



Privacy Impact Assessment  
for the

## **HSIN 3.0 Shared Spaces**

### **On the Sensitive but Unclassified Network**

DHS/OPS/PIA-007

**July 25, 2012**

**Contact Point**

**James Lanoue**

**DHS Operations**

**HSIN Program Management Office**

**202-298-9580**

**Reviewing Official**

**Mary Ellen Callahan**

**Chief Privacy Officer**

**Department of Homeland Security**

**(202)-343-1717**



## Abstract

The Homeland Security Information Network (HSIN) is maintained by the Department of Homeland Security (DHS), Office of Operations, Coordination and Planning (OPS) on the Sensitive but Unclassified (SBU) network. HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources between federal, state, local, tribal, territorial, private sector, international, and other non-governmental partners 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<sup>1</sup>) about the homeland security enterprise, HSIN users, and members of the public who are the subject of documents, reports, or bulletins contained in the HSIN collaboration spaces. This Privacy Impact Assessment (PIA) only covers the substantive material posted and shared within the HSIN collaboration spaces, and not the individual user accounts.<sup>2</sup> Federal records contained within HSIN are governed by the source system of records notice (SORN) and Freedom of Information Act (FOIA). Non-federal records contained in HSIN are governed by the laws and regulations applicable to the relevant foreign, state, or local agencies who participate in HSIN.

## Overview

HSIN is a user-driven, web-based, information-sharing platform that connects homeland security mission partners consisting of DHS and 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 commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism and in undertaking incident management activities. HSIN is designed to allow all relevant, authorized stakeholders<sup>3</sup> access to 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 providing: 1) timely and accurate information related to detecting, preventing, responding to, and recovering from terrorist attacks and natural disasters; 2) timely and accurate information regarding

---

<sup>1</sup> Handbook for Safeguarding Sensitive Personally Identifiable Information (PII) at the Department of Homeland Security, 10-06-2011, [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_guide\\_spii\\_handbook.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf)

<sup>2</sup> See the DHS/OPS/PIA-007 – Homeland Security Information Network (HSIN) R3 User Accounts for more information regarding HSIN user accounts.

<sup>3</sup> See the DHS/OPS/PIA-007 – Homeland Security Information Network (HSIN) R3 User Accounts for more information regarding HSIN user accounts.



vulnerabilities and threats in order to manage incidents, mitigate risks, and reduce post-incident loss of life and property; 3) near-real-time collaboration and incident management; 4) information exchange for emergency management response and recovery operations; and 5) a mechanism to connect disparate information users in a dynamic and diverse information exchange environment.

HSIN, has been declared the “primary system for operational information sharing and collaboration within DHS and with our security partners,” by Secretary Michael Chertoff on January 9, 2006 in a memorandum regarding HSIN Deployment. Furthermore, HSIN directly supports the President’s *National Information Sharing Security Strategy* to “ensure a central data access point for queries and key services to DHS shared data by other critical communities such as law enforcement.”

As the nation’s largest service for the secure and trusted dissemination and sharing of SBU homeland security information, including but not limited to, Sensitive Security Information (SSI), Law Enforcement Sensitive (LES), and For Official Use Only (FOUO), HSIN enables information sharing across the entire homeland security enterprise. By providing an innovative, interoperable, customer-driven, cost-effective information-sharing environment that enables 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, international, and other non-governmental partners through two types of collaborative spaces: HSIN Communities of Interest (COIs)<sup>4</sup> and the HSIN Shared Space. All HSIN COIs are governed by a Charter, which is in turn based on the HSIN COI Model Charter. The HSIN COI Model Charter is a comprehensive statement of the rights, duties, and privileges of a COI and its members. The Model serves as a template from which the specific Charter of each COI is developed.

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. This PIA covers the substantive material discussed or uploaded by the HSIN COIs into the HSIN Shared Space. Each COI Sponsor<sup>5</sup>

---

<sup>4</sup> 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 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 the HSIN Project Management Office (PMO).”

<sup>5</sup> A COI Sponsor must be a public authority, often holding a high-ranking position in the government sector (e.g. Director of Emergency Management or Homeland Security Advisor). Each COI must have at least one sponsor. A COI is approved by the HSIN PMO.



and/or Site Manager is responsible for monitoring the specific content uploaded into the HSIN Shared Space from a given COI, ensuring compliance with the COI Charter and all other sources of HSIN policy<sup>6</sup>. All new COIs must be approved by the HSIN PMO. The PMO also ensures that each COI has a comprehensive Charter, based on the HSIN Model COI Charter, and has a public-sector, government Sponsor. Content on the Shared Space is ultimately controlled by its original publisher and the COI from which it was published. Content on the Shared Space is regulated based on the content markings that have been applied to it by its originator, the Trusted Vetting Official (TVO) of a given COI, and the credentials of a user attempting to view a particular content item.

HSIN Program Management Office (PMO) is a data steward and is not responsible for the content that users and COIs post to any element of HSIN. HSIN PMO does not retain custody or exclusive control over content at any location within HSIN, as the content is governed under relevant and applicable federal, state, local, territorial and tribal information management, privacy, public disclosure (or “sunshine”) and records management statutes, regulations, or memoranda of understanding between DHS and content providers.

### Types of Information included in HSIN COIs

HSIN is the designated information-sharing portal for DHS and serves as the principal platform for consolidation and/or interoperability with other DHS information-sharing portals, to include, but not limited to, Virtual USA, and the Emergency Management and Response-Information Sharing and Analysis Center (EMRISAC), amongst other planned portal consolidations. This capability is critical to both day-to-day operational decision-making and successful execution of large-scale emergency operations. HSIN is the only federal portal that provides information sharing among DHS and its federal, state, local, tribal, territorial, private sector, and other non-governmental partners across the full spectrum of homeland security missions. HSIN facilitates information sharing and coordination across all DHS mission areas, including, but not limited to:<sup>7</sup>

- Emergency Management Community;
- Critical Infrastructure Community;
- Law Enforcement Community;
- Public Health;

---

<sup>6</sup> All COIs must have a public sector, government sponsor, under the HSIN Model COI Charter. All COIs will be required to have a charter that outlines their authorities, rights, roles, and privileges of its members. The HSIN PMO will retain a copy and require that COI Charters be modified if the mission or substantial criteria changes.

