Privacy Impact Assessment
for the

HSIN R3 User Accounts

DHS/OPS/PIA-008

July 25, 2012

Contact Point
James Lanoue
DHS Operations
HSIN Program Management Office
202.282.9580

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

Abstract

The Homeland Security Information Network (HSIN) is maintained by the Department of Homeland Security (DHS), Office of Operations Coordination and Planning (OPS). HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as in undertaking incident management activities. 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.

HSIN contains personally identifiable information (PII) about the homeland security enterprise HSIN users and about members of the public who are subjects of documents, reports, or bulletins contained in the HSIN collaboration spaces. The HSIN platform allows these diverse communities to work together to perform investigations, identify terrorist activities, respond to areas affected by natural disasters, and provide coordination during recovery operations. Each Community of Interest (COI) Sponsor and/or Site Administrator is responsible for monitoring the specific content uploaded into HSIN from that COI, ensuring compliance with the COI Charter. This Privacy Impact Assessment (PIA) covers the user account registration information required for access to the HSIN Release 3 (R3) community.

Overview

HSIN is a user-driven, web-based, information-sharing platform that connects homeland security mission partners, consisting of DHS and its federal, state, local, tribal, territorial, private sector, international, and other non-governmental partners within a wide spectrum of homeland security mission areas. DHS OPS maintains HSIN. HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector, international, and other non-governmental partners involved in identifying and preventing terrorism and in undertaking incident management activities. HSIN is designed to allow all relevant, vetted stakeholders access to the information regardless of jurisdictional, geographic, or agency boundaries, so long as it has been determined that the information is appropriate to be shared.

DHS mission partners rely on HSIN as an environment that promotes trust and sharing, and supports the DHS and Information Sharing Environment (ISE) 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; and (5) connecting disparate information users in a dynamic and diverse information exchange environment.

HSIN is the information-delivery mechanism for DHS ISE, which is mandated by the Intelligence Reform and Terrorism Prevention Act (IRTPA) (6 U.S.C. §§ 485(b), (d)).

As the nation's largest service for the secure and trusted dissemination and sharing of sensitive but unclassified (SBU) homeland security information, HSIN enables information sharing across the entire homeland security enterprise. This innovative, interoperable, customer-driven, cost-effective information sharing environment will enable near real-time, critical information exchange and situational awareness to all types of users and their various operational needs through secured access. HSIN effectively and efficiently meets the President's goals for secure information sharing.

Information shared through HSIN may relate to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, and natural disasters. Information is shared through HSIN among federal, state, local, tribal, territorial, private-sector, and other non-governmental partners through two types of collaborative spaces: HSIN COIs[1] and the HSIN Shared Space.

The HSIN platform allows these diverse communities to work together to perform investigations, identify terrorist activities, respond to areas affected by natural disasters, and provide coordination during recovery operations.

HSIN User Account Information

This PIA covers the user account registration information required for access to the HSIN R3 community. Users must submit basic biographic information to establish their identity and nexus to one of the homeland security enterprise mission areas within HSIN.[2] All HSIN users must agree to the HSIN Terms of Service prior to acceptance into the HSIN information sharing environment. The Terms of Service define a HSIN user's basic rights, duties, and privileges as a registered user of HSIN.

[1] A Community of Interest is defined in the HSIN COI Model Charter as a, "community of HSIN Users sponsored by DHS, a DHS-approved government agency or private sector entity, or an existing COI who have a homeland security mission, and (i) wish to limit access to certain information to those within that community, and (ii) are able to provide independent management of a COI Site in accordance with the standards and policies of HSIN PMO.

[2] HSIN mission areas include: Emergency Management; Critical Infrastructure and Key Resources; Law Enforcement; Public Health; Intelligence Community; and Emergency Services.

When registering for a new account with HSIN, applicants will be requested to fill out mandatory and optional fields listed in Table 1 below. Additionally, applicants must undergo an identity authentication process. The identity authentication process uses a third-party Identity Proofing (IdP)[3] service to generate knowledge-based questions based on commercial identity verification information collected by third-party companies from financial institutions, public records, and other service providers. The information accessed by the IdP may include information such as the individual's commercial transaction history, mortgage payments, and past addresses. An individual must correctly answer the knowledge-based questions generated by the IdP in order to authenticate his or her identity and enable access to use HSIN.

In order to generate these knowledge-based questions, the IdP service collects basic PII from the individual including name, address of residence, date of birth and, on an optional basis, the individual's Social Security number (SSN); however, the SSN will not be stored by the HSIN Program Management Office (PMO).[4] Each individual will be asked a minimum of two and a maximum of four knowledge-based questions. The identity verification platform pulls data from aggregate providers that use only data that is high-level, basic information, including, but not limited to, name, previous addresses of residences, motor vehicle registration information, and demographics (such as age) data. If there is not enough data to generate at least two questions, (i.e., the person lacks sufficient information to generate an adequate number of questions), then the individual's identity cannot be authenticated and he or she will not be able to continue through HSIN online registration.

The fact that an individual was unable to use the IdP service will be sent to HSIN, but no other information. The IdP will send a transaction number, the fact that knowledge-based questions could not be generated, and the date and time of the transaction. This information will allow HSIN PMO to gather statistics on how many individuals are unable to use the IdP.

If there is sufficient information to generate two to four questions, the IdP will evaluate the answers to the questions and return a pass/fail indicator to HSIN PMO. If the individual does not successfully answer the questions generated by the IdP, he will not be authenticated and he will not be able to continue through the HSIN online registration process. If and when the prospective user fails identity authentication, the system will provide the applicant with a limited number of opportunities to retry identity proofing. Should these retry attempts also fail, the

[3] DHS has deployed the use of an IdP service for DHS/ USCIS Self Check Program following the same process, see DHS /USCIS/PIA-030(b) for additional information.

