HSIN Release 3 Terms of Service[1]

The HSIN Release 3 Terms of Service includes five (5) Parts. Each Part is directed to a particular piece of the HSIN Enterprise. The five Parts include:

PART 1 - GENERAL TERMS AND CONDITIONS

PART 2 - USER SPECIFIC TERMS AND CONDITIONS

PART 3 - COI SPONSOR SPECIFIC TERMS AND CONDITIONS

PART 4 - HSIN APPLICATIONS

PART 5 - HSIN PROGRAM MANAGEMENT OFFICE SPECIFIC TERMS AND CONDITIONS

1 The HSIN PMO retains the right to unilaterally modify the terms of this document, and must provide notice of such modifications to the entire enterprise.

PART 1 – GENERAL TERMS AND CONDITIONS

Purpose and General Statement of the "Terms of Service" (TOS)

These Terms of Service define a HSIN user's basic rights, duties and privileges as a registered user of HSIN. These Terms of Service apply to a user's and COI's use of HSIN, on HSIN, while accessing HSIN.

By using Homeland Security Information Network (HSIN) services and clicking "accept" upon notice of the Terms of Service (Terms), the user agrees to these Terms. HSIN provides an information-sharing "network of trust" service designed to meet the sensitive but unclassified (SBU) information sharing requirements of the homeland security enterprise. By accessing HSIN, the user acknowledges and accepts these Terms. These Terms define the rights, duties and services afforded to all users of HSIN. The HSIN Program Management Office (PMO) reserves the right to change these Terms of service at any time, as such; communications about changes will be provided timely and appropriately. As a result, requirements may evolve that may expand the Terms of Service offered. These Terms can be modified, and expanded upon, in a Community of Interest (COI) Model Charter, however, no Charter can contravene these Terms or any other existing HSIN policy. HSIN cannot be used for any illegal purposes. Department of Homeland Security (DHS) is not responsible for monitoring the specific content of HSIN; rather DHS provides the communication environment and user access controls. For all purposes, including the Freedom of Information Act (FOIA) and the Privacy Act, DHS is not the custodian of substantive information on HSIN. Federal, state and local HSIN users are bound by their own jurisdictional requirements. The HSIN PMO is a Data and Content Steward. It is not responsible for the content that users and COIs post to any element of HSIN. Nor is it responsible for the content for the content that users and COIs retain custody and exclusive control over at any location within HSIN. Such content remains under the users' and COIs' relevant and applicable Federal, state, municipal, territorial and tribal information management, privacy, public disclosure (or "Sunshine laws") and records management statutes, and/or regulations.

HSIN Disclaimer

The user is entering an Official United States Government System, which includes the device being used to connect to the HSIN system, and may be used only by authorized users for authorized purposes. Unauthorized access is a violation of the laws of the U.S. and the policies of the U.S. Department of Homeland Security, and may result in administrative or criminal penalties. Every effort is made to ensure the quality, integrity, and utility of the information on this site while ensuring privacy and security. This information system is maintained by the U.S. Government and is designed to comply with federal laws of the United States. It is protected by various provisions of Title 18, United States Code, Section 1030, and

other federal or state criminal and civil laws. Violations of Title 18 are subject to criminal prosecution in federal court. By using this information system, the user understands and consents to the following: The user has no reasonable expectation of privacy when he/she uses HSIN; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor and/or intercept any communication or data transiting or stored on this information system. For all purposes, including the Freedom of Information Act (FOIA) and the Privacy Act, DHS is not the custodian of substantive information on HSIN. Federal, state and local HSIN users are bound by their own jurisdictional requirements. For information that is owned by DHS, DHS may disclose or use any communications or data transiting or stored on this information system as required by lawful government purpose, including but not limited to law enforcement purposes, including those resulting from a court order or law enforcement investigation. Anyone who accesses HSIN without authorization or exceeds their access authority, and by any means of such conduct obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer, may be subject to fine or imprisonment, or both. If any materials on HSIN or use of HSIN are contrary to the law of the place where accessed and viewed, the site is not intended for access and view and shall not be used or viewed. Therefore, Visitors are responsible for informing themselves of the laws of their specific jurisdiction[2] and complying with them. The user is not authorized to process classified information on this system.

Behavior on HSIN

COI Sponsors will take responsibility for user compliance to his/her behavior within their COI and throughout HSIN. Rules of behavior that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of sensitive-but-unclassified information. Rules of behavior inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing the HSIN system and COI portal, which include accessing, storing, receiving, or transmitting information. They are consistent with DHS IT security policy and procedures within DHS Management Directive 4300.1 (Information Technology Systems Security), and the DHS Sensitive Systems Policy Directive 4300A, specifically 4.1.2.b, 2.2.11.a and NIST 800-53, PL-4. Users, and COIs are responsible for all such rules of behavior, and will be held accountable for actions performed on HSIN, based on a given User's acceptance of the Terms of Service upon becoming a registered HSIN user, under the auspices of an approved/authorized COI Sponsor COI's Charter.

[2] Jurisdiction – E.g. The same State, city, or agency, or at minimum, the same type of entity, such as State-for-State, law enforcement for law enforcement, etc.

These actions include accessing, storing, receiving, or transmitting information. Users are given access only to those COI(s) for which their attributes are permissioned and to which the COI Sponsor or Site Validator approves and validates their access. Users must choose passwords that are at least twelve characters long and have a combination of letters (upper-and lower-case), numbers and special characters. Users must protect passwords and access from disclosure and may not share passwords or other authentication materials. Passwords cannot be provided to any third party, including Site Owners. Proper storage and protection of authentication methods must be adhered to, so as to prevent the risk of the system being compromised. Users must not attempt to bypass access control measures under any condition. HSIN does not endorse or recommend any products, processes, or services of non-federal or commercial entities. The views and opinions of authors expressed within products on HSIN does not necessarily state or reflect those of the U.S. Government, and they may not be used for lobbying, advertising, or product endorsement purposes. Some HSIN web pages may provide links to external internet sites for the convenience of users. The U.S. Government is not responsible for the availability or content of those external sites, nor does the U.S. Government endorse, warrant, or guarantee the products, services, or information described or offered at those other internet sites. Users should be aware that external sites referenced by links within HSIN do not necessarily abide by the concept of operations, policies, or rules to which HSIN adheres. The compliance policies and rules concerning information coordination required for access to HSIN are not intended to create or confer any right, privilege, or benefit to any private person including any person in litigation with the United States or any agency or individual using HSIN.

Liability & Indemnification Clause

DHS is held harmless from and against any third-party claim, cause of action, etc. related from : (a) content that a user posts or transmits; (b) activity that occurs through or by use of a user's credentials; (c) use of or reliance on any user content; and (d) violation of this TOS.

This site is maintained by the U.S. Government. The information available from this site may include law enforcement sensitive information; material contributed or licensed by individuals, companies, or organizations that may be protected by U.S. and foreign copyright laws; or material that is otherwise not subject to public release under or due to the Freedom of Information Act or the Privacy Act. , The U.S. Government does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or processes disclosed through this system since much of the information that may be communicated on this system may be pre-analytical (raw) suspicious activity information from numerous Federal and state governmental, law enforcement, and many private sector sources. The U.S. Government does not endorse or recommend any products, processes, or services of non-federal or commercial entities. The views and opinions of authors expressed

within products on HSIN sites do not necessarily state or reflect those of the U.S. Government[3], and they may not be used for lobbying, advertising, or product endorsement purposes. Some HSIN web pages may provide links to external internet sites for the convenience of users.

The U.S. Government is not responsible for the availability or content of those external sites, nor does the U.S. Government endorse, warrant, or guarantee the products, services, or information described or offered at those other internet sites. Users should be aware that external sites referenced by links within HSIN do not necessarily abide by the concept of operations, policies, or rules to which HSIN adheres. The compliance policies and rules concerning information coordination required for access to HSIN are not intended to create or confer any right, privilege, or benefit to any private person including any person in litigation with the United States or any agency or individual using HSIN.

Mobile Device Access

It is recommended that a user secures the devices he/she is using when accessing HSIN and ensures such devices are secured when unattended via a locking cable, locked office, or locked cabinet or desk.[4] HSIN provides mobile device services for free, however normal carrier rates and fees shall still apply to the user. When a COI determines that such requirements are not adhered to by a user(s), COIs shall report alleged violations to HSIN Security, to be addressed.