<sup>7</sup> Please note that this list includes major mission areas, which are not themselves Communities of Interest, but rather, include COIs within each mission area.



- Intelligence Community; and
- Emergency Services.

Most of the information shared through HSIN does not contain PII; is used to provide the homeland security enterprise with nationwide situational awareness.

### HSIN Account Provisioning

HSIN maintains strict permission controls when evaluating access credentials for a prospective applicant. In order to gain access to HSIN, potential users must submit biographical information to verify their identity and employment information and must articulate a mission need to use HSIN. In order to become a HSIN user, an individual must be nominated or may gain access through federated membership;<sup>8</sup> both processes require identity verification and a mission need assessment. This initial verification of identity is conducted, in part, through use of a third-party service. DHS has published a separate PIA that covers the specifics of the HSIN user account.<sup>9</sup> DHS evaluates mission-based roles to access information in both the COI and Shared Space through a series of questions that determine what information the user may access or discover.

Currently, there are eight categories, or controlling content tags, used to determine access to information in the Shared Space: 1) Law Enforcement Sensitive (LES); 2) Protected Critical Infrastructure Information (PCII); 3) SBU; 4) U.S, Citizen only;<sup>10</sup> 5) DHS-only; 6) Federal-only; 7) State/local/tribal/territorial-only; 8) Private Sector-only; and any combination thereof. These tags are controlling tags. In order for users to access information, their permissions must match the controlling tags placed on the information. For example, a piece of information may be tagged as “LES, Federal-only,” in which case only users with both the roles of LES and Federal-only will be able to access the information. Information may be discoverable, but not accessible via the HSIN Shared Space by those who do not have the appropriate permissions; in these instances, the user must go through traditional methods to access the information from the originator, rather than being able to access it immediately. In some cases, there may be additional, non-controlling tags used to mark content, which simply provide a user notice of what particular content contains, but does not control access to content.

---

<sup>8</sup> Future sources of federated, HSIN user membership are likely to include Law Enforcement Online (LEO) and Regional Information Sharing Systems (RISSNET).

<sup>9</sup> DHS/OPS/PIA-008 Homeland Security Information Network (HSIN) R3 User Accounts

<sup>10</sup> This tag indicates that the content may only be accessed by U.S. Citizens and not, for example, international users. During the registration process, it is determined whether a prospective user is a US citizen, or not. If not, and the registrant is thus of international origin, the international user must go through a special, 4300A exception process, to be allowed access to HSIN.



## HSIN Communities of Interest (COIs)

As part of the nationwide information-sharing efforts that HSIN supports, HSIN includes different COIs within the network. HSIN COIs are separate collaborative environments wherein users involved in the same subject matter area or industry may post and view potentially relevant news and information and utilize collaborative tools. The posting environment functions like an internet message board where threads<sup>11</sup> are posted and users' replies are exchanged and posted within threads. Collaborative tools consist of document libraries (common resources), sites/sub-sites, alerts, web/video conferencing, instant messaging, and calendars—allowing COIs to choose which ones to enable. Each COI Sponsor is responsible for the content maintained and shared within the COI, and through the COI to the Shared Space.

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). Each COI establishes membership criteria that potential users must meet to gain access to said community. HSIN PMO works in cooperation with each COI to ensure such rules are enforced. A regular review of COIs will be conducted by HSIN PMO to validate and justify a COI's purpose, objectives, and operational need.

Every COI has specific validating authorities who review and approve potential users into the community. The validating authorities are responsible for verifying the legitimacy of the potential user's application into the COI. Prospective HSIN users possess, at minimum, the following attributes: (1) the applicant's work assignment supports a DHS Information Sharing Environment (ISE) mission relevant to the COI; (2) the applicant is determined to have valid access to SBU information including FOUO information through the nomination and validation process; and (3) the applicant accepts and adheres to the HSIN Terms of Service. In addition to these controls, individual COIs may maintain additional criteria for admitting new users into their communities.

Upon approval of a HSIN account, each user is assigned to a primary COI based on the user's information-sharing requirements, permissions, attributes, and interests.<sup>12</sup> A HSIN Standard Operating Procedure will define the details of this process. The user then becomes a member of the COI after passing that COI's nomination and validation process. A user can ultimately become a member of more than one COI if membership in such COIs is appropriate and if all membership criteria are met. A user's COI membership is the principal content-

---

<sup>11</sup> User-posted subjects for discussion.

<sup>12</sup> As noted in the HSIN COI Model Charter, "a user will identify with one primary COI. This COI will be selected by the user from a list of qualified options based upon the user's attributes. The validator of the COI selected will need to confirm and vet the user for membership. This primary COI will be the community held accountable for all activities from that user. Likewise, a user is accountable to the rules of every COI they are a part of."



permissions control mechanism for users. The COI membership works directly in conjunction with content tags to ensure that content is shared appropriately and securely. A user may be nominated and validated into additional COIs after their primary appointment is completed.

An initial list of primary COIs is provided in the Appendix below. Additional COIs created or eliminated as part of an annual review cycle will be added to or removed from the Appendix, as needed.

COIs may have a number of sites and/or sub-sites within them. For example, the Federal Emergency Management (FEMA) COI has multiple sub-sites created to meet specific needs. The HSIN EM COI includes sub-sites such as the American Red Cross Disaster Operations Center, the FEMA Operations Center, the National Response Coordination Center, and sites for each of the nine FEMA-coordinated Emergency Support Functions. Access to information in sub-sites may be more restricted than in the overall COI. For example, information in the American Red Cross Disaster Operations Center may not be available to all individuals who are members of the HSIN EM COI.

An additional feature of HSIN 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.

Documents and materials posted in the COI may be marked for dissemination based on the eight criteria noted above; however, materials are available to all members in the COI as soon as they are posted. Some materials may contain PII. HSIN users are reminded at the time of posting that his or her materials will be shared with all members of that COI, and possibly further. Depending on the membership of a particular COI, this may mean broad sharing with federal, state, local, tribal, and/or territorial agencies, or more narrow sharing with DHS-only because the COI only permits access by DHS employees. A COI can establish its own specific criteria around content posting. Furthermore, there are other rules around sharing information related to active investigations that may be established by an agency or COI. As access and role permissions develop in HSIN, the use of tags within the COI will be added as an additional control beyond membership in a particular COI.