[4] HSIN will require individuals to authenticate their identity through the IdP and providing a SSN enhances the ability of the IdP to generate knowledge-based questions. Since HSIN aims to make itself accessible to any individual who wants to check his own work authorization status, DHS determined collecting SSN on a voluntary basis would make HSIN accessible to more individuals.

system will present the applicant with the appropriate help desk phone number to call, based on the reason code of their failure.

IdP does not maintain the questions posed or the answers provided by the individual. The IdP will send a transaction number, the reason for failure, the date and time of the transaction, and an error code to HSIN PMO. This information will facilitate troubleshooting and system management and improvement so that HSIN PMO can maintain statistics of how many individuals are unable to authenticate through the IdP. All PII entered by the individual during the IdP session and any questions generated by the IdP are deleted at the end of the session.

If the individual is able to answer the questions correctly, his or her identity is authenticated, a pass indicator is returned to HSIN, and the individual will continue through the HSIN online registration process. The next steps include aligning the applicant's personal and professional attributes collected from the HSIN Account Request Form to specific COI that support their job function. These immediately aforementioned steps are intended to automatically streamline and identify an applicable relationship between an applicant and COI(s). Once a recommended COI relationship has been identified, the Validator of that COI will either reject or approve the applicant's membership in the COI. All COIs operate under customized charters and may have specific membership criteria that an applicant must meet to qualify for entry.

The IdP maintains the time/date stamp and the fact the inquiry was made to conduct an identity check.

HSIN will maintain the user registration and profile information to enable HSIN PMO to have an audit trail of how the individual has used HSIN. Basic user profile information is retained so that other members can benefit from his/her contributions, understand the user's qualifications and expertise for context, and judge the accuracy of the information contributed. Additionally, the retention of users' profiles permits the community to contact their in reference to that particular subject matter and their declared expertise through job changes and reassignments. Audit trails may be reviewed in response to suspected violations of the HSIN Terms of Service.

Individuals may also gain access to HSIN through a federated user account. Federated users are not required to go through the HSIN IdP process because their membership in another existing information sharing portal provides the requisite identity validation. Federated users must follow all other processes for gaining access to HSIN COIs.

Privacy Risks and Mitigation Strategies

DHS uses the services of a third-party IdP to authenticate identity for HSIN. This may present privacy risks, including the potential for an individual to inaccurately assume that DHS collects and maintains commercial identity verification information, as well as the risk that an individual may not be able to authenticate his identity using the IdP. The main benefit of HSIN is to allow appropriate and timely information sharing among homeland security partners. The use of the IdP service provides additional assurance that the individual's identity is correctly authenticated.

DHS is using the services of a third-party IdP to authenticate identity. The IdP uses commercial identity verification information collected by third-party companies from financial institutions, public records, and other service providers. This commercial identity verification information does not belong to DHS, nor will DHS collect or retain such information. Nevertheless, there is a risk that an individual seeking to make use of HSIN may inaccurately assume that DHS collects and retains this information. To mitigate this risk, the HSIN secure web portal user interface will employ unique branding and/or different color schemes in the header and footer screens, such as different color scheme and screen layout and messaging on the portal, so that the user will understand when they are interacting with DHS and when they are interacting with the IdP. Directional guidance will also be displayed explaining why the IdP is collecting the information, what the information is being used for, and offering the user a way to exit the HSIN service and delete their information before the identity authentication takes place.

There may be instances when an individual is unable to authenticate his identity using the IdP. For example, the IdP may not be able to generate knowledge-based questions if sufficient data pertaining to an individual cannot be located. In addition, an individual may not receive a passing score because the IdP information maintained is incorrect. If and when the prospective user fails identity authentication, the system will provide the applicant with a limited number of opportunities to retry identity proofing. Should these retry attempts also fail, the system will present the applicant with the appropriate help desk phone number to call, based on the reason code of their failure.

Information shared through HSIN may relate to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, and natural disasters. Information is shared through HSIN among federal, state, local, tribal, territorial, and private-sector partners through two types of collaborative spaces: HSIN COIs[5]

[5] A Community of Interest is defined in the HSIN COI Model Charter as a "community of HSIN Users sponsored by DHS, a DHS-approved government agency, or private sector entity, or an existing COI who have a homeland security mission, and (i) wish to limit access to certain information to those within that community, and (ii) are able

and the HSIN Shared Space. For a thorough privacy risk analysis of the information collected, maintained, used, and disseminated within HSIN COIs and the Shared Space, please see HSIN R3 Shared Spaces Privacy Impact Assessment, DHS/OPS/PIA-007 HSIN R3 Shared Spaces. This Privacy Impact Assessment only covers HSIN R3 user account registration 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 that the National Operations Center (now a component of DHS Operations Coordination and Planning since the July 2005 Secretary Michael Chertoff reorganization of the Department) to "(1) provide situational awareness and 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; and (2) ensure that critical terrorism and disaster-related information reaches government decision-makers."

Sections 121(d)(1), (4), (11), (12)(A), (15), and (17) further provide DHS OPS with authority to establish and collect the information in HSIN R3. Consistent with the Paperwork Reduction Act of 1995, 44 U.S.C. § 3507(d), OPS has considered the impact of the information collection burden imposed on the public in the registration process and is complying with the required Paperwork Reduction Act processes for this information collection. HSIN user account registration information is maintained in strict compliance with the notification, access, and amendment requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

Section 1016(b)(1) of IRTPA, 6 U.S.C. § 485, requires the President to create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties.