Safeguarding Sensitive But Unclassified (SBU) Information

HSIN stores Sensitive but Unclassified (SBU) information, not classified information; therefore, nothing above a "FOR OFFICIAL USE ONLY" (FOUO) marking is permitted on this system. The default classification of all documents posted on HSIN shall be FOUO for all users, including international users. The marking "FOR OFFICIAL USE ONLY" will be used to identify SBU information within the system that is not otherwise specifically described and governed by statute or regulation. FOUO information will not be disseminated in any manner – orally, visually, or electronically – to unauthorized personnel. Access to FOUO information is based on "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information's originator. A security clearance is not required for access to FOUO information.[5] When discussing or transferring FOUO information to another individual(s), ensure that the individual with whom

[3] Privacy Impact Assessment (PIA) Operations Directorate, HSIN page 29
[4] HSIN 3.0 DHS Security Plan_draft_0.2, May 2, 2012
[5] DHS MD 11042, Safeguarding Sensitve But Unclassified Information, 5/11/2004

the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information. FOUO information may be shared with other agencies, Federal, State, tribal, or local government and law enforcement officials, and non-governmental entities in compliance with relevant laws, regulations and agency policies determining its use, management and dissemination.

Additionally, the HSIN PMO, in alignment with DHS standards, requires the appropriate marking on all documents. Users shall prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the marking "FOR OFFICIAL USE ONLY." Likewise, materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions.

HSIN governmental users involved in information coordination processes are subject to the Federal, state, municipal, and tribal information management, privacy, and public disclosure (or "Sunshine laws") statutes and regulations of their jurisdictions. Compliance with all applicable Federal, state, municipal, and tribal laws and regulations is a non-delegable responsibility of the individual users and the agencies to which they belong. Some representative examples of the types of statutes and regulations applicable would include but are certainly not limited to 5 U.S.C. 552, The Freedom of Information Act; 5 U.S.C. 552b, The Privacy Act of 1974, 5 USC 552a (as amended); 28 C.F.R. Part 23, Criminal Intelligence System Operating Policies; Executive Order 12333, United States Intelligence Activities; and DoD Directive 5240.1R, Procedures Privacy Impact Assessment Operations Directorate, Homeland Security Information Network Page 28, Governing the Activities of DoD Intelligence Components That Affect United States Persons. Again, these laws and regulations are only applicable to the extent that they apply to a particular agency or individual using HSIN. The Department of Justice has defined the National Operations Center (NOC) [6] as a law enforcement activity that is 28 C.F.R. Part 23 compliant for information sharing with law enforcement agencies and activities operating criminal intelligence systems through support under the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. §§ 3711). The NOC and all LE communities operating within the HSIN system shall be governed by the provisions of 28 C.F.R. Part 23 and operated in a manner that conforms with or respects all agency/jurisdiction specific law enforcement regulations and policies.

[6] Formerly referred as the Homeland Security Operations Center.

Information reported or posted by a particular Federal, state, municipal, or tribal agency may be coordinated within/among the relevant or applicable community to which it was reported or posted by the source agency, but remains subject to any limitations on use/dissemination imposed by the reporting/posting source agency and remains in the "custody and exclusive control" of the source agency for privacy and information release requirements imposed by law or regulatory policy. Other than the Federal, state, municipal, and tribal governmental and law enforcement agency users that are directly subject to privacy and information requirements imposed by the laws and policies of their jurisdictions, no HSIN user shall be afforded nor shall seek, obtain, or exploit access to privacy or proprietary record information obtained within HSIN.

Private sector information on HSIN shall be handled incompliance with all applicable laws and regulations on the protection of proprietary critical infrastructure information.

Personally Identifiable Information

All HSIN users must adhere to the privacy requirements listed in this section when making information available in any COI and in any other way through HSIN. Specifically, all HSIN users must:

1. Ensure that all included PII is necessary to the understanding of information they make available in HSIN. Any PII that is not necessary must be removed from the information prior to making it available to HSIN. Generic information can be substituted for the PII to facilitate understanding of the information such as "an individual" instead of person's name.
2. Ensure that all PII is current and accurate prior to including in any information they make available in HSIN.
3. Tag all information they make available in HSIN that contains personally identifiable information as "PII" in addition to any other tags they may include for that information.
4. "Personally Identifiable Information" or "PII" is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to an individual regardless of whether the individual is a U.S. Citizen, legal permanent resident, or a visitor to the U.S.
5. "Sensitive Personally Identifiable Information" or "SPII" is any PII which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
6. Tag all information containing PII for the specific categories of user roles (see "HSIN Site(s) User Roles" in Part 3 of this document) that are appropriate.
7. Upon receiving notice of changes to PII, update that PII they made available in HSIN.

Freedom of Information Act (FOIA)

For all purposes, including the Freedom of Information Act (FOIA) and the Privacy Act, DHS is not the custodian of substantive information on HSIN. Federal, state and local HSIN users are bound by their own jurisdictional requirements. For information that is owned by DHS, only HSIN documents that are subject to FOIA will be handled by the source agency's FOIA processes and procedures. DHS is only responsible for documents owned by DHS. How HSIN PMO and its COIs choose to respond to a FOIA request is based on the particular facts of a FOIA request and the applicable laws. HSIN users and COIs are responsible for the content that they publish to any element of HSIN and/or for which they retain custody and exclusive control at any location within HSIN. HSIN users and COIs are thus subject to the Federal, state, municipal, territorial and tribal information management, privacy, public disclosure (or "Sunshine laws") and records management statutes, and/or regulations of their jurisdiction(s) for the content that they publish and/or for which they retain custody and exclusive control.

HSIN PMO is a Data and Content Steward. It is not responsible for the content that users and COIs post to any element of HSIN. Nor is it responsible for content that remains under the custody and exclusive control of a user or COI at any location within HSIN. COIs are responsible for such content under their relevant and applicable Federal, state, municipal, territorial and tribal information management, privacy, public disclosure (or "Sunshine laws") and records management statutes, and/or regulations. Each instance of a FOIA / Sunshine law request is unique and depends on the specific content being requested and the particular law being used to pursue the request. The HSIN PMO will always work to ensure and facilitate with the COI, appropriate compliance with such requests, based on their particular facts, but remains not responsible for the content that users and COIs post and/or retain custody and exclusive control over. It is the duty of that COI, or COIs, to respond to FOIA requests.

A COI Sponsor may provide additional information, at its discretion, within its COI Charter, on the Federal, State, municipal, territorial and tribal information management, privacy, public disclosure (or "Sunshine laws") and records management statutes, and/or regulations which it feels are relevant and applicable to its COI, and all the related procedures it will follow when addressing issues related to such laws and regulations.

Intellectual Property Rights

A user and COI Sponsor, retains ownership of content posted or published in that particular COI and Site. Using HSIN services does not give ownership of any intellectual property rights or accessed content to HSIN PMO or any other party. In order to use content, a user must request and obtain permission from its owner. These Terms do not grant the user the right to use any branding or logos provided and/or included on the published content of other users.

Records Management Responsibilities

HSIN is a Data and Content Steward and is not responsible for the management of the records[7] of content created, posted and/or shared by HSIN users, nor is it responsible for the compliance of users and/or COIs with the records management laws and/or regulations that apply to their published content and/or COIs. HSIN users and COI Sponsors are responsible for adhering to the Federal, state, local, territorial or tribal records management laws, regulations and policies that apply to the content which they publish and/or retain custody and control over, regardless of such content's media format(s). Each member's content contributions will carry that users Federal/state/local jurisdiction laws regarding FOIA, Privacy, and Records Management.

As a matter of policy, HSIN will provide capacity for data storage for COIs for content that is up to and no more than five (5) years in age, based on the time from a content item's last modification date. In the event that a user becomes inactive, his or her content shall be retained under the COI's records management policy and procedure. Content owners and/or COIs may contact the HSIN PMO to set up alerts for COI Sponsors regarding expiring data that may be up for deletion. After such time, content owners and/or COIs must directly provide for the archival of their content and records, if required under the laws and policies of their original jurisdiction. 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. However, ultimately records management is the responsibility of content owners and/or the content controlling COI. The HSIN PMO is responsible for ensuring retention of records for the content which it, itself, publishes and retains custody and control over on HSIN. The content published by the HSIN PMO (e.g. HSIN Central, etc.) will adhere to NARA schedule N1-563-11-010 for records management which states:

- Documents "published" from day-to-day operations, including the instant-messaging and web-conferencing tools are "Steady state" (normal day-to-day) and are stored for five years and then destroyed.