### HSIN Shared Space

The HSIN Shared Space allows authorized stakeholders and content contributors to publish finished products and relevant documents that that (1) have appropriate markings providing sharing permissions at the document level, and (2) are targeted to an authorized audience based on their credentials and related COI and system-wide rules for sharing. Before uploading information into the HSIN Shared Space, COI users submit content to their COI's TVO for dissemination approval. The TVO is a user within the COI, selected by the COI Sponsor and trained by the HSIN PMO, to perform such duties as content management including content dissemination outside of the COI. The COI Sponsor and Site Administrator, working in



conjunction with the TVO, determines the COI's rules for how, when, and which content may be shared into the Shared Space. TVOs determine whether the information content is appropriate for sharing, is relevant to the DHS mission area, as listed above, and is tagged as necessary to limit access. The content owner must mark content as either "accessible," meaning it can be found and viewed in full upon being added to the Shared Space, or as "discoverable," meaning it can be found by any user through the Shared Space who meets the criteria associated with the content but not viewed until a request is approved by the TVO or content owner. The content owner remains the owner of the document when shared through the Shared Space.

## **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 Chertoff reorganization of the Department) to "(1) provide situational awareness and a common operating picture for the entire Federal government and for State, local, tribal and territorial governments as appropriate, in the event of a natural disaster, act of terrorism, or other man-made 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 3.0.<sup>13</sup>

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, established 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."<sup>14</sup>

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

HSIN is a tool for information sharing within the homeland security enterprise. The information contained within HSIN is covered by the applicable SORN(s) depending on the source of the record for federal records. Non-federal records contained in HSIN are governed by

<sup>13</sup> Refers to the next release of HSIN. "HSIN" and "HSIN 3.0" are used interchangeably throughout this document.

<sup>14</sup> Chertoff, Secretary Michael. *Homeland Security Information Sharing Network Deployment*. January 9, 2006





the laws and regulations applicable to the relevant foreign, state, or local agencies that participate in HSIN and by relevant foreign, state, or local agencies that are the stewards of the information. For example, records accessible within HSIN related to the situational awareness mission of OPS are covered by DHS/OPS-003—Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, 75 Fed. Reg. 69689 (Nov. 15, 2010).

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

Yes. As of May 2, 2012, the HSIN Program Management Office (PMO) had developed a HSIN 3.0 System Security Plan (SSP) in full compliance with DHS 4300a, in anticipation of a final authorization to operate (ATO). In addition, HSIN maintains a HSIN/Common Operational Picture (COP) Incident Response Plan to guide the PMO in responding to security incidents.

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

Information maintained within HSIN is subject to its source record retention policy, as discussed in Section 5.1, including deference to the records management rules and procedures of specific content owners, including users and COIs of all kinds, from all originating jurisdiction types. The HSIN PMO is responsible for ensuring retention of records for the content it publishes and retains custody and control over on HSIN. It is responsible for adhering to the National Archives and Records Administration (NARA) schedule N1-563-11-010.

Documents “published” from day-to-day operations, including the HSIN instant-messaging and web-conferencing tools are, stored for five years and then destroyed.

Records that are part of Phase 2 or 3 Events<sup>15</sup> are transferred to the National Archives for permanent retention five years after the event or case is closed.

---

<sup>15</sup> A Phase 2 Event is an event meeting any of the four criteria outlined in the Homeland Security Presidential Directive 5 (HSPD 5), including: (1) Man-made events and natural disasters, chemical, biological, radiological, nuclear, explosive, and cyber events, floods, fires, and tsunamis, and other events causing loss of life and large scale evacuations (likely leading to a Presidential Directive Decision) and requiring significant Federal involvement; (2) an event significantly impacting the US critical infrastructure and industrial accidents occurring in densely populated areas; (3) a credible threat with possible/actual terrorist nexus and US homeland security implications; and; (4) a National Security Special Event whose public safety, threat, complexity, or other attributes require extensive Federal information sharing, interagency support, and incident management preparedness. A Phase 3 Event is an event so catastrophic that the Federal Government must assume the highest level of operational posturing and activity; and/or a domestic event with a confirmed terrorist nexus. (Source: System Schedule for National Operations Center (NOC) Senior Watch Officer (SWO)/Tracker Logs, United States Department of Homeland Security, Headquarters Systems Schedules, Office of Operations Coordination, 12/8/11).



**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 does not apply to the HSIN 3.0 Shared Space because no information is collected directly from the public.

## Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

**2.1 Identify the information the project collects, uses, disseminates, or maintains.**

Information collected, used, disseminated and maintained within HSIN Shared Space varies by the mission need of each COI. Information posted in the COIs is based on the stated mission of the COI, as documented in each COI Charter. Information posted in the Shared Space is based on the mission of DHS. It is possible that a high volume of content retained in a given COI will never be shared to the Shared Space, or that a high volume will be shared to Shared Space – it will be dependent on the particular rules of a particular COI and its users. The information contained within HSIN is covered by the applicable SORN(s) depending on the source of the record for federal records. Non-federal records contained in HSIN are governed by the laws and regulations applicable to the relevant foreign, state, local or private parties that participate in HSIN and by relevant foreign, state, local or private parties that are the stewards of the information.

Information posted in the COIs and the Shared Space will be tagged based on the following eight attributes: 1) LES; 2) PCII; 3) SBU; 4) U.S. Citizen-only;<sup>16</sup> 5) DHS-only; 6) Federal-Only; 7) State/local/territorial/tribal-only; 8) Private Sector only; and any combination thereof. Access to information made available in the COI is based on membership in the COI and currently is not controlled through tagging of information in the same way as in the Shared Space. The tags listed above are controlling tags in the Shared Space. In order for users to access information, their permissions must match the controlling tags placed on the information. For example, a piece of information may be tagged as “LES, Federal-only,” in which case only users with both the roles of LES and Federal-only will be able to access the information. Information may be discoverable, but not accessible via the HSIN Shared Space by those who do not have the

---

<sup>16</sup> This tag indicates that the content may only be accessed by US citizens and not, for example, international users. During the registration process, it is determined whether a prospective user is a US citizen, or not. If not, and the registrant is thus of international origin, the international user must go through a special, 4300A exception process, to be allowed access to HSIN.



appropriate permissions; in these instances, the user must go through traditional methods to access the information from the originator, rather than being able to access it immediately. In some cases, there may be additional, non-controlling tags used to mark content, which simply provide a user notice of what particular content contains, but does not control access to content. Content containing PII<sup>17</sup> can be marked as such using an additional, non-controlling content tag, in addition to the eight controlling tags listed above.