Former DHS Secretary Chertoff's Memorandum of January 9, 2006, establishes HSIN as the "primary system for operational information sharing and collaboration" with DHS and its external partners, and "the platform by which we will provide operational information and decision support, share documents, supply situational awareness, and conduct alert, warning and notifications."[6]

---

to provide independent management of a COI Site in accordance with the standards and policies of the HSIN PMO."
[6] Chertoff, Secretary Michael. *Homeland Security Information Sharing Network Deployment*. January 9, 2006

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

User account information maintained within HSIN is covered by the DHS/ALL/004 - General Information Technology Access Account Records (GITAAR) SORN, 74 Fed. Reg. 49882 (Sep. 29, 2009), which covers information collected in order to provide authorized individuals with access to DHS information technology resources. The system enables DHS to maintain: account information required to approve user access to information technology; lists of organizational points of contact; and lists of emergency points of contact. The system will also enable DHS to provide individuals access to certain programs and meetings and, where appropriate, will allow for sharing of information among individuals in the same program to facilitate collaboration. The system also allows DHS to track and audit usage of the system to ensure ongoing compliance with the HSIN Terms of Service.

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

Yes. A HSIN 3 System Security Plan (SSP) has been developed by HSIN PMO as of May 2, 2012, in full compliance with DHS 4300a, in anticipation of a final authorization to operate. In addition, HSIN maintains a HSIN/Common Operating Picture (COP) Incident Response Plan to guide HSIN PMO response to security incidents.

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

For user account information, NARA's General Records Schedule 24, Section 6, "User Identification, Profiles, Authorizations, and Password Files" states that inactive profile records will be destroyed or deleted six (6) years after the user account is terminated or the password is altered, or when no longer needed for investigative or security purposes, whichever is later; this records schedule covers the retention period.

All other records maintained by HSIN are discussed further in HSIN R3 Shared Spaces Privacy Impact Assessment, DHS/OPS/PIA-007.

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 PRA applies to HSIN User Accounts, as members of the private sector can apply for HSIN user accounts. HSIN PMO is actively pursuing full PRA review and will ensure full and appropriate compliance.

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.

User registration information for HSIN includes information for all persons authorized to access HSIN, including employees, contractors, grantees, private enterprises, and any lawfully designated representative of the above. In addition, representatives of federal, state, local, territorial, tribal, international, or foreign government agencies or entities may have access to HSIN in furtherance of the DHS mission.

The personal and employment data collected for HSIN R3 user registration is limited to the information necessary to validate the registrant's identity and certify their nexus to one of the homeland security enterprise mission areas within HSIN. Information collected within HSIN from a new registrant is listed in Table 1 below:

HSIN New Registrant Information[7]	
Mandatory fields	**Optional fields**
Primary Community	Salutation
Reason for Access	Middle Initial
First Name	Suffix
Last Name	Nickname
DOB	Ext.
Primary E-Mail	Fax
Alternate Secondary E-Mail	Pager
Business Phone	Other Phone
Mobile Phone	Business Location: (Street 2, Street 3,)
Primary Contact Method	Home Location: (Street 1, Street 2, Street 3, City,
Secondary Contact Method	Postal/ZIP, Country, State)
Job Title	Deployed Location: (Street 1, Street 2, Street 3, City,
Job Role	Postal/ZIP, Country, State)
Organization	Topic(s) of Interest
Business Location: (Street 1, City, Postal/ZIP,	HSIN Supervisor Information (Secondary E-Mail, Mobile

[7] This list is subject to change. A user is free to consult https://government.hsin.gov/sites/HSINr3/DecSupport.aspx to find the very latest modifications to this list. The PMO retains the right to unilaterally update this TOS as required and will do so, to update the latest changes in system development.

Country, State) HSIN Supervisor Information: (Full Name, Organization, Primary E-Mail, Job Title, Business Phone, Ext., Primary Contact Method, Secondary Contact Method) Sector Country of Citizenship Username Password Security Question (x4) Security Answer (x4) TFA Delivery Value 1 (required phone, email, or SMS)	Phone) SBU Category PCII Authorized User Number Credential SSN Two-factor Authentication (TFA) Delivery Value 2 (optional phone, email, or SMS) TFA Delivery Value 3 (optional phone, email, or SMS) Home Phone Number

Table 1: HSIN New Registrant Information

Table 2 below shows the PII fields stored or not stored by HSIN PMO.

Stored	Not Stored*[8]
Salutation **First Name** **Middle Initial** **Last Name** **Suffix** **Business Phone** **Mobile Phone** **Email** TFA Delivery Value 1 (required phone, email, or SMS) TFA Delivery Value 2 (optional phone, email, or SMS) TFA Delivery Value 3 (optional phone, email, or SMS) **Password** **Security Question & Answer (x4)**	Home Address (street, city, state, postal) * Date of Birth SSN * Country of Citizenship* Fax* Pager* Other Phone* Business Address* Deployed Address*

Table 2: Identification of Stored and Not Stored PII Information

There is a 45-day period for a user to be vetted into a COI based upon the attributes collected from the registration questionnaire. After such time, if the user has not been vetted, he or she will need to repeat the registration process. During the vetting process, the prospective user does not have access to any COI until a COI accepts his or her registration. At this initial level of access, migrating users will have read-only access to the home page and HSIN Central until the appropriate COI(s) accept them.

[8] Content marked with an asterisk (*) are optional input fields and only stored if the user provides the content.

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

Basic biographic and contact information from users applying for access to HSIN is collected directly from the user. Prospective users directly provide information related to their individual profile, including their name, email address, employment, and supervisor's name and email address.