[7] Defined in 44 U.S.C. 3301 as including ``all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them (44 U.S.C. 3301).'' (See also § 1222.10 of this part for an explanation of this definition).

- Records that are part of a Level 2 or 3 event are transferred to the National Archives five years after the event or case is closed for permanent retention in the National Archives.

PART 2 – USER SPECIFIC TERMS AND CONDITIONS

HSIN Account Provisioning

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 must 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.8 Nominations into COIs will expire after 60 days. After the 61st day, the HSIN user must be re-nominated. 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- 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. A user shall have the right to independently, self-nominate into a particular community of interest, subject to the validation and membership rules of a particular COI.

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;[9] both processes require identity verification and a mission need

[8] 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."

[9] Future sources of federated, HSIN user membership are likely to include Law Enforcement Online (LEO) and Regional Information Sharing Systems (RISSNET).

assessment. This initial verification of identity is conducted, in part, through use of a third-party service. 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;[10] 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.

User Account Inactivity

Under current HSIN system capabilities, in which no functionality yet exists for automatically resetting one's password online, a user shall be considered an active user if they have logged in within 90 days of their most recent login to HSIN. Starting two weeks before the 90th day mark, a user who has not logged in to HSIN up to such time, will receive three email notifications from the system requesting that they login to their HSIN account in order to avoid becoming inactive. If a user fails to login to the system within 90 days of their last login, starting on the 91st day their account will become inactive. To re-gain an active account status, a user shall be required to call the HSIN Help Desk and answer their security questions to reset their password. Inactive users will only have the ability to reset their password with the HSIN Help Desk up to the 364th day mark, from their last login. On the 365th day, an inactive user's account shall become deactivated from HSIN. At such time, the user shall be required to re-register their information, including a new Nomination-Validation, and Identity Proofing process, to fully update their

[10] 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.

identifying information. A deactivated user who has not logged into HSIN six years since their last login, shall have their account information purged from all HSIN system records.

Under future HSIN system capabilities[11], in which an automated, online, password reset capability shall exist for all HSIN users, a user shall be considered active if they have logged in within the past 45 days. Starting two weeks before the 45th day mark from a last login, a user will receive one email notification from the system requesting that they login to their HSIN account in order to avoid becoming inactive. If a user fails to login to the system within 45 days of their last login, starting on the 46th day, and up to 364 days since their last login, a user shall be considered inactive but may restart their access by using the automated, online, password reset capability or by calling the HSIN Help Desk. Users will have up to three (3) chances to successfully renew access through the automated capability. If the user is unsuccessful in retrieving their password after three (3) chances, he/she must call the HSIN Help Desk and answer their security Q&A to reset their password. On the 365th day of inactive status, a user's account shall be deactivated and the user shall be required to re-register their information including a new Nomination-Validation, and Identity Proofing process, to fully update their identifying information. A deactivated user who has not logged into HSIN six (6) years since their last login, shall have their account information purged from all HSIN system records. HSIN will retain the deactivated user's profile information for up to six (6) years.[12] During this time, a user may reinstate access by calling the HSIN Help Desk.

Account Failed Login Attempts

A user will be locked from their account after three (3) consecutive failed logon attempts.[13] To reinstate access under the current operational environment, a user must call the HSIN Help Desk. At a future time under HSIN Release 3, once the capability is fully implemented, users will have the ability to click "Forgot Password" on the login screen, to automatically reset their password, bypassing the need to contact the customer service representatives at the HSIN Help Desk.

User Roles, Rights, and Duties

HSIN registered users have the right to access the system so long as these TOS are accepted and they have cleared all mandatory identity proofing and nominations/validations procedures. Each HSIN COI may extend additional rights, roles and duties to their particular accepted users in

[11] An implementation date of said future capabilities is to be determined.
[12] NARA Schedule 24, section 6
[13] DHS 4300A, Section 5.2.1.a

their specific COI Charter, so long as such are not in contravention of these TOS or any other HSIN policy.

COI Sponsor Roles, Rights and Duties and their Staff:

For full details, please refer to Part 3 - COI Sponsor Specific Terms and Conditions.

Normal Publication / Management

HSIN acts only as a Data and Content Steward and is not responsible for content posted by its users. HSIN users own all the content and information that they post on the system, and control, in part, how it is shared within the COI(s) to which they belong and/or in the shared space. A user shall have the right to post content within any COI of which they are a member and for which they have the correct permissions, as provided by the HSIN PMO and the COI Sponsor, and embodied in the rules established in a COI's Charter. When a user wants to publish material that is discoverable in the Shared Space, he/she will be required to follow a standard process of approval by their COI's Trusted Vetting Official (TVO). (See *Shared Space Activities* section.) HSIN will require default and customizable tags to increase sharing. See *Knowledge Management Policy* for full details. As required, COIs may establish additional rules and procedures, in adherence to but not contravention with all other HSIN policies, governing the management and creation of content.

Federated User Rights

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. This user shall be granted revocable rights to access HSIN using the same credentials as his or 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, such as this one, including additional COI membership criteria, in the same way as any other registered, HSIN user.

Identity Proofing

In order to verify the registrant's identity, Personally Identifiable Information (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 identity verification provider is leveraged to ensure full and effective validation through identity confirmation. This confirmation will involve a "soft-inquiry" on the prospective user's consumer report. This type of inquiry does

not affect one's consumer report. This information will be used solely for the limited purpose of identity proofing, and will not be stored onto 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. Anyone granted user account access to any DHS information system (including DHS employees, contractors, and others working on behalf of DHS) shall have no expectations of privacy associated with its use. By completing the authentication process, the user acknowledges his or her consent to monitoring, thus ensuring compliance with DHS 4300A 4.8.5.c.

International User Guidance

Properly vetted international users, by the DHS Foreign Disclosure Officer (FDO), have the same roles, rights and privileges as a HSIN-user with US citizenship. As a result, there is no bar against "labeling" an international user or from sharing law enforcement sensitive (LES) information with foreign partners / users. There are some, varied restrictions on sharing information with foreign partners/users however, those rules are country specific. Each COI and its Site Owners need to know and enforce those country-specific international agreements within their COI, and may also develop additional rules, guidelines and procedures on the inclusion of international users in their particular community and their content publication and readership rights

Information Sharing Guidance

To effectively share information, HSIN encourages users to adopt a new information sharing vision – a "responsibility to provide". This vision enables cross-mission collaboration while still addressing the need to protect privacy, civil liberties, sources, and methods.[14] A full description of information sharing guidance is outlined in the *Knowledge Management Policy.*

SYSTEM ACCESS

Level One Access

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 (POC) be provided. Prospective users may only be given access to those COIs for which they will be required to perform official duties for. These users must not attempt to access COIs or other data that they are not specifically authorized to access. Users shall not share identification or authentication materials of any kind, nor shall any DHS users allow any other person to operate

[14] HSIN KM Implementation Plan v2 09162011

any DHS system by employing the user's identity. These controls are consistent with DHS 4300a, 5.1.1.c, 5.1.d and NIST 800-53, PL-4 and PS-6. Additionally, prospective users will be required to answer a set of questions mapping their attributes to their job function and/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 third- party identity verification provider. The information collected for identity proofing purposes is not stored or retained and is used solely for the limited purposes of the identity proofing process described above in *Identity Proofing*.