Most of the information shared through HSIN does not contain PII, however, what PII is on HSIN will likely be of diverse type and origin, as noted below. HSIN may contain PII information on individuals known, reasonably believed to be, or suspected of being involved in or linked to domestic, foreign, or international terrorist groups; individuals related to activities or circumstances where the health or safety of that individual may be threatened; individuals with outstanding warrants in any federal, state, local, territorial, and/or tribal area; and individuals who may pose a threat<sup>18</sup> to the United States. Access to such information, along with the standards for its sharing, are based on individuals COI membership, their credentials, the manner in which the content is marked and the decision of a COI to allow such information to be shared to the Shared Space. PII is considered a content marker in the HSIN system and not a controlling tag. As noted above, while most of the information shared within HSIN does not contain PII, what PII is on HSIN will likely be of diverse type and origin. To the extent PII is part of HSIN, the following information may be made available through HSIN:

- Full name;
- Date and place of birth;
- Social Security Number;
- Citizenship;
- Contact information including phone numbers and email addresses;
- Address;
- Physical description including height, weight, eye, and hair color;
- Distinguishing marks including scars, marks, and tattoos;
- Automobile registration information;

---

<sup>17</sup> The definition of PII which HSIN shall follow is provided in the footnote below Handbook for Safeguarding Sensitive Personally Identifiable Information (PII) at the Department of Homeland Security, 10-06-2011, [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_guide\\_spII\\_handbook.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spII_handbook.pdf)

<sup>18</sup> Defined as a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property. DHS Risk Lexicon at 3.3 (September 2008).



- Watch list information;
- Medical records;
- Financial information;
- Results of intelligence analysis and reporting;
- Ongoing law enforcement investigative information;
- Historical law enforcement information;
- Information systems security analysis and reporting (e.g. information collected for analysis to ensure security of critical infrastructure and sectors);
- Public source data including commercial databases, media, newspapers, and broadcast transcripts (e.g. information collected during an incident response for situational awareness, which is all public source, used for immediate operations needs);
- Intelligence information including links to terrorism, law enforcement, and any criminal and/or incident activity, and the date information is submitted;
- Intelligence and law enforcement information obtained from federal, state, local, tribal, territorial, private sector, international, and other non-government partners;
- Law enforcement, domestic security and emergency management officials and private sector entities or individuals;
- Information obtained from the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC) or terrorist watchlists about individuals known or reasonably suspected to be engaged in conduct constituting, preparing for, aiding, or relating to terrorism;
- Limited information about the provider of the published content, when the provider's information is critical to a law enforcement and/or other DHS mission (e.g. an investigation lead, an intelligence analyst, or an emergency responder).
- The date and time national disaster information is submitted, and the name of the contributing/submitting individual or agency; and
- Name of the contributing or submitting agency, organization, or individual.



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

Sources of the information collected, used, and maintained within HSIN include, open source information available on the Internet, such as news reports; finished products, such as homeland security intelligence or law enforcement products; meeting notices; information bulletins; and federal, state, local, tribal and territorial law enforcement notices.

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

Daily, weekly, and monthly reports, notices, and bulletins, as well as real time law enforcement and emergency management alerts, are compiled and shared within HSIN. These law enforcement, intelligence, or situational awareness products fulfill the HSIN mission of sharing information within the homeland security enterprise related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, and natural disasters. These reports are compiled by subject matter experts and may be based on information collected from federal, state, local, tribal, and territorial law enforcement databases, publicly available news articles and open source information found on the Internet, or in public records.

## **2.4 Discuss how accuracy of the data is ensured.**

HSIN relies on the data within the original source systems being accurate and does not collect information directly from the public or any other primary source. These original source systems may be federal, state, local, tribal, territorial systems, private-sector, and/or international users' systems. The law enforcement, intelligence, incident management, or situational awareness products generated and shared by HSIN users rely on a variety of source record systems and public records to verify the accuracy of information before it is shared within HSIN.

## **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:** There is a privacy risk that HSIN users will provide more PII than is appropriate within HSIN.

**Mitigation:** Each COI's charter includes rules, including the COI's rules on what types of content shall be shared to the Shared Space, how and whether PII content shall be marked, where PII may be included in a given COI in the first place, and so on, that are enforced to ensure that PII is only posted to a given COI as required, and only placed in the Shared Space as needed to advance the mission of the ISE, IRTPA, and Section 515 of the Homeland Security



Act. As a result, content containing PII may be properly identified with content markings within a given COI prior to being shared in the Shared Space; however, the markings function only as a tag, not as a control. Additional content markings will ensure that access to such content is limited to only those individuals with the appropriate credentials and need-to-know criteria. HSIN PMO works in cooperation with each COI to ensure such rules are enforced.

**Privacy Risk:** Since HSIN is a tool for sharing information from original source systems and does not collect information directly from individuals, there is a privacy risk that the data in HSIN will become inaccurate.

**Mitigation:** Each COI's charter has enforceable rules, to be enforced by the COI Sponsor, Administrator, and all other members of the COI's management, to ensure that PII is only posted to a given COI and to the Shared Space as authorized, to advance the mission of the ISE, IRTPA, and Section 515 of the Homeland Security Act. The charters also state as a matter of policy, such information is removed from the system as soon as appropriate and no longer required. HSIN PMO coordinates with each COI to ensure that all Charters include a provision for removing outdated or inaccurate content. HSIN PMO is also exploring development of business processes to remove shared content from the Shared Space when it no longer appears to be required, and to establish a standard rule across all COIs requiring their regular review and removal of content that has been posted for an extensive period of time and which may no longer be accurate.

HSIN PMO works in parallel with the COI Sponsor(s) and/or Site Administrators of each COI to ensure that documents posted in the Shared Space are reviewed annually for content relevancy and accuracy. Additionally, HSIN PMO monitors and produces regular reports capturing inactive COI sites. This helps to ensure that unused community sites are purged from the system. Lastly, HSIN PMO will work with all COIs to ensure all such rules outlined in the Terms of Service, COI Charter, and all other applicable documents are enforced.