Additional sources of information include a user's supervisor, who must supply confirmation that the user has a nexus to a homeland security enterprise mission area and is permitted to use HSIN for work-related purposes. Also, HSIN relies upon a third-party identity verification provider to ensure full and effective validation through identity confirmation. No information, other than the results of the confirmation check, are returned to HSIN and the prospective user. If a prospective or current user has any inquiries, he should contact the third-party identity proofing service. This information will be used solely for the limited purpose of identity proofing, and will not be stored on HSIN. Users may decline to provide their information, but by doing so, their application for access will be rejected and they will not receive an account.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

In order to verify the registrant's identify, PII will be collected to validate one's credentials for access into HSIN, a COI, or any HSIN collaboration space within the HSIN system. During this process, a third-party IdP will be used to ensure full and effective validation through identity confirmation. DHS will not collect this information; the IdP will use the information solely for the limited purpose of identity proofing and sending the confirmation. The third-party IdP is contractually bound to only use the information collected from individuals for identity verification, as defined by the HSIN business process, limited fraud identification, and prevention.

The IdP maintains an audit log of the time and date of the request for validation, the name of individual, whether they passed or failed, and if they failed the reason for the failure. No commercial data associated with this process will be received or maintained on HSIN. Users may decline to provide their information, but by doing so, their application for access will be rejected and they will not be provided an account.

2.4 Discuss how accuracy of the data is ensured.

HSIN R3 users are responsible for verifying the accuracy of the autobiographic information they place in their own profiles. Users may update their profile information at any time to expand, reduce, or correct information they have provided; however, certain profile information is mandatory and is derived from the user's application: name, email address, and the user's Department or Agency. Upon request of the user, the HSIN R3 program manager may make changes to the mandatory fields.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that a registrant's application may be denied based on the results of the use of a third party validator that may return incorrect data.

Mitigation: HSIN PMO has engaged identity verification provider to conduct these services under contract that is required to provide a level of accuracy related to the information used to provide the service.

Privacy Risk: Since some information is collected directly from individuals, there is a risk that individuals will be able to circumvent supervisor approval for use of HSIN by providing false information.

Mitigation: HSIN R3 will use a thorough nomination, validation, and identity proofing process to register prospective users. In addition, following this initial, extensive review, users must be nominated and validated into specific COIs, each with its own process. For HSIN R3, HSIN PMO will establish clear security response procedures, facilitating quick communication between COIs and HSIN Security, to report suspicious activity and efficiently resolve any security issues facing the system. These measures, taken in combination, should mitigate the risk of a prospective user using false information to gain access to HSIN.

Privacy Risk: In order to utilize HSIN, an individual must first pass the IdP authentication process. It is possible that some individuals will not be able to use HSIN because their identity cannot be authenticated through the IdP process.

Mitigation: There are several reasons why a user's identity could not be validated. For example, an individual may not have resided in the country long enough to establish enough history for which to draw the authentication questions and therefore, his identity could not be verified. Another reason could be that the information contained in the commercial databases is

incorrect, thus providing insufficient information from which to develop authenticating questions. A third reason could be that an individual is attempting to illegitimately access HSIN. If and when the prospective user fails identity authentication, the system will provide the applicant with a limited number of opportunities to retry identity proofing. Should these retry attempts also fail, the system will present the applicant with the appropriate help desk phone number to call, based on the reason code of their failure.

HSIN PMO will regularly review and monitor the success rate of the IdP process. Additionally, HSIN clearly communicates the necessary actions an applicant must take in order to correct a failed IdP verification attempt. If and when the prospective user fails identity authentication, the system will provide the applicant with a limited number of opportunities to retry identity proofing. Should these retry attempts also fail, the system will present the applicant with the appropriate help desk phone number to call, based on the reason code of their failure.

Privacy Risk: DHS is using the services of a third-party IdP to authenticate identity. The IdP uses commercial identity verification information it has collected from financial institutions, public records, and other service providers. This commercial identity verification information does not belong to DHS, nor will DHS collect or retain such information. Nevertheless, there is a risk that an individual seeking access to HSIN may inaccurately assume that DHS collects and retains this information.

Mitigation: The HSIN secure web portal user interface will employ unique branding, such as different color scheme and screen layouts and messaging on the portal so that the user will understand when they are interacting with DHS and when they are interacting with the IdP. Directional guidance will also be displayed explaining why the IdP is collecting the information, what the information is being used for, and offering the user a way to exit the HSIN service and delete their information before the identity authentication takes place.

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.

HSIN is designed to facilitate the secure integration and interoperability of information sharing resources among federal, state, local, tribal, territorial, private-sector, international, and other non-governmental partners involved in identifying and preventing terrorism and in undertaking incident management activities. HSIN is designed to allow all relevant, vetted

stakeholders access to the information regardless of jurisdictional, geographic, or agency boundaries, so long as it has been determined that the information is appropriate to be shared.

User registration information is used to (1) verify the potential user's identity; (2) contact his/her supervisor to obtain approval for the applicant's use of HSIN; and (3) determine a user's access to different shared spaces within the HSIN environment. User account information is also used to determine a user's operational and permission roles within HSIN. Information within the registration account may also be used to determine HSIN "federated users." A federated HSIN user is one whose roles, rights, and privileges have already been vetted securely in a federated portal that operates under a federated agreement.

A federated user shall receive revocable rights to access HSIN using the same credentials as her original federated portal. Access shall be available through web browser, mobile device, or other application. Such users shall be subject to the rules governing a particular HSIN COI, including additional COI membership criteria, in the same way as any other registered HSIN user.

In addition, aggregated information is used for reporting and metrics on the utilization of the system. Such metrics include an analysis of the number of active users from the various partner segments that HSIN supports and the number of users who have logged into the system in the past 24 hours.

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.

No, the HSIN search function does not possess such capability**.**

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

Any component within DHS may use HSIN to enhance its information-sharing capabilities. Users have the ability to set up COIs, which operate under their specific Charter and the HSIN Terms of Service. COIs may specify membership criteria and other controls pertaining to who gains access to what information within the COI. These controls are designed to ensure security and integrity of HSIN and to limit damages to HSIN, providing users with transparency on their rights, duties, and privileges.