The information collected for HSIN registration purposes (SEE table below summarizing such information), to provision and manage a user's actual account, is collected and stored, and may be shared by any DHS entity or component for the sole purpose of processing and validating the registrant's identity and ensuring the user's relevance to a legitimate community within HSIN and/or the qualifications of entry into particular HSIN collaboration spaces. In compliance with the Privacy Act and the Privacy Impact Assessment[15] governing HSIN R3 information that is collected and stored on HSIN from a new registrant includes:

HSIN New Registrant Information[16]	
Mandatory fields	**Optional fields**
Primary Community Reason for Access First Name Last Name DOB Primary E-Mail Alternate Secondary E-Mail Business Phone Mobile Phone Primary Contact Method Secondary Contact Method Job Title Job Role	Salutation Middle Initial Suffix Nickname Ext. Fax Pager Other Phone Business Location: (Street 2, Street 3, County) Home Location: (Street 1, Street 2, Street 3, City, County, Postal/ZIP, Country, State) Deployed Location: (Street 1, Street 2,

[15] PIA OPS HSIN User Accounts final, 20120725

[16] 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.

HSIN New Registrant Information[16]	
Mandatory fields	**Optional fields**
Organization Business Location: (Street 1, City, Postal/ZIP, Country, State) HSIN Sponsor Information: (Full Name, Organization, Primary E-Mail, Job Title, Business Phone, Ext., Primary Contact Method, Secondary Contact Method) Sector Country of Citizenship Username Password Confirm Password Security Question Security Answer Authentication (TFA) Delivery Method	Street 3, City, County, Postal/ZIP, Country, State) About Me User Interests Certifications HSIN Sponsor Information (Secondary E-Mail, Mobile Phone) Verification SBU Category PCII Certification Credential SSN

There is a 45-day period for a user to be vetted into a COI based upon the attributes collected from the questionnaire. After such time, if the user has not been vetted, he/she will need to repeat the registration process. During this process, the prospective user does not have access to any COI, until a COI accepts its registration. As a caveat, at this general level of access preceding admission to a particular COI, migrating users will be granted read-only access to the home page, HSIN Central, until the appropriate COI(s) have accepted them.

Level Two Access

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. The nomination and validation procedures can either be executed by one person or multiple persons within the COI. A single user may possess the roles of Nominator and Validator. However, under normal, non-incident response circumstances, an individual user holding both the nominator and validator roles, may not execute nomination and validation functions for the same, single registering HSIN user, or a user joining a COI. Registering users must be nominated and validated by a different nominator and validator under normal, non-incident response circumstances. Nomination and/or validation approval authority cannot be delegated to an authority outside the COI's management. The COI Sponsor and Site Validators are the ultimate authorities over who shall be a member however; the Site Validator may delegate another person to perform the administrative task of either accepting or rejecting the newly nominated, prospective user into its COI. With

exceptions, the COI Sponsor should be from the same jurisdiction. jurisdiction-type, and/or mission type (based on the stated purpose of the COI, as determined by the COI), as the majority of the users making up the COI. If there are multiple jurisdictions within a COI, the Site Owner must be from the same jurisdiction-type, and/or mission type, as the majority of users making up the COI (based on the stated purpose of the COI, as determined by the COI).[17] The table below illustrates a non-conclusive list of sample COI's.

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 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)

[17] 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 nom/val process, having nominators and validators best positioned to perform their duties.

	• Department of Veterans Affairs (VA) • Department of Defense (DOD) • Defense Information Systems Agency (DISA) • Defense Intelligence Agency (DIA) • Defense Security Service (DSS) • 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 2: Sample Communities of Interest

Privacy

HSIN PMO requires the collection of personal information to provide better services to its users. HSIN PMO uses this information to (1) offer tailored content, (2) protect HSIN's integrity, and (3) improve services. The personal and employment data collected for HSIN's identity proofing process is limited to the information necessary to validate the registrant's identity as a legitimate and approved validating authority of the respective COI, the qualifications of entry into particular HSIN collaboration spaces, or to access specific information within HSIN. This identity-proofing information is collected by a private third party (i.e., that information is not submitted to or provided to the HSIN Program) to prove the registrant's identity, and is protected by the third party by agreements between this party and the HSIN Program. The information collected for identity proofing purposes is not stored, sold, traded or otherwise used beyond these specific and prescribed purposes. The information collected for HSIN registration purposes (SEE table below summarizing such information), to provision and manage a user's actual account, is collected and stored, and may be shared by any DHS entity or component for the sole purpose of processing and validating the registrant's identity and ensuring the user's relevance to a legitimate community within HSIN and/or the qualifications of entry into particular HSIN collaboration spaces. Additionally, limited amounts of data will be shared among internal members of the COI for the purposes of Site maintenance (administration) and for supporting collaboration (notifying users of other members in their COI(s)). Information shared for these purposes, would be limited to name, email address, organization, and role within the COI. Once a user has been successfully validated and accepted into HSIN and/or a COI, the user may modify his or her profile to change, add, or delete all optional fields. Information that is collected and stored on HSIN from a new registrant includes:

HSIN New Registrant Information[18]	
Mandatory fields	**Optional fields**
Primary Community Reason for Access First Name Last Name Primary E-Mail Alternate Secondary E-Mail Business Phone Mobile Phone Primary Contact Method Secondary Contact Method Job Title Job Role Organization Business Location: (Street 1, City, Postal/ZIP, Country, State) HSIN Sponsor Information: (Full Name, Organization, Primary E-Mail, Job Title, Business Phone, Ext., Primary Contact Method, Secondary Contact Method) Sector Country of Citizenship Username Password Confirm Password Security Question Security Answer Authentication (TFA) Delivery Method	Salutation Middle Initial Suffix Nickname Ext. Fax Pager Other Phone Business Location: (Street 2, Street 3, County) Home Location: (Street 1, Street 2, Street 3, City, County, Postal/ZIP, Country, State) Deployed Location: (Street 1, Street 2, Street 3, City, County, Postal/ZIP, Country, State) About Me User Interests Certifications HSIN Sponsor Information (Secondary E-Mail, Mobile Phone) Verification SBU Category PCII Certification Credential SSN

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. The effectiveness of authentication and security protections are verified through audits of system operation and usage conducted by the HSIN PMO's Security Assessment team. The privacy risk is also minimized by the system's

[18] 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.

architecture which stores collected information as encrypted data in a single location or data repository. This structure reduces the risk to the data by minimizing its proliferation in multiple locations and systems.

HSIN PMO reserves the right to uphold the integrity of the HSIN system, and by doing so may take any necessary actions to ensure a secure system and network. Users acknowledge that they have no expectation of privacy while using this system and consent to all activities being monitored, and that disciplinary actions may result from determination of any violations. These controls are consistent with DHS 4300a, 4.1.2.a and 4.8.5.c. 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 and/or retain custody and exclusive control over at any location within HSIN, under their relevant and applicable Federal, state, municipal, territorial and tribal information management, privacy, public disclosure (or "Sunshine laws") and records management statutes, and/or regulations. The HSIN PMO holds the duty to report breaches to the affected parties once such information is determined creditable. Furthermore, the HSIN PMO holds itself accountable for abiding by and enforcing this privacy policy.

Prohibited Content and Activities

All users specifically acknowledge that the HSIN PMO is not liable for the defamatory, offensive, or illegal conduct of other users, links, or third parties and that the risk of injury from the foregoing rests entirely with the user and its COI. Links on Sites, particularly links to third- party, off-network sites, do not constitute an endorsement from the HSIN PMO. Links are provided from users to provide information only. Inappropriate activities include viewing, downloading, storing, transmitting or copying materials that are sexually explicit or sexually oriented, related to gambling, music files, illegal weapons, terrorist activities, or any other prohibited activities related to commercial products or services.[19] Additionally, any activity that is not aligned to the fulfillment of the DHS Information Sharing Environment (ISE) Strategy or the COI's mission/vision/objectives is prohibited. It is the responsibility of the TVO and ultimately the COI Sponsor to evaluate the content and usefulness of information obtained and distributed on or from their Sites. Since the HSIN PMO is not responsible for the availability of these outside resources or their contents, direct any concerns regarding any external link to its original Site Owner or COI Sponsor. Information shall not be designated as FOUO in order to conceal government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency, or to avoid any regulations on the proper publication,

[19]DHS MD 4600.1, G.7

dissemination or use of information.[20] Illegal content may not be furnished on HSIN. Content that promotes or advertises products or services is strictly prohibited from being on HSIN. DHS staff may not use personally owned equipment and software to process, access, or store sensitive information without the written prior approval of the HSIN PMO.[21] Continued misuse of HSIN shall result in account termination.