## 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 allows users to share information of a wide variety of types, within their COIs or the HSIN Shared Space consistent with their individual authorities and missions. Most of the information shared within HSIN does not contain PII and is used to provide the homeland security enterprise with nationwide situational awareness. The charter for each COI provides users with guidance on what information is appropriate to be maintained in the COI. Information maintained in the COI is tagged, but access at the document level is not controlled for access because everyone in the COI was validated as having a need to know the information and meeting the criteria for entry prior to being approved by the Sponsor. If information is shared in



the COI, all members of the COI are able to review it. Future releases of HSIN will put in place additional technical controls. Information maintained in the Shared Space will be viewable based on the tags.

On occasion, the following products shared within HSIN may contain PII:

- Law Enforcement Alerts, including Be On the Lookouts (commonly referred to as BOLOs), Amber Alerts, Silver Alerts, and Federal Protection Service (FPS) Alerts;
- Requests for Information (RFIs);
- Finished Intelligence Products;
- Officer Safety Bulletins; and
- Suspicious Activity Reports (SARs).

These alerts, bulletins, and products are used within HSIN to provide stakeholders across the homeland security enterprise with effective and efficient collaboration for decision-making and accurate, timely information sharing and situational awareness. Daily, weekly, and monthly reports, notices, and bulletins are compiled and shared within HSIN to fulfill its mission of sharing information within the homeland security enterprise related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, and natural disasters.

### **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. HSIN PMO, however, is the administrative agency responsible for management, operation, and maintenance of all aspects of HSIN—in coordination with OPS and the whole community of HSIN stakeholders. HSIN PMO sets goals to support development and implementation of the HSIN environment, develops training for HSIN users, and serves as the



data governance steward for HSIN policy documents, including the HSIN Model Charter and HSIN Terms of Service.

HSIN PMO is a data steward and is not responsible for the content that users and COIs post to any element of HSIN. HSIN PMO does not retain custody or exclusive control over content at any location within HSIN, as the content is governed under relevant and applicable federal, state, local, territorial and tribal information management, privacy, public disclosure (or “sunshine”) and records management statutes, regulations, or memoranda of understanding between DHS and content providers.

### **3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** There is a privacy risk that information within HSIN may be used in a manner that is inconsistent with a HSIN user’s specific mission area and authorities.

**Mitigation:** All HSIN users may have the ability to be nominated into a specific COI however, they must meet that COI’s membership criteria. By identifying these controls for membership, HSIN aims to mitigate the privacy risk that information within HSIN, or the COI, may be used in an inconsistent manner not aligning to a user’s specific mission area. Additionally, all HSIN users are required to operate within the bounds of their actual authorities, the Terms of Service, and the rules established by their COI in its charter. Each COI establishes a charter that defines the COI’s purpose, objectives, and management structure, clearly defining how the COI will work to advance the mission of the ISE, IRTPA, and Section 515 of the Homeland Security Act. HSIN PMO works in cooperation with each COI to ensure such rules are enforced. A regular review of COIs will be conducted by HSIN PMO to validate and justify a COI’s purpose, objectives, and operational need. When conducting the review, the PMO will ensure direct consult, as required, with essential parties such as Privacy Office, Office for Civil Rights and Civil Liberties, and Office of General Counsel. If it is found that a COI is no longer required, HSIN PMO works with the appropriate COI sponsor(s) to eliminate that COI. Additionally, HSIN PMO will monitor and produce regular reports that identify inactive COIs and/or sites. This process will be defined by policy established by the PMO. Having identified inactive sites, the PMO will consult with the appropriate COI Sponsors to either increase activity, or eliminate the COI and/or sites in question. By regularly eliminating inactive COIs/sites, HSIN will ensure that only COIs and sites that actually continue to serve a mission-related purpose remain on the network. Collectively, these rules and bounds will mitigate the risk of uses of content on HSIN that are inconsistent with specific mission areas and authorities.

**Privacy Risk:** There is a privacy risk that too much information will be published to the HSIN Shared Space.

**Mitigation:** Each COI’s charter includes enforceable rules to ensure that PII is only posted to a given COI as required, and only posted to the Shared Space as needed to advance the





mission of the Information Sharing Environment, IRTPA, and Section 515 of the Homeland Security Act. HSIN PMO works in cooperation with each COI to ensure such rules are enforced.

The HSIN Shared Space allows authorized stakeholders and content contributors through the TVO to publish finished products and relevant documents that (1) have appropriate markings providing sharing permissions at the document level; and (2) are targeted to an authorized audience based on their credentials and related COI and system-wide rules for sharing. Before uploading information into the HSIN Shared Space, COI users first create and submit content to their COI's TVO for approval. The TVO is responsible for reviewing content and applying the information-sharing rules and preferences of the particular COI to ensure the information can appropriately be shared. The TVO also reviews the credentials required for users outside the COI, and whether other COIs and federated members have sufficient rights and needs to view the shared content in the Shared Space, in accordance with the content creator's original stipulations and all other COI and HSIN policies.

Information content is considered appropriate for sharing when the TVO determines that it is in both the COI's and the greater HSIN community's interest to have such content shared, either on a case-by-case or rules-based basis. Content is shared based on the markings the TVO attaches to the content and the corresponding credentials of a user with whom such content may be shared. The TVO approves, rejects, or modifies the request for sharing. At the TVO's discretion, content may be marked as accessible or discoverable. If marked accessible, the content can be viewed in full by authorized users based upon content's markings and tags. If marked as discoverable, the user must request access to the information and the TVO or content owner must approve the request prior to sharing the information with the user.

## 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.**

HSIN Shared Space does not collect any information directly from individuals, and therefore does not have an opportunity to provide notice of such collection. Notice of collection by the underlying government systems performing the original collection is described in the individual PIAs and SORNs for those systems. For example, many DHS records accessible within HSIN are covered by the following SORN: DHS/OPS-003—Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, 75 Fed. Reg. 69689 (Nov. 15, 2010). Non-federal partners are responsible for following their own requirements for providing notice.



### **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 or decline to the basic rights, duties and privileges defined for HSIN users. There are no opportunities for users to seek consent to specific uses, or for individuals to decline to provide information or opt out of the sharing environment. HSIN relies on the source record systems to provide opportunities to individuals from whom this information is collected.