At a minimum, prospective HSIN COI users must possess the following attributes: (1) the applicant's work assignment supports a DHS ISE mission relevant to the COI; (2) the applicant is credentialed to access FOUO information; and (3) the applicant accepts and adhere to the HSIN Terms of Service. All members of HSIN can view basic contact information for other users on HSIN. Once a user is accepted into a COI, that COI membership becomes the primary means by which a user's access to content is defined, along with the credentials defined by the user profile, working in conjunction with content tagging and rules-based permissions.

The HSIN PMO is a data and content steward and is not responsible for the content that users and COIs post to any element of HSIN or retain custody and exclusive control over at any location within HSIN, under their relevant and applicable federal, state, local, territorial and tribal information management, privacy, public disclosure (or "sunshine") and records management statutes, or regulations.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that user account information may be used in a manner inconsistent with the purpose of the original collection.

Mitigation: HSIN user account information is only used to provide authorized individuals with access to DHS information technology resources. HSIN is designed to allow all relevant, vetted stakeholders access to the information regardless of jurisdictional, geographic, or agency boundaries, so long as the information is appropriate to be shared. In order to verify the registrant's identity, PII will be collected to validate one's credentials for access into HSIN, a COI, or any HSIN collaboration space within the HSIN system. During the authentication process, the IdP will be used to ensure full and effective validation through identity authentication. Third-party validation is used to ensure objectivity during the nomination, validation, and identity proofing process. By dividing the roles of nominator and validator, the risk of inappropriate, unilateral vetting is significantly reduced, ensuring that any new user, or a member of a COI, has been reviewed and confirmed as an appropriate, secure user on HSIN and in a given COI. The data fields listed in Table 1 above are all strictly necessary to ensure such effective validation. If a user's original criteria for membership in HSIN changes, he or she will need to be re-validated into a community.

Privacy Risk: There is a risk that the IdP will misuse the data collected during the identity verification process.

Mitigation: The IdP is contractually bound to only use the information collected from individuals for identity verification, as defined by the HSIN business process, limited fraud

identification, and prevention. HSIN PMO confirms IdP compliance by ensuring all contract terms are adhered to through project management and compliance meetings throughout the term of the contract. The HSIN PMO will also provide guidance to HSIN users on how to notify the HSIN PMO of any irregularities in their credit reports as a result of using HSIN.

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.

Users of HSIN R3 COIs receive notice of collection and use through a Privacy Act Statement and advisory notices. Users receive a Privacy Act Statement on the user access request form at the time of enrollment. Additionally, users receive notice that their activity on HSIN R3 will be logged and monitored in accordance with DHS authorities and policies to ensure appropriate use of DHS systems. The user notice is provided prior to each login.

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

In the HSIN Terms of Service, all prospective users have the opportunity to consent to or decline the basic rights, duties, and privileges defined for HSIN users. Beyond the PII required to establish an account, all other PII is voluntarily provided by the user at his/her discretion. Users who choose not to provide the additional information necessary to complete the user profile may see the value of their participation in HSIN R3 diminish, but it will not affect their ability to have an account.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: An individual seeking to make use of HSIN may inaccurately assume that the IdP authentication information belongs to and is collected and retained by DHS.

Mitigation: The HSIN secure web portal user interface will employ unique branding, such as different color scheme and screen layouts and messaging on the portal so that the user will understand when they are interacting with DHS and when they are interacting with the IdP. Directional guidance will also be displayed explaining why the IdP is collecting the information,

what the information is being used for, and offering the user a way to exit the HSIN service and delete their information before the identity authentication takes place.

Privacy Risk: HSIN users will not understand how their registration information is being collected and used by DHS.

Mitigation: The HSIN secure web portal user interface will have a clear Privacy Act notice at the point of collection as well as a link to the privacy policy on each page. Specific information on the use of the IdP will also be provided as the applicant goes through the process of applying for membership.

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.

HSIN user account records will be retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, "User Identification, Profiles, Authorizations, and Password Files." Inactive records will be destroyed or deleted six (6) years after the user account is terminated or the password is altered, when a user no longer wishes to be a registered user, or when no longer needed for investigative or security purposes, whichever is later.

DHS uses the services of a third-party IdP to authenticate an individual's identity. The third-party IdP uses commercial identity verification information to create the knowledge-based questions used to authenticate identity. This information does not belong to DHS, nor will DHS collect or retain the information from other sources relied upon by the third-party provider. The IdP maintains the time/date stamp so that the identity check inquiry is recorded and can be audited at a later date.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that HSIN user account information will be retained longer than is necessary.

Mitigation: HSIN R3 retains user account information for up to six (6) years from the time the account is deactivated. Retention of user account information while the account is active

is appropriate given the user's role in the homeland security mission space. By retaining the user's profile, other members can benefit from his/her contributions, understand the user's qualifications and expertise for context, and judge the accuracy of the information contributed. Additionally, the retention of users' profiles permits the community to contact them in reference to that particular subject matter and their declared expertise through job changes and reassignments.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes, name, date of birth, home address, SSN (if provided), and home phone (if provided) will be collected for identity authentication purposes by a third-party IdP. This information sharing is covered under the contract with the third-party IdP service provider. The third-party IdP service will not disclose or share any of the information provided under this service as stated under the terms and conditions of the contract.

The authentication questions posed by the IdP are not shared with DHS, only the the pass/fail outcome of the identity authentication.

In addition to the third party IdP, HSIN will share user information with the sponsoring agency to ensure employment is accurately reflected and the individual has a need to be in a particular COI.

By default, a user's basic contact information, as listed in the Table 3 below, will be shared with all registered HSIN users in order to allow collaboration among the various community members.