HSIN may not be used for lobbying, advertising, or product endorsement purposes. 18 U.S.C. § 1030 prohibits unauthorized or fraudulent access to government computer systems. If the user registration information associated with this action is not the correct information, he or she is in violation of this law and should exit this system immediately. Completing this action may subject the user to a fine of up to $5,000 or double the value of anything obtained via this unauthorized access, plus up to five years imprisonment.

User Requirements Management

HSIN Sponsors have a right to engage with the HSIN PMO to address their new system requirements. To do so, Users, through their COI Sponsors, may engage one of the major user working groups noted in the governance diagram (SEE Figure 5, HSIN Policy Management Plan), or, may utilize their Mission Advocate, Outreach team, or online feedback forms. These technical requirements are managed through the HSIN Change Control Board (CCB) and vetted, adopted or rejected through the HSIN Senior Leadership Team (SLT).

Training[22]

The HSIN PMO shall offer baseline training to users regarding the topics below, however the duty to pursue such applicable training is the responsibility of users and their COIs. Training topics provided from the HSIN PMO include:

1. Classifications and Markings (PII, SSI, FOUO, etc.)
2. COI Roles / Limitations
3. Content / design standards
4. Freedom of Information Act (FOIA)
5. General Program Support (E.g. – Communications, Help Desk, Mission Advocate Support, etc.)
6. Knowledge Management Guidance relevant to HSIN

[20] DHS MD 11042.1
[21] DHS 4300a, 4.8.3.a
[22] All training requirements will be designed to require the minimal time required to express essential content, while achieving desired training ends. The HSIN Outreach Team will work with all affected parties to ensure flexibility in scheduling and efficiency of use of training time.

7. Mobile Device Access
8. Nomination / Validation Authorization
9. Privacy, as requested by DHS Privacy
10. Records Management, as requested by HSIN's records management officer
11. Rules of Behavior[23]
12. Section 508 Guidance
13. Shared Space Activities
14. Templates
15. Tools (Jabber, Connect, My Site, et al.)

To the greatest extent possible, HSIN PMO provided training shall be enhanced and coordinated with COI training resources, including the use of train-the-trainer events. HSIN PMO shall deliver a baseline understanding of the training topics above, however, it is the responsibility of each COI Sponsor of a community to ensure its users are properly trained on specific information required to support that mission area. Recurring and evolving training topics will be made available to all users accessible 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 Owners, Site Designers, Content Managers, Content Approvers, and Members have attended the appropriate courses in advance of the majority of end users. As a standard, in-person classroom or virtual training shall be provided for Site Owners, Site Designers, Content Managers, Content Approvers and Members from the HSIN PMO. In addition, to accommodate users spanning the continental U.S and its territories. The training team shall be prepared to support virtual training for up to 25 concurrent users as required. As supplemental instruction, the training team will provide a combination of short (15 minutes per topic) Connect casts, quick reference cards (QRCs), and computer based training (CBTs). These modules would also include best-practice guidance on topics such as document management and content dissemination.

[23] HSIN PMO will coordinate with all COIs to ensure that all users are trained regarding rules of behavior and has accepted the full Terms of Service and acknowledges their COI specific rights (DHS 4300A 4.1.2.b and NIST 800-53, PL-4)

Part 3 - COI SPONSOR SPECIFIC TERMS AND CONDITIONS

HSIN Communities of Interest (COIs)

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), unless an exception has been granted by the HSIN PMO. 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.

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.

Figure 1 below illustrates the privileged roles within a COI.

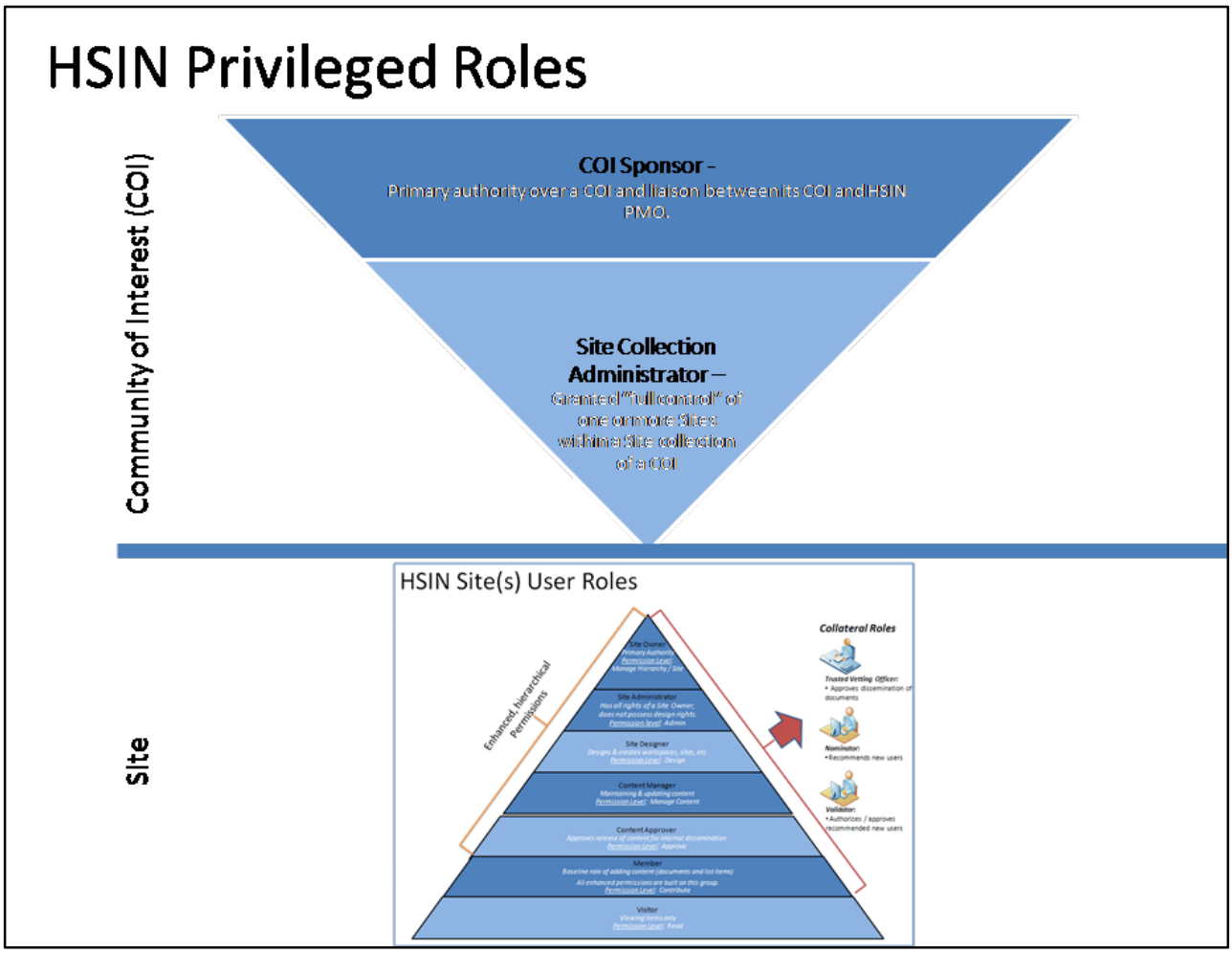

Figure 1: HSIN Privileged Roles

Figure 2 below provides a blown-out version of the HSIN Site(s) User Roles graphic in Figure 1. These roles will be established, permissioned, and staffed by the COI Sponsor of that given community. The illustration depicts a hierarchical role where responsibility and privileges increase for the user as the permissions are enhanced.

Privileged Roles

These roles are established for users that require elevated permissions to one or more COI. COIs that request users to obtain a privileged role must provide proper verification that such users are trained and have knowledge of HSIN specific capabilities. Such roles may be undertaken by one or more individuals of a COI.