Given the mission of HSIN to support homeland security, most of the source record systems that provide PII were collected for law enforcement purposes; therefore, generally, the information will not be available to the public because it could impede law enforcement activities.

### **4.3 Privacy Impact Analysis: Related to Notice**

**Privacy Risk:** There is a privacy risk that individuals are not provided adequate notice that their information will be shared within HSIN.

**Mitigation:** Individuals are provided notice that their information may be shared outside of DHS through the Routine Use sections of the applicable SORNs, and through the publication of this PIA. Additionally, non-federal entities may only share information with DHS when it is directly related to the DHS mission. The TVO reviews all submissions for sharing to ensure it meets this criteria.

## **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 users and COI Sponsors are responsible for adhering to the applicable federal, state, local, territorial, and/or tribal records management laws, regulations, and policies that apply to the content they publish or over which they retain custody and control, regardless of such content's media format. Each member's content contributions will follow that user's applicable laws such as, FOIA, Privacy Act, and Records Management requirements.

HSIN PMO is responsible for ensuring retention of records for the content which it itself publishes and retains custody and control over on HSIN. It is responsible for adhering to two NARA schedules for records management for such content, including:



- Five-year record—Documents “published” from day-to-day operations, including HSIN’s instant-messaging and web-conferencing tools.
- Permanent record—Documents “published” from a crisis event stemming from Level II or Level III activities, to be held by HSIN for the first five years and then transferred to the National Archives for permanent retention.

As a matter of policy, HSIN provides capacity for data storage for COIs for content that is up to (and no more than) five years old, starting from the content item’s last modification date. Content owners or COIs may contact the PMO to set up alerts for COI sponsors regarding expiring data that may be up for deletion. After that time, content owners or COIs must directly provide for the archiving of their content and records, if required under the laws and policies of their original jurisdictions. Alternatively, on a case-by-case basis, HSIN PMO may offer additional services to COIs regarding data transfer prior to purging if and when requested by a COI or user. Ultimately, however, records management is the responsibility of content owners and/or the content-controlling COI.

## 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** Because HSIN relies on information from other systems, it is possible that incorrect information could be included in HSIN and then corrected in the underlying system. Consequently, a search in HSIN could return the incorrect information.

**Mitigation:** Each COI’s charter includes enforceable rules to ensure that PII is only posted to a given COI as required, and only posted to the Shared Space as needed to advance the mission of the Information Sharing Environment, IRTPA, and Section 515. HSIN PMO works in cooperation with each COI to ensure such rules are enforced. Under the terms of their charters, and the HSIN Terms of Service, users and content owners in HSIN are 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 coordinates with each COI to ensure that its charter includes a provision for removing outdated, no longer accurate, shared content. HSIN PMO is also exploring developing a business process to remove shared content that has been in the Shared Space for an inappropriately long time, and archiving that content. HSIN PMO works in cooperation with each COI to ensure all such rules are enforced.



## 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.**

HSIN is an information-sharing tool for the homeland security enterprise. The authorities listed in Section 1.1 of this document assign DHS responsibility for providing intelligence fusion, threat information, and incident management capabilities horizontally across the federal government and among federal, state, local, tribal, territorial, private sector, international, and other non-governmental partners. HSIN is the primary platform by which information is shared, fulfilling the DHS mission requirements to provide encompassing, integrated situational awareness both in the form of disseminated information and in the common operating picture.

HSIN maintains strict permissions controls when evaluating the credentials for a prospective applicant. These controls are designed to limit potential 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 access HSIN using a standard two-factor authentication process. Two-factor authentication helps to ensure the integrity of the system by validating the registering user's identity. 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. Each COI establishes membership criteria and potential users must meet those requirements in order to gain access to the COI. 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's application. The primary COI and its Sponsor(s) have authoritative responsibilities over the COI's users. Responsibility for all nomination and validation procedures for the COI resides with the COI's 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. For example, a state COI cannot delegate nomination/validation authority to a federal agency that is not a sponsor of the COI. The COI Sponsor is responsible for accepting newly nominated prospective users into the COI. Although there may be some exceptions, the COI Sponsor is usually from the same jurisdiction or jurisdiction type (e.g. a State sponsor for a COI whose members are primarily from a state) as the majority of the users making up the COI. When there are multiple jurisdictions within a COI, the COI Sponsor is strongly preferred to be from the same jurisdiction type as the majority of users making up the COI.



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 has a need to access forms of SBU information, including but not limited to FOUO information, that is established during the nomination, validation, and user registration process; and 3) the applicant accepts and adheres to the HSIN Terms of Service. In addition to these controls, individual COIs may maintain supplemental criteria for admitting new users into their communities. Verified users are given access privileges to only their Primary COI; however, users can be members of more than one COI if it is appropriate and the membership criteria are met.

All HSIN users are required to operate within the bounds of their actual authorities, the Terms of Service, and the rules established by each COI in its respective charter. Each COI will establish a charter that defines its purpose, objectives, and management structure, clearly defining how the COI will work to advance the mission of the ISE, IRTPA, and Section 515 of the Homeland Security Act. HSIN PMO will work in cooperation with each COI to ensure such rules are enforced. Additionally, a regular review of COIs will be conducted by HSIN PMO to justify their purpose, objectives, and operational need. If it is found that a COI is no longer required, the 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.

The HSIN Shared Space allows authorized stakeholders and content contributors to finished products and relevant published documents that: (1) have appropriate markings providing sharing permissions at the document level; and (2) are targeted to an authorized audience based on credentials and related COI and system-wide rules for sharing. Before uploading information into the HSIN Shared Space, COI users submit content to their COI's TVO for approval. The TVO is responsible for reviewing content and applying the information sharing rules and preferences of the relevant COI to ensure the information can appropriately be shared. The TVO also reviews the credentials required for users outside the COI to access content in the Shared Space, consistent with the content creator's original stipulations and all other COI and HSIN policies. TVO determines whether the information content is appropriate for sharing, is relevant to the DHS mission, and is tagged as necessary to limit access.

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

HSIN is not a system of records under the Privacy Act; rather, it is a tool for information sharing within the homeland security enterprise. The information contained within HSIN is covered by the applicable system of records notice(s) depending on the source of record.

## **6.3 Does the project place limitations on re-dissemination?**

Yes, HSIN has system controls that limit and track the re-distribution of information from



the COIs and within the Shared Space.