HSIN Users "My Profile" Category	Display Name
Basic Information	User Name
	Name
	Salutation
	First Name
	Middle Initial
	Last Name
	Suffix
	Nickname
	About Me
	Picture
	Certifications
	User Interests
	Business Phone

Table 3: Basic Information Shared Among All HSIN Registered Users

Furthermore, a user may select to share the additional fields listed in Table 4 below, with all members of the HSIN community. The middle column identifies the user registrant information that may be shared with, and only with, the HSIN user community. The column on the right identifies whether or not the user information is defaulted to be shared with "everyone" or "only me," meaning only the user to whom the information belongs as opposed to the HSIN user community.

"My Profile" Category	Display Name	"Show To" Default
Basic Information	Primary Community	Everyone
Contact Information	Primary E-Mail	Everyone
	Secondary E-Mail	Everyone
	Extension	Everyone
	Mobile Phone	Only Me
	Fax	Everyone
	Pager	Only Me
	Other Phone	Only Me

"My Profile" Category	Display Name	"Show To" Default
	Primary Contact Method	Everyone
	Secondary Contact Method	Everyone
Employment Information	Job Title	Everyone
	Job Role	Only Me
	Organization	Everyone
Business Location	Street 1	Only Me
	Street 2	Only Me
	Street 3	Only Me
	City	Only Me
	County	Only Me
	Postal/ZIP	Only Me
	Country	Only Me
Home Location	Street 1	Only Me
	Street 2	Only Me
	Street 3	Only Me
	City	Only Me
	County	Only Me
	Postal/ZIP	Only Me
	Country	Only Me
Deployed Location	Street 1	Only Me
	Street 2	Only Me

"My Profile" Category	Display Name	"Show To" Default
	Street 3	Only Me
	City	Only Me
	County	Only Me
	Postal/ZIP	Only Me
	Country	Only Me

Table 4: Additional User Registration Fields that may be Shared within the HSIN Community

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

The external sharing of information from these systems of record is compatible with the following routine uses:[9]

- To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

- To sponsors, employers, contractors, facility operators, grantees, experts, and consultants in connection with establishing an access account for an individual or maintaining appropriate points of contact, and when necessary to accomplish a DHS mission function or objective related to this system of records.

- To other HSIN users in the same operational program supported by an information-technology system, where appropriate notice to the individual has been made that his or her contact information will be shared with other members of the same operational program in order to facilitate collaboration.

[9] *See* DHS/ALL/004 - General Information Technology Access Account Records (GITAAR) SORN (74 FR 49882; September 29, 2009), available at http://edocket.access.gpo.gov/2009/E9-23513.htm.

6.3 Does the project place limitations on re-dissemination?

Dissemination of account information to anyone not involved with the creation, maintenance, deactivation, or deletion of the account is not authorized. Directory and profile information is only available online to active account holders.

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

Records of disclosures of PII outside the Department, used to support identity proofing with third parties by HSIN PMO and/or the third-party identity verification providers are maintained through standard system audit records. Such records are maintained for those PII fields which the PMO actually stores.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The privacy risk is more user registration information than is appropriate may be shared inappropriately outside of DHS.

Mitigation: In order to mitigate this risk, HSIN PMO has set up the IdP so that registrant's identity is verified, but DHS does not collect the additional PII required to conduct the verification

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?

HSIN R3 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. However, certain profile information is mandatory and is derived from the user's application: name, email address, and the Department or Agency with which the user is affiliated. When individuals access their HSIN account information, they will be able to edit the following fields listed below in Table 5.

Editable Fields
About Me
Picture
Certifications
User Interests
Secondary E-Mail
Business Phone
Ext.
Mobile Phone
Fax
Pager
Other Phone
Primary Contact Method
Secondary Contact Method
Job Title
Job Role
Street 1
Street 2
Street 3
City
County
Postal/ZIP
Country
Street 1
Street 2
Street 3
City
County
Postal/ZIP
Country
Street 1
Street 2
Street 3
City
County
Postal/ZIP
Country
Authorization Expiration Date
Security Question
Security Answer

Table 5: Editable fields from HSIN profile page

There may be instances when an individual is unable to authenticate his/her identity using the IdP authentication process. There are several reasons why this could happen. For example, an individual may not have resided in the country long enough to establish a credit or address history and therefore, his identity could not be verified. Another reason could be that the information contained in the commercial databases is incorrect. Alternatively, an individual

could be attempting to illegitimately access HSIN. If an applicant is unable to authenticate his or her identity, an error message will display directing the applicant to call the HSIN Help Desk in order to inquire and/or be directed to the IdP provider to resolve the issue.

HSIN PMO will regularly review and monitor the success rate of the IdP process. HSIN will also clearly communicate the necessary actions an applicant must take in order to correct a failed IdP verification attempt.

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

HSIN R3 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. However, certain profile information is mandatory and is derived from the user's application: name, email address, and the Department or Agency with which the user is affiliated. When individuals access their HSIN account information, they will be able to edit the fields listed above in Table 5. Should a user seek to update profile information that cannot be unilaterally updated, the user may contact the HSIN Help Desk or HSIN Outreach Team for assistance.

In addition above, individuals may seek notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Privacy Office, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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

HSIN registrants are notified in the form of a Privacy Act Statement on their user account creation questionnaire, the publication of this PIA, and the publication of the DHS/ALL/004 - General Information Technology Access Account Records (GITAAR) SORN, 74 Fed. Reg. 49882 (Sep. 29, 2009), in the Federal Register and on www.dhs.gov/privacy.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that HSIN users will not be able to correct or amend their HSIN user information.