COI Sponsor

The COI Sponsor role defines obligations taken on by a COI Sponsor when establishing a COI within HSIN. These obligations, support services, and operational controls provided by the HSIN PMO, represents a partnership. The COI Sponsor role is the primary authority over the COI. COI Sponsors must hold a position from a public sector institution, and that institution must be clearly recorded in the COI's Charter. Each COI must have at least one sponsor. This individual may delegate the day-to-day implementation and execution responsibilities to a work unit under management control, and that surrogate(s) must be clearly designated in the COI's Charter. This role establishes and staffs the required roles within their COI, acts as a liaison between its COI and the HSIN PMO, and establishes and updates its COI Charter. This role also approves and sets policies, governance standards, and communicates the established security measures of its Sites. The following duties will be undertaken by the COI Sponsor:

- Being the primary authority over the COI, sponsors and manages the activities of the COI on HSIN. The individual(s) must hold a position from a public sector institution, and that institution must be clearly recorded in the COI's Charter. Each COI must have at least one sponsor. This individual may delegate the day-to-day implementation and execution responsibilities to a work unit under management control, and that surrogate(s) must be clearly designated in the COI's Charter.
- Establishes and staffs the required roles and responsibilities to manage the COI and execute responsibilities;
- Ensuring orderly conduct is sustained within their COI and its Sites;
- Acting as a liaison between its COI and the HSIN PMO;
- Establishing and updating the COI Charter;
- Enforcing penalties on its users;
- Coordinating investigations with the HSIN PMO and HSIN PMO-Security;
- Validating the action to purge inactive accounts;
- Validating the action to lock down accounts;
- Authorizes the HSIN PMO to terminate account(s) within this COI;
- Approving and setting policies and governance standards to Sites as well as outline the established security measures;
- Monitoring, through technical workflow or delegation to TVO or Content Manager, to ensure duplicate documents do not exist in or are posted from their COI, documents are appropriately tagged, abide by Federal, state/local jurisdiction for Privacy, FOIA, and Records Management.

Site Collection Administrator

The Site Collection Administrator role will have the Full Control permission level on all Web sites within a site collection. They have Full Control access to all site content in that site collection, even if they do not have explicit permissions on that site. They can audit all site

content and receive any administrative alert. A primary and a secondary site collection administrator can be specified during the creation of a site collection. HSIN programmatic / technical changes will not override custom permissions and groups as set up by the Site Collection Administrator. However, if default HSIN values have been changed by the Site Colleciton Administrator, then a HSIN release update may set back permissions to the default value. This permission level is the highest permission level that can be granted to an end user of HSIN, but requires a COI to present a business justification to the HSIN PMO and may also require a subsequent HSIN CCB approval to be granted, on a case by case basis.

HSIN Site(s) User Roles[24]:

These roles are established, permissioned, and staffed by the COI Sponsor. This list of HSIN Site(s) User Roles are hierarchical and each role must be adopted for the operation of all Sites within a COI. Each HSIN Site may extend additional rights, roles and duties to their particular accepted users, so long as such are not in contravention of these HSIN Terms of Service or any other HSIN policy. Users within each Site can maintain multiple user roles. The SharePoint 2010 permission levels are identified in the below descriptions of the HSIN Site(s) User Roles and denoted by the use of quotation marks.

[24] In the future, particular site(s) may adopt the "Permission Manager" role or others, as required. The Permission Manager role will be granted the permissioned role of "Manage Permissions" at the Site level. Stakeholders are eligible to be assigned to the Permission Manager role, but HSIN Program support staff will also be assigned to the role in many cases. This role is intended to manage the permissions and groups of its libraries and lists within a Site. For any role assigned to HSIN Program Support staff, the COI Sponsor, or surrogate, must be consulted. These roles include Permission Manager Role, Site Owner, Site Designer, Content Manager Content Approver, Nominator and Validator. The Permission Manager capability must be available to the Site Collection Administrator whether or not a Permission Manager role exists. HSIN programmatic / technical changes will not override custom permissions and groups as set up by the Permission Manager or Site Collection Administrator.

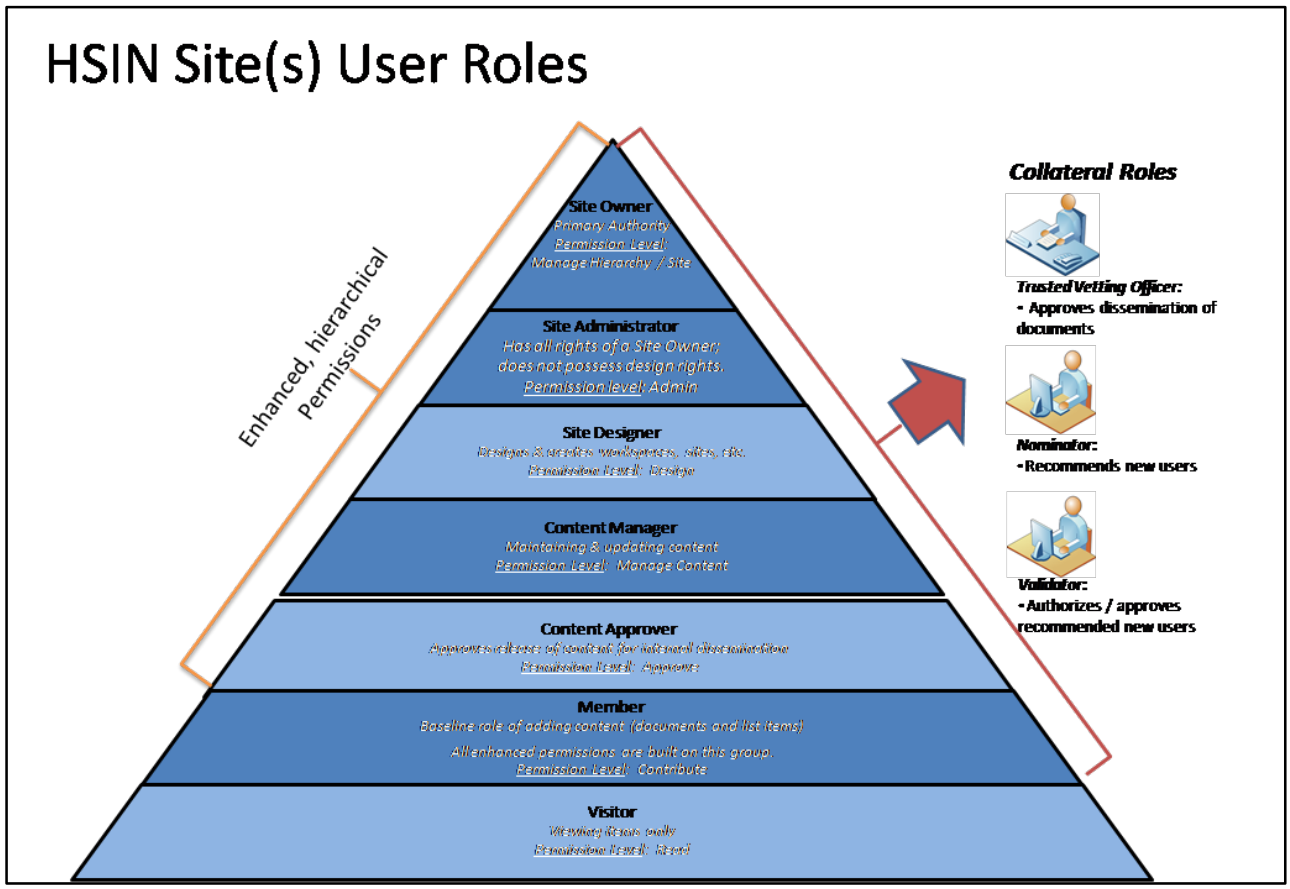

Figure 2: HSIN User Roles

Site Owner

A Site Owner will be granted the permissioned role of "Hierarchy Manager" and Site Owner at the Site level. The role of the Site Owner will be the highest level of Site control (as opposed to Site Collection control) stakeholders are eligible to be assigned. This role is intended to manage the Site infrastructure which includes activities such as creating document libraries, lists, and discussion boards, and shall include permissions for SharePoint design, applying style sheets, and applying themes. In select cases, for particular sites, this role may be assigned to HSIN Program support staff through coordination of the COI and the HSIN PMO. Any HSIN COI may request creation of this role and its associated permissions levels from the HSIN PMO, however, the role cannot become active without the consent of the HSIN Outreach Team, based on a business need established by a COI and/or Site.

Site Administrator

A Site Administrator shall have all of the rights, duties and permissions of a Site Owner, with the exception that a Site Administrator shall have no rights or permissions for SharePoint design,

applying style sheets, nor applying themes. A COI and/or Site may adopt the role of Site Administrator at will.