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

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

## **6.5 Privacy Impact Analysis: Related to Information Sharing**

**Privacy Risk:** Authorized users may inappropriately disclose this information, either intentionally or unintentionally.

**Mitigation:** All HSIN users are required to complete privacy training that addresses the appropriate and inappropriate uses and disclosures of information they receive as part of their official duties. HSIN PMO will provide baseline training to all HSIN users of all types, and make SOPs, guides, etc. available on the system itself. Per the COI Model Charter and Terms of Service, it is the responsibility of the COI Sponsor to ensure all of his/her members are appropriately trained. All users also read and sign the HSIN Terms of Service outlining basic rights, duties, and privileges defined for HSIN users. Prior to setting up a new COI, COI sponsors complete a Model Charter that details the appropriate use of PII within each COI. HSIN PMO keeps the Model Charters on file.

All use of the system and access to data is monitored and audited. Should a user inappropriately disclose information, the disclosure will be referred to the appropriate internal investigation entity and the individual is subject to loss of access. Additionally, users are required to undergo full identity access management to be recertified annually.

HSIN PMO, in coordination with the respective COI, has the ability to track content access requests through the use of logs and standard workflows defining the movement of content. In so doing, access requests and the movement of content, including re-dissemination to parties outside the Department, can be documented. Workflows may be used to ensure that certain types of marked content cannot technically be shared with unauthorized users or communities.



## 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?**

Since HSIN is not a Privacy Act system of records, it does not have a SORN detailing procedures for individuals to access and correct their information. The information within HSIN is covered by the applicable system of records notice(s) depending on the purpose and source of record. For example, many DHS records accessible within HSIN are covered by DHS/OPS-003—Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, 75 Fed. Reg. 69689 (Nov. 15, 2010).

Individuals seeking notification of and access to any record contained in the source 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.

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

The information shared through HSIN from underlying DHS-owned systems may be corrected by means of the processes described in the PIAs and SORNs for those systems. HSIN users who share information within the COIs or HSIN Shared Space are responsible for the integrity of the data they provide. If erroneous information is entered, the user is required to correct his or her entry immediately upon determining it to be incorrect. This procedure can and may be done at any time upon identification of incorrect information, so long as the user had editable rights to such a document. To clarify, this requirement applies to any data a user has access to, not just data provided by the user.

At times, erroneous information may be published in a finished intelligence product. When incorrect information is discovered, a revised product is published to correct the information or note the questionable fact or content; the incorrect product is removed from HSIN. For any products externally disseminated and in need of recall or correction, a recall message or revised product is disseminated to the recipients of the original product(s) with appropriate instructions.



Individuals seeking notification of and access to any record contained in the source system of records, or seeking to contest its content, may submit a request in writing to the Headquarter 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.

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

Individuals seeking correction of and access to any record contained in the source 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.

### **7.4 Privacy Impact Analysis: Related to Redress**

**Privacy Risk:** There is a privacy risk that individuals will be unable to correct or amend information about them that is shared in HSIN.

**Mitigation:** Individuals may correct information as provided for in the applicable SORN or via the process afforded by international, state, local, territorial, or tribal HSIN users.

## **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, can be documented. Workflows may be used to ensure that certain types of marked content cannot technically be shared with unauthorized users and/or communities.

As of May 2, 2012, HSIN PMO has developed a HSIN 3.0 System Security Plan (SSP) in





full compliance with DHS 4300a, in anticipation of a final ATO. All HSIN users are required to operate within the bounds of their actual authorities, the Terms of Service, and the rules established by each COI in its respective Charter. Each COI will establish a charter that defines its purpose, objectives, and management structure, clearly defining how the COI will work to advance the mission of the ISE, IRTPA, and Section 515 of the Homeland Security Act. 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, the PMO will work with the appropriate COI sponsors to eliminate that COI. Collectively, these rules and bounds will mitigate the risk of use of HSIN content in a manner 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. In addition, the HSIN PMO offers baseline training regarding the privacy-related topics listed below to all HSIN users, of all kinds, from all jurisdiction types, in various mediums, as a function of becoming a user. 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

Recurring and evolving training topics are made available to all users accessible from the HSIN Central 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 U.S and its territories, the training team is prepared to support virtual training, as required. The 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.



### **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 when evaluating the credentials for a prospective applicant. These controls are designed to limit damage 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. 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.

Alternatively, if HSIN registration information is saved and stored in HSIN, it may be shared by any DHS entity or component involved in the process of validating the registrant's identity. This validation process is to ensure a user's attributes align with COIs and/or collaboration spaces that match his or her qualifications and/or permissions.

The COI sponsor is responsible for accepting the newly nominated, prospective user 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. Where there are multiple jurisdictions within a COI, the COI sponsor is strongly preferred to 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 to gain access to the respective 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) have authoritative responsibilities over the COI's users. One or more persons within the COI can execute the nomination and validation procedures.

COI sponsor(s) are responsible for the COI's respective nomination and validation procedures. An authority within the COI's established management must perform nomination and/or validation duties—such duties cannot be delegated to an individual or organization outside of the COI's management structure. For example, a state COI cannot delegate nomination/validation authority to a federal agency that is not a sponsor of the COI. In addition to these controls, each COI maintains other criteria for admitting new users into its community. At a minimum, a user applicant for a given HSIN COI, must possess the following credentials: (1) supports a DHS ISE mission; (2) credentialed to handle forms of, but not limited to, SBU information including FOUO; and (3) adheres to and accepts the HSIN Terms of Service.

Once verified, the user gains access only to her Primary COI; however, a user can be a member of more than one COI if appropriate and if relevant 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 collected during the initial questionnaire.



## **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 damage and ensure that the security and integrity of HSIN are upheld. Additionally, these controls provide users transparency with regard to the terms of service and make enforcing penalties easier. Users may decline to provide their information during this initial review process, but by doing so, their application for access will be rejected. Upon successful review and authentication, each user is assigned to a primary COI.

The HSIN Shared Space allows authorized stakeholders and content contributors to publish finished products and relevant documents that: (1) have appropriate markings providing sharing permissions at the document level; and (2) are targeted to an authorized audience based on their credentials and related COI and system-wide rules for sharing. To upload information into the HSIN Shared Space, a COI's user must first create and submit content to the COI's TVO for approval. The TVO is responsible for reviewing content to ensure that it can appropriately be shared, based on the information-sharing rules and preferences of its particular COI, and the credentials required for users outside the COI to view the shared content.