Mitigation: A HSIN user shall have the right to edit/modify his profile information in his HSIN Mysite (a.k.a. My HSIN) profile, which is viewable by other HSIN users. A HSIN user shall not have the right to unilaterally modify the registration information retained by the Program for purposes of program and system management. To modify and/or update such information, the user will have to contact the HSIN Help Desk.

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?

HSIN PMO, in coordination with COIs, has the ability to track content access requests through the use of logs and standard, automated workflows defining the movement of content. In so doing, access requests and the movement of content, including re-dissemination, are documentable. Workflows may be utilized to ensure that certain types of marked content cannot, technically, be shared with certain types of users and/or communities.

A HSIN 3.0 System Security Plan (SSP) has been developed by HSIN PMO as of May 2, 2012, in full compliance with DHS 4300a, in anticipation of a final authorization to operate. All HSIN users are required to operate within the bounds of their actual authorities, the Terms of Service, and the rules established by the relevant COI in its Charter. Each COI will establish a Charter that will define its purpose, objectives, and management structure, clearly defining how the COI will work to advance the mission of ISE, IRTPA, and Section 515. HSIN PMO will work in cooperation with each COI to ensure such rules are enforced, and will enforce rules regarding the regular review of COIs and whether their purpose and objectives still justify the operation of the COI. If it is found that a COI is no longer required, PMO will work with the appropriate COI sponsors to eliminate that COI. Collectively, these rules and bounds will mitigate the risk of uses of content on HSIN inconsistent with specific mission areas and authorities.

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

All OPS employees, contractors, and other personnel receive initial on-boarding within 30 days and annual privacy and security awareness training thereafter. HSIN PMO will offer baseline training regarding the topics below; however, the duty to pursue such applicable training is the responsibility of users and their COIs. Privacy-related training topics provided from HSIN PMO include:

- Privacy and FOIA compliance
- Records Management
- COI Roles/Limitations

- Classifications and Markings (PII, SSI, FOUO, etc.)
- Nomination/Validation Certifications
- Mobile Device Access
- Shared Space Activities
- 508 Compliance

Recurring and evolving training topics will be made available to all users from the HSIN Central landing page. HSIN training material will be tailored to ensure the content is relevant to the audience and delivered in flexible pre-recorded modules and short virtual conference training sessions that will allow the opportunity for the trainees to ask questions and explore within their operational context. A training delivery schedule will be established to ensure all site managers, site designers, content managers, and contributors have attended the appropriate courses in advance of the majority of end users. In-person classroom training shall be provided for site managers, site designers, content managers, and content contributors. In addition, to accommodate users spanning the continental U.S and its territories, the training team shall be prepared to support virtual training as required. As supplemental instruction, the training team will provide brief online training modules that will also include best-practice guidance on topics such as document management and content dissemination.

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

HSIN maintains strict permissions controls for use when determining if an applicant for membership to HSIN can become a registered HSIN user. These controls are designed to ensure the security and integrity of HSIN and limit damages, provide users transparency on terms of service, and make enforcing penalties easier.

A qualified individual may only be considered for access to HSIN either by being nominated by a current user or calling the HSIN Help Desk to request that a point of contact be provided. Prospective users will be required to answer a set of questions mapping their attributes to their job function or purpose for using HSIN. The personal and employment data collected for HSIN's identity proofing process is limited to the information necessary to validate the registrant's identity by a legitimate and approved validating authority of the respective COI, the qualifications to enter into particular HSIN collaboration spaces, and/or to access specific information within HSIN.

HSIN Registration information will be saved and stored on HSIN and may be shared by any

DHS entity or component involved in the process of validating the registrant's identity for access to a particular COI or collaboration space.

There is a 45-day period for a user to be vetted into a COI based upon the attributes collected from the questionnaire following his/her successful completion of the initial HSIN registration and identity proofing procedures. After such time, if the user has not been vetted, he/she will need to repeat the registration process. During the vetting process, the prospective user does not have access to any COI until a COI accepts his or her registration. At this initial level of access, migrating users will have read-only access to the home page and HSIN Central until the appropriate COI(s) accept them.

In order to gain access to HSIN, potential users must submit biographical and employment information so that they may be verified as legitimate potential users. This initial verification of identity is conducted through a third-party service. Users may decline to provide their information during this initial review process, but by doing so, their application for access will be rejected and they will not be provided an account. Upon successful review and authentication, each user is assigned to a primary COI based on their information sharing requirements, permissions, and interests. At this point, the User must also access HSIN using a two-factor authentication process, which is standard for all HSIN users. Two-factor authentication helps ensure the integrity of the System by validating the registered user's identity.

The COI sponsor is responsible for evaluating the newly nominated, prospective user for acceptance into its COI. With exceptions, the COI sponsor should be from the same jurisdiction or jurisdiction-type as the majority of the users making up the COI. If there are multiple jurisdictions within a COI or sub-COI, the COI Site Manager must be from the same jurisdiction-type as the majority of users making up the COI. Each COI establishes membership criteria and potential users must meet those requirements in order to gain access to such community. Every COI empowers specific validating authorities to vet potential users into the community. Those validating authorities are responsible for verifying the legitimacy of the potential user. The primary COI and its sponsor(s) will have authoritative responsibilities over the COIs users.

Each COI has one or more sponsors with authoritative responsibility over the COI's users. Responsibility for all nomination and validation procedures for the COI resides with the COI sponsor(s). Nomination and/or validation duties are performed by an authority within the COI's established management—such duties cannot be delegated to an individual or organization outside of the COI's management structure (e.g., a state COI cannot delegate authority to a federal agency who is not also a sponsor of the COI).