Site Designer

A Site Designer will be granted the permissioned role of "Design" at the Site level. Stakeholders are eligible to be assigned to the Site Designer role but HSIN Program support staff will also be assigned in many cases. This role is intended to manage the look and feel of Site content and the user interface ensuring that designs do not conflict with required elements of the provided HSIN templates, and that these designs meet the 508-specific requirements. This role is responsible to take 508 Awareness Training.

Content Manager

A Content Manager will be granted the permissioned role of "Manage Content" at the Site level. Stakeholders are eligible to be assigned to the Content Manager role but HSIN Program support staff will also be assigned in some cases. This role is intended to manage list and library items. This role is also responsible for marking all 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 HSIN Shared Space who meets the criteria associated with the content but not viewed until a request is approved by the TVO or content owner. "Discoverable" items cannot be found in the shared space without being promoted to the shared space first. The content owner remains the owner of the document when shared through the Shared Space.

Content Approver

A Content Approver will be granted the permissioned role of "Approve" at the Site level. Stakeholders are eligible to be assigned to the Content Approver role but HSIN Program support staff will also be assigned in some cases. This role is intended to approve minor versions of list and library items. This role is responsible for approving the release of content for internal Site dissemination.

Member

A Member will be granted the permissioned role of "Contribute" at the Site level. All users of a Site are eligible to be assigned to the Member role, regardless of their enhanced role. This role is the baseline role and intended to add, edit, and delete their own library and list items.

Visitor

A Visitor will be granted the permissioned role of "Read" at the Site level. Users are eligible to be assigned to the Visitor role in limited cases. This role is intended to view content only and will have limited operational use.

Collateral Roles:

These roles are established and assured staffing by the COI Sponsor. This list of SharePoint Collateral Roles are not hierarchical, nor is each role exclusive. Users within each Site can maintain multiple collateral roles. A Site shall adopt such roles as required for its operations. Such roles may be undertaken by the same individual, or multiple individuals.

Trusted Vetting Official (TVO)

The TVO role will be granted the permissioned role of "Read" at the Site level. Stakeholders trained and certified by the HSIN PMO will be assigned to the TVO role but this role will not be assigned to HSIN Program support staff , unless it's for a HSIN Program managed Site. The TVO is intended to authorize content publishing from a governed site[25] to the HSIN Shared Space. Each Site must have one primary TVO and may have several alternate.

Nominator

A Nominator role will be granted the permissioned role of "Read" at the Site level. Stakeholders trained and certified by the HSIN PMO will be assigned to the Nominator group and HSIN Program support staff will also be assigned in many cases. The Nominator group is intended to provide initial nomination for end users to a specific governed site. Nominators must be from the same jurisdiction, jurisdiction-type (e.g. State, local, private), and/or mission type, as the majority of the users within the given Site, (based on the stated purpose of the COI, as determined by the COI). Qualified, trained users may perform both the role of a nominator and a validator however, they cannot perform both functions for the same registering user. Nominators are responsible for recommending potential new users who possess the following criteria:

- Performs a job function that meets at least one of the homeland security mission areas[26]; and
- Has a valid email address.

Validator

A Validator will be granted the permissioned role of "Read" at the Site level. Stakeholders trained and certified by the HSIN PMO will be assigned to the Validator role and HSIN Program support staff will only be assigned in limited cases. Validators must be from the same jurisdiction, jurisdiction-type (e.g. State, local, private), and/or mission type, (based on the stated

[25] Governed site – A site where access to the Site must be requested of and granted by the Site Owner. Persons obtaining access have the appropriate credentials to access and contribute to content on the Site.

[26] Mission areas: Emergency Management, Law Enforcement, Critical Infrastructure, Emergency Services, Intelligence, and Public Health – HSIN Program Plan 2012-2014 (Final)

purpose of the COI, as determined by the COI), as the majority of the users within the given Site. Qualified, trained users may perform both the role of a nominator and a validator however, they cannot perform both functions for the same registering user Validators are responsible for confirming a nominated user for the following[27]:

- The nominated user meets the COI's membership criteria;
- The nominated user's email address format is validly entered; and
- A valid role has been identified.

COI & Site Inactivity

The COI Sponsor acknowledges that the HSIN PMO will take the following actions, in consultation with the COI Sponsor, to remove and/or remedy an inactive COI and/or Site. The HSIN PMO will monitor and produce monthly reports capturing inactive COI and/or Sites. This report enables coordination and ensures that unused community Sites will be purged from the system. When determining whether a COI and/or Site is inactive at any point in time, the HSIN PMO shall consider four (4) primary factors. These shall include:

1. Absence of Logons
    a. The HSIN PMO shall assess whether or not a user or very limited number of users has accessed the COI in question during the previous six (6) months. (I.e. a very small percentage of all users eligible to use the COI, such as less than 10%).
2. Absence of New Content
    a. The HSIN PMO shall assess how much new content, if any, has been posted to the COI in question during the previous six (6) months and which areas of content have not been accessed for an exceptional amount of time, including over one (1) year. (E.g. if no new content, or only a very limited amount of new content has been posted).
3. Insufficient content following As-Is Mapping
    a. The HSIN PMO, as part of the normal data migration process for R3 shall assess, following normal As-Is Data Mapping, whether there is sufficient content remaining in the COI for justify the time and expense of full COI migration.
4. End of Mission and/or Original Intent
    a. The HSIN PMO shall assess whether the original intent and/or mission of the COI in question has in fact been met, making its ongoing operation unnecessary.

[27] HSIN Release 3 User Story ID #348, 4/10/12

A simple user connection is not considered "activity." Malicious modifications, defined as when users modify content or conduct activity for the sake of demonstrating Site activity when there is in fact none, are strictly prohibited. Inactivity of multiple Sites residing in one COI can result in total COI deletion.

If a COI, or Site, is deemed inactive, the HSIN PMO will send three courtesy emails, over the period of one-month, to the COI Sponsor and/or Site Owner(s) attempting to notify and validate whether or not the COI and/or Site is "inactive". If the COI Sponsor and/or Site Owner(s) agrees that the COI and/or Site is "inactive" and it no longer supports a mission need, the HSIN PMO will take action to purge the Site from the system. If the HSIN PMO does not receive a response from the COI Sponsor and/or Site Owner within ten (10) business days after the last courtesy email, the COI and/or Site will be purged. In either case, the content in the COI and/or Site will be kept on file for five (5) years from the content's last "modified" date unless such content was developed in response to a Level II or Level III incident.[28] Whereas, such content shall be kept on file permanently. All other "expired" content will be purged from the system.

If the COI Sponsor and/or Site Owner(s) requests the HSIN PMO to not purge a COI and/or Site, the HSIN PMO shall not purge the COI and/or Site until an agreement is reached with the COI Sponsor and/or Site Owner(s).

HSIN PMO will annually review all COI and/or Site activity reports, using this information to consult with HSIN Outreach to identify any and all COI's and/or Sites that should be found to be inactive. It will then use the process above to purge the Site. A COI and/or Sites may be re-established at the request of a COI Sponsor within a one year period from purge date, without going through the complete COI stand-up/justification/Charter process.

