Flash Alerts training will be conducted. During this training, users will learn how to properly use specific functionality and will learn what specific information can and cannot be sent out via Flash Alerts. In addition, while creating a Flash Alert, users will manually confirm via a pop-up that no PII is in the notification prior to distribution.

Furthermore, HSIN will perform audits of the information sent using Flash Alerts to ensure no PII was disseminated. If it is found that a user sent out PII using Flash Alerts, the user's rights will be removed and he or she will not be able to distribute emergency notifications via Flash Alerts moving forward.

Notice

When an individual initially registers for HSIN, he or she is required to read and accept the HSIN Terms of Service.[11] This gives the individual user notice of the type of information and the purposes for which HSIN collects PII. This notice includes that an individual user's information will not be sold to any social media sites or other commercial entity.

Additionally, in order to receive Flash Alerts, an individual user must submit additional contact information PII. A Privacy Act Statement is presented to the individual prior to the point of collection of this additional information. This Privacy Act Statement includes the authority for collecting this information, the purpose for collecting it, and that disclosure of the information is voluntary.

[9] Prior to opting-in, users are notified that standard text messaging rates apply to receiving Flash Alerts.
[10] The Learning Management System (LMS) is an internal training system available to users on the HSIN platform.
[11] The HSIN Terms of Service can be viewed here: https://www.dhs.gov/what-hsin.

Privacy Risk: There is a privacy risk that an individual may not understand why HSIN Exchange is collecting information that may have been previously collected during that individual's registration to HSIN.

Mitigation: This privacy risk is mitigated through the Privacy Act Statement presented to the individual user prior to submitting the information to HSIN Exchange. Also, notice for this initiative and the information collected is provided by the publication of this PIA Update and the previously listed SORNs.

Data Retention by the project

The retention of HSIN user account records has not changed from the original PIA. Records are securely retained and disposed of in accordance with the NARA's General Records Schedule (GRS) 3.2, item 031, "Systems Requiring Special Accountability for Access." Inactive records are destroyed or deleted six (6) years after the user account is terminated or password is altered. However, longer retention is authorized if required for business use. DHS retains the records for this time to ensure effective and efficient administration of the registration process over time, and to comply with any potential audit, legal, or investigative requirements that may arise in the normal course of the homeland security information environment's business.

Information Sharing

Information sharing has not changed from the original PIA. The information sharing conducted through HSIN Exchange and Flash Alerts can all be completed using the normal HSIN processes, as described in the HSIN 3.0 Shared Spaces on the Sensitive But Unclassified Network PIA.[12] However, the updated methods of communication described in this PIA provide more efficient means of sharing information.

The additional features of HSIN Exchange and Flash Alerts allows users to elect to receive alerts and warnings sent automatically by email, phone, or fax. These alerts are emergent, real-time, one-way communications geared to provide notice of an ongoing activity's status or to direct the user to a particular location within HSIN for additional information or detailed collaboration.

Redress

Redress procedures have not changed from the original PIA. Individual users are responsible for verifying the accuracy of the autobiographic information they place in their own profiles. Users may update many elements of their profile information at any time to expand, reduce, or correct information they have provided.

[12] *See* DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces on the Sensitive But Unclassified Network PIA (July 25, 2012), *available at* https://www.dhs.gov/privacy.

Auditing and Accountability

HSIN's Service Ops has the ability to track information through the use of logs and standard, automated workflows defining the movement of content throughout HSIN. In so doing, access requests and the movement of content, including re-dissemination, can be documented. HSIN's Service Ops will regularly perform audits of the information sent using Flash Alerts to ensure no PII was disseminated. HSIN's Service Ops will run audits on a random sampling of Flash Alerts content until an automated process can be implemented. During these audits, if it is found that a user sent out PII using Flash Alerts, the user's rights will be removed and he or she will not be able to distribute emergency notifications via Flash Alerts moving forward.

Within 30 days of on-boarding, all DHS personnel receive initial training. Annual privacy and security awareness training is completed thereafter. In addition, the HSIN Program Management Office (PMO) offers baseline training regarding the privacy-related topics listed below to all HSIN users.

- Privacy and Freedom of Information Act (FOIA) compliance
- Records Management
- Community of Interest (COI) Roles/Limitations
- Classifications and Markings (PII, SSI, FOUO, etc.)
- Nomination/Validation Certifications
- Mobile Device Access
- Shared Space Activities
- HSIN PII Training

Recurring and evolving training topics are made available to all users accessible from the HSIN landing page. HSIN training material is tailored to ensure the content is relevant to the audience and delivered in flexible pre-recorded modules and short virtual conference training sessions that allows the opportunity for the trainees to ask questions and explore their operational context. A training delivery schedule ensures all site administrators, site designers, content managers, and contributors attend in-person classroom training and other appropriate courses before the majority of end users. In addition, to accommodate users spanning the continental United States and its territories, the HSIN training team is prepared to support virtual training, as required. The HSIN training team may also provide supplemental instruction in the form of brief online training modules that include best-practice guidance on topics such as document management and content dissemination.

The procedures in place to determine which individual users may access the information on HSIN Exchange and how HSIN reviews/approves new access to HSIN Exchange by organizations, both within and outside DHS, have not changed from the original PIA. HSIN maintains strict permissions controls when evaluating the credentials for a prospective applicant. These controls are designed to ensure that the security and integrity of HSIN are upheld. Additionally, these controls provide users transparency on the terms of service. A qualified individual may only be considered for access to HSIN either by being nominated by a current user or by calling the HSIN Help Desk to request that a point of contact (POC) be provided. Prospective users are required to answer a set of questions mapping their attributes to their job function or purpose for using HSIN.

Responsible Official

James Lanoue
HSIN Program Manager
HSIN Program Management Office
Office of the Chief Information Officer
Department of Homeland Security

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security