The COI Sponsor shall be responsible for evaluating the newly nominated prospective

user for acceptance into its COI. With exceptions, the COI sponsor should be from the same jurisdiction or jurisdiction type as the majority of the users making up the COI. If there are multiple jurisdictions within a COI or sub-COI, the COI sponsor must be from the same jurisdiction-type as the majority of users making up the COI.[10] In addition to these controls, the COI maintains additional criteria for admitting new users into its community. At a minimum, prospective HSIN COI users must possess the following attributes: (1) the applicant's work assignment supports a DHS ISE mission relevant to the COI; (2) the applicant is credentialed to access FOUO information; and (3) the applicant accepts and adhere to the HSIN Terms of Service.

Once verified, the user receives access privileges to only her Primary COI; however, a user can be a member of more than one COI if it is appropriate and the membership criteria are met. At this second level of access, the user has been vetted into a COI and has functional capabilities consistent with the attributes defined during the initial registration questionnaire. A user's COI membership is the principal content-permissions control mechanism for users. The user's COI membership, and all the user attributes that such membership defines, work in concert with specific content tags attached to particular content, to determine the accessibility of content for a particular user.

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?

HSIN maintains strict permission controls when evaluating the credentials for a prospective applicant. These controls are designed to limit damages and ensure that the security and integrity of HSIN are upheld. Additionally, these controls provide users transparency on the terms of service and make enforcing penalties easier. Users may decline to provide their information during the initial review process, but by doing so, their application for access will be rejected and they will not be provided an account. Upon successful review and authentication, each user is assigned to a primary COI.

Each COI will establish a Charter that will include enforceable rules to ensure that PII is only posted to a given COI as required, and only shared to the Shared Space as required to advance the mission of the ISE, IRTPA, and Section 515. HSIN PMO will work in cooperation with each COI to ensure such rules are enforced. Under the terms of these Charters, and the

[10] The requirement that a Sponsor(s) be from the same jurisdiction and/or jurisdiction type as the majority of its COI's user-members should not be interpreted in any way as to limit cross or multi-jurisdictional information sharing and collaboration. This provision is provided to ensure the integrity of the nomination/validation process, having nominators and validators best positioned to perform their duties.

HSIN Terms of Service, each User and content owner in HSIN shall be responsible for ensuring that content loaded onto HSIN is the most accurate and up-to-date available, and that outdated, inaccurate information is withdrawn from HSIN. HSIN PMO will coordinate with each COI to ensure that its Charter includes a provision for removing outdated, no longer accurate, shared content. HSIN PMO will also explore potential development of business processes to remove shared content that has been in the Shared Space for an inappropriately long period of time, archiving the content in conjunction with individual COI rules. The HSIN Program Office will work in cooperation with each COI to ensure all such rules are enforced.

Responsible Officials

Donna Roy
HSIN Program Director
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix

Primary Communities of Interest[11]

DHS Components and Offices	• Chief Financial Officer (CFO) • Citizenship and Immigration Services Ombudsman (CISOMB) • Civil Rights and Civil Liberties (CRCL) • Customs and Border Protection (CBP) • Office of Counternarcotics Enforcement (CNE) • Domestic Nuclear Detection Office (DNDO) • Executive Secretariat (ESEC) • Federal Emergency Management Agency (FEMA) • Federal Law Enforcement Training Center (FLETC) • Office of the General Counsel (OGC) • Office of Health Affairs (OHA) • U.S. Immigration and Customs Enforcement (ICE) • Office of Inspector General (OIG) • Office of Intelligence and Analysis (I&A) • Office of Legislative Affairs (OLA) • Management (MGMT) • National Cybersecurity Center (NCSC) • National Protection & Programs Directorate (NPPD) • Office of Operations Coordination and Planning (OPS) • Office of Policy (PLCY) • Privacy Office (PRIV) • Office of Public Affairs (OPA) • Science and Technology (S&T) • Transportation Security Administration (TSA) • United States Citizenship and Immigration Services (USCIS) • United States Coast Guard (USCG) • United States Secret (USSS)
Departments & Federal Agencies	• Federal Bureau of Investigations (FBI) • Department of State (DOS) • Department of Interior (DOI) • Department of Energy (DOE) • Department of Veterans Affairs (VA) • Department of Defense (DOD) • Defense Information Systems Agency (DISA) • Defense Intelligence Agency (DIA) • Defense Security Service (DSS)

[11] Please note that this is an initial, non-final list of primary COIs submitted as of 06/2012. The list is likely to change, with some COIs currently listed deleted, and others added. The list is likely to change and be revised as HSIN 3.0's Full Operating Capability date nears, and from that date forward.

	• Department of Agriculture (USDA) • Department of Education (ED) • Department of Health and Human Services (HHS) • Department of Housing and Urban Development (HUD) • Department of Justice (DOJ) • Department of State (DOS) • Department of the Treasury • Department of Transportation (DOT)
States	• Alabama • Alaska • American Samoa • Arizona • Arkansas • California • Colorado • Connecticut • Delaware • District of Columbia • Florida • Georgia • Guam • Hawaii • Idaho • Illinois • Indiana • Iowa • Kansas • Kentucky • Louisiana • Maine • Maryland • Massachusetts • Michigan • Minnesota • Mississippi • Missouri • Montana • Nebraska • Nevada • New Hampshire • New Jersey • New Mexico • New York • North Carolina • North Dakota • Northern Marianas Islands • Ohio • Oklahoma • Oregon • Pennsylvania • Puerto Rico • Rhode Island • South Carolina • South Dakota • Tennessee • Texas • Utah • Vermont • Virginia • Virgin Islands • Washington • West Virginia • Wisconsin • Wyoming
Territories	• American Samoa • Guam • Northern Marianas Islands • Puerto Rico • Virgin Islands

Tribal	• Alaska • Great Plains • Northwest • Southern Plains • Eastern • Navajo Pacific	• Southwest • Eastern Oklahoma • Midwest • Rocky Mountain • Western

Table 6: Primary Communities of Interest