COI Management and Content Creation

The HSIN PMO shall review and vet the request for the creation of any new COI.[29] Such review and vetting is critical to ensure that a new COI does not duplicate the stated purpose of an

[28] SF 115 Attachment

[29] COI - A social community, rooted in the common information sharing interests, requirements, and identity of a group of HSIN Users, that is technically organized around a Site or a Site Collection, 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 and/or Site in accordance with the standards and policies of the HSIN PMO. All COIs must have a Charter, a formal governance structure and a management structure.29 A user is accountable to the rules of every COI that they are a part of.

existing COI. COI Sponsors are responsible for re-evaluating their COI annually to ensure its purpose is still relevant, and that its operation is justified and active. All COIs will display official HSIN seals, logos and banners along with the seals, logos and banners appropriate to the COI to assist in its mission, in accordance with DHS co-branding policies and regulations, including Section 508 requirements. COIs are free to develop Sites as they require. The HSIN PMO need only be consulted when a new COI is requested. Such consult is intended to avoid creation of a COI that duplicates another, existing COI elsewhere on HSIN, which could in turn contribute to the duplication of the stated purpose. Site Designers have the ability to add pages and layout content within their COI without consulting the HSIN PMO. COIs are free to create webparts and functionalities they require to achieve the stated purpose of the COI. Such creation shall be done in full compliance with all HSIN policies and be accomplished in such a way so as to prevent any confusion over the mission, authority, and control of one COI versus another. All Sites must be listed in an addendum to a COI's operating charter to maintain a record of the COI's basic Site structure. The HSIN PMO is not responsible for whether or not the COI's Sites, documents, and all other media-uploads are Section 508 compliant. The HSIN PMO is only responsible for the documents and media-uploads that it, itself posts to and manages on HSIN. The posting of content within this COI may be performed by any user with the correct permissions, as provided by the HSIN PMO and the COI, and embodied in the rules established in this Charter. When a user wants to publish material that is discoverable in the Shared Space, he/she will be required to follow a standard process of approval by their COI sponsor's established policy and procedures. (See *Shared Space Activities* section.) HSIN will require default and customizable metatags to increase sharing. (See *Knowledge Management Policy* for full details.) As required, COIs may establish additional rules and procedures, in adherence with the provisions of this COI Model Charter and all other HSIN policies, governing the management and creation of content.

Sharing With Other COIs, Federated Users and Shared Space Activities

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.

Quick Incident Vetting

HSIN PMO supports quick incident vetting defined when current HSIN users nominate and validate provisional users onto the system to support a crisis event. These provisional users, or provisional for the purpose of the crisis, will have restricted, limited access to that COI and its Site(s), where they will be able to share documents and collaborate in a limited space for the purpose of emergency response. For more information on quick incident vetting see Crisis Management Policy.

PART 4 - HSIN APPLICATIONS

General Terms and Provisions

The HSIN ToS applies to all HSIN applications. No HSIN application rules or guidelines, as provided in this section (HSIN Applications), should be interpreted as contradicting or conflicting with the other sections of the HSIN ToS, unless otherwise specifically stated.

In the context of applications on HSIN, the HSIN Application Content Owner will be an identified stakeholder who shall assume a role similar to the role of a HSIN COI Content Manager as defined in *Part 1 - General Terms and Conditions, "Records Management Responsibilities,"* in the HSIN ToS. In this role, the HSIN Application Content Owner will be responsible for the following:

(1) As stated in *HSIN ToS Part 1 - General Terms and Conditions, "Freedom of Information Act (FOIA),"* the HSIN PMO is a data and content steward. It is not responsible for the content that HSIN application users post to any element of HSIN, nor is it responsible for content that remains under the custody and exclusive control of a HSIN user or at any location within HSIN or its applications. It is ultimately the responsibility of the HSIN Application Content Owner and application users to manage such content under their relevant and applicable Federal, state, municipal, territorial, and tribal information management, privacy, public disclosure (or "Sunshine laws"), records management statutes, and/or regulations.

(2) The HSIN Application Content Owner manages the records management and retention policy for application user data and data generated on or by the application in line with their own jurisdictional requirements (e.g., Federal, state, and local) and NARA schedule N1-563-11-010 for records management, as outlined in *HSIN ToS Part 1 - General Terms and Conditions*, *"Records Management Responsibilities"*.

The following provides an overview of the purpose, governance, privacy protections, and key business rules for all HSIN applications. Additional sections will be added to this part of the ToS as more applications are developed and become available to users.

HSIN Exchange and Flash Alerts

Purpose of the Application

HSIN offers a secure, centralized requests for information (RFI) management application called HSIN Exchange. HSIN Exchange provides law enforcement and intelligence professionals across the nation with an application that streamlines information requests and tracking capabilities, along with the ability to prioritize both incoming and outgoing RFIs. HSIN Exchange enables more efficient response and tracking capabilities in a secure environment, while reducing duplication of systems and effort outside of HSIN.

HSIN Exchange also allows authorized users the ability to create, send, and receive emergency notifications called Flash Alerts. Flash Alerts are notifications that HSIN Exchange users can receive via text message to their mobile phones. The goal of the Flash Alerts notifications is to remove the burden of maintaining contact information for other groups in an emergency situation and to assist operators working in a fast tempo. When an incident (e.g., terrorist attack, earthquake, etc.) requires a Flash Alert to be sent to a certain group or combination of groups (e.g., Fusion Centers in a region

of the United States), Flash Alerts leverage the contact information provided in HSIN Exchange to inform individual users across many different groups that the incident has occurred.

Application-Specific Privacy Protections

Pursuant to *HSIN ToS Part 2 - User Specific Terms and Conditions, "Privacy,"* the HSIN PMO uses personally identifiable information (PII) information to: (1) offer tailored content; (2) protect HSIN's integrity; and (3) improve services on HSIN and its applications. HSIN Application Content Owners and users must adhere to the privacy requirements listed outlined in *HSIN ToS Part 1 - General Terms and Conditions,* "Personally Identifiable Information," when collecting, maintaining, using, or disseminating PII.

Information included in RFIs uploaded into HSIN Exchange may contain PII. It is the responsibility of the authorized user(s) to manage the PII on RFIs. Similarly, in order to receive Flash Alerts, individual users must "opt-in" within the HSIN Exchange platform. Users must input additional contact information PII, to include which groups they want to receive Flash Alerts from and what mobile phone number should receive the Flash Alerts. This information is voluntarily provided by each individual user to whom it pertains.

The inclusion of PII on HSIN Exchange is protected under the procedures outlined in the DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces On The Sensitive But Unclassified Network Privacy Impact Assessment (PIA).[1] The information shared on HSIN Exchange/Flash Alerts, to include the sharing of PII, is protected under the DHS/ALL/PIA-061-1(e) HSIN R3 User Accounts: HSIN Exchange Flash Alerts PIA, which was adjudicated by the DHS Office of Privacy in April 2017. In addition, a Privacy Threshold Analysis was put into place in June 2017 to cover the exchange of PII on this application for up to three years.

Application User Registration and Permission Granting Process

HSIN Exchange utilizes user information to provide individual's access to the application in order to create, send, or receive RFIs and Flash Alerts. HSIN Exchange defines roles at an enterprise level. All HSIN Exchange users must first be granted access to HSIN through the protocols described in the DHS/ALL/PIA-061-1 HSIN R3 User Accounts PIA.[2] The only information HSIN Exchange uses from HSIN to grant new users access to the application is the individual's full name (i.e., first name and last name), HSIN user ID, and email address associated with the user's HSIN account.[3] For a user to access HSIN Exchange, an access request is made on behalf of an individual to the Group Administrator who is the assigned individual overseeing access requests. Once the request is received, the Group Administrator verifies the individual has a valid HSIN account. The Group Administrator then provisions access to the HSIN Exchange group.

Organization of Application Users, Features, and Implementation

HSIN Exchange

Within HSIN Exchange users are organized into stakeholder sets, and within stakeholder sets, groups.[4] HSIN Exchange enables stakeholder sets to define how many groups comprise the stakeholder set, as well as what information should be captured and shared in their RFI form(s). At the group level, groups are able to define access criteria and how their group will interact with other

[1] *See* DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces On The Sensitive But Unclassified Network (July 25, 2012), *available at*: https://www.dhs.gov/publication/dhsopspia-007-hsin-30-shared-spaces-sensitive-unclassified-network.

[2] *See* DHS/ALL/PIA-061-1 HSIN Release 3 User Accounts: HSIN Enterprise Reporting Solution (August 28, 2014), *available at:* https://www.dhs.gov/publication/dhsopspia-008e-hsin-r3-user-accounts-hsin-enterprise-reporting-solution.

[3] HSIN Exchange is not part of HSIN and exists as a separate, stand-alone application. Information provided by users within HSIN Exchange remains within the application.

[4] A group is a Fusion Center or federal, state, or local organization that handles RFIs.

stakeholder sets and other groups within their own stakeholder set. Groups are also able to define unique contact information about their group, which is available in a group directory for all groups participating in HSIN Exchange to access. At the user level, individuals are able to update their own contact information relevant to their role in HSIN Exchange to receive notifications, separate from that in their HSIN profile. As a result, the information updated in HSIN