Information content is considered appropriate for sharing when the TVO determines that it is in both the COI's and the greater HSIN community's interests to have such content shared, either on a case-by-case or rules-based basis. Shared content shall only be appropriately shared based on the markings the TVO attaches to the content and the corresponding credentials of a user with whom such content may be shared. The TVO approves, rejects, or modifies the request for sharing content. At the TVO's discretion, content may be marked as accessible or discoverable. If marked accessible, the content can be viewed in full by authorized users based upon the content's tags and markings. If marked as discoverable, the user must request access to the information and the TVO or content owner must approve the request prior to sharing the information with the user.

Each COI charter shall 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 of the Homeland Security Act. HSIN PMO will work in cooperation with each COI to ensure such rules are enforced. Under the terms of the COI charters and the HSIN Terms of Service, each User and content owner is 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 respective Charter includes a provision for removing outdated, no longer accurate, shared content. HSIN PMO will also explore potential development of business processes to archive shared content that has been in the Shared Space for an inappropriately long period of time, consistent with individual COI rules. HSIN PMO works 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<sup>19</sup>

<p><b>DHS Components and Offices</b></p>	<ul style="list-style-type: none"> <li>• Chief Financial Officer (CFO)</li> <li>• Citizenship and Immigration Services Ombudsman (CISOMB)</li> <li>• Civil Rights and Civil Liberties (CRCL)</li> <li>• Customs and Border Protection (CBP)</li> <li>• Office of Counternarcotics Enforcement (CNE)</li> <li>• Domestic Nuclear Detection Office (DNDO)</li> <li>• Executive Secretariat (ESEC)</li> <li>• Federal Emergency Management Agency (FEMA)</li> <li>• Federal Law Enforcement Training Center (FLETC)</li> <li>• Office of the General Counsel (OGC)</li> <li>• Office of Health Affairs (OHA)</li> <li>• U.S. Immigration and Customs Enforcement (ICE)</li> <li>• Office of Inspector General (OIG)</li> <li>• Office of Intelligence and Analysis (I&amp;A)</li> <li>• Office of Legislative Affairs (OLA)</li> <li>• Management (MGMT)</li> <li>• National Cybersecurity Center (NCSC)</li> <li>• National Protection &amp; Programs Directorate (NPPD)</li> <li>• Office of Operations Coordination and Planning (OPS)</li> <li>• Office of Policy (PLCY)</li> <li>• Privacy Office (PRIV)</li> <li>• Office of Public Affairs (OPA)</li> <li>• Science and Technology (S&amp;T)</li> <li>• Transportation Security Administration (TSA)</li> <li>• United States Citizenship and Immigration Services (USCIS)</li> <li>• United States Coast Guard (USCG)</li> <li>• United States Secret (USSS)</li> </ul>
<p><b>Departments &amp; Federal Agencies</b></p>	<ul style="list-style-type: none"> <li>• Federal Bureau of Investigations (FBI)</li> <li>• Department of State (DOS)</li> <li>• Department of Interior (DOI)</li> <li>• Department of Energy (DOE)</li> <li>• Department of Veterans Affairs (VA)</li> <li>• Department of Defense (DOD)</li> <li>• Defense Information Systems Agency (DISA)</li> <li>• Defense Intelligence Agency (DIA)</li> <li>• Defense Security Service (DSS)</li> </ul>

<sup>19</sup> This is an initial, non-final list of primary COIs submitted as of 06/2012. The list may be revised as needed.



	<ul style="list-style-type: none"> <li>• Department of Agriculture (USDA)</li> <li>• Department of Education (ED)</li> <li>• Department of Health and Human Services (HHS)</li> <li>• Department of Housing and Urban Development (HUD)</li> <li>• Department of Justice (DOJ)</li> <li>• Department of State (DOS)</li> <li>• Department of the Treasury</li> <li>• Department of Transportation (DOT)</li> </ul>
<p><b>States</b></p>	<ul style="list-style-type: none"> <li>• Alabama</li> <li>• Alaska</li> <li>• American Samoa</li> <li>• Arizona</li> <li>• Arkansas</li> <li>• California</li> <li>• Colorado</li> <li>• Connecticut</li> <li>• Delaware</li> <li>• District of Columbia</li> <li>• Florida</li> <li>• Georgia</li> <li>• Guam</li> <li>• Hawaii</li> <li>• Idaho</li> <li>• Illinois</li> <li>• Indiana</li> <li>• Iowa</li> <li>• Kansas</li> <li>• Kentucky</li> <li>• Louisiana</li> <li>• Maine</li> <li>• Maryland</li> <li>• Massachusetts</li> <li>• Michigan</li> <li>• Minnesota</li> <li>• Mississippi</li> <li>• Missouri</li> <li>• Montana</li> <li>• Nebraska</li> <li>• Nevada</li> <li>• New Hampshire</li> <li>• New Jersey</li> <li>• New Mexico</li> <li>• New York</li> <li>• North Carolina</li> <li>• North Dakota</li> <li>• Northern Marianas Islands</li> <li>• Ohio</li> <li>• Oklahoma</li> <li>• Oregon</li> <li>• Pennsylvania</li> <li>• Puerto Rico</li> <li>• Rhode Island</li> <li>• South Carolina</li> <li>• South Dakota</li> <li>• Tennessee</li> <li>• Texas</li> <li>• Utah</li> <li>• Vermont</li> <li>• Virginia</li> <li>• Virgin Islands</li> <li>• Washington</li> <li>• West Virginia</li> <li>• Wisconsin</li> <li>• Wyoming</li> </ul>
<p><b>Territories</b></p>	<ul style="list-style-type: none"> <li>• American Samoa</li> <li>• Guam</li> <li>• Northern Marianas Islands</li> <li>• Puerto Rico</li> <li>• Virgin Islands</li> </ul>



<b>Tribal</b>	<ul style="list-style-type: none"><li>• Alaska</li><li>• Great Plains</li><li>• Northwest</li><li>• Southern Plains</li><li>• Eastern</li><li>• Navajo Pacific</li><li>• Southwest</li><li>• Eastern Oklahoma</li><li>• Midwest</li><li>• Rocky Mountain</li><li>• Western</li></ul>
---------------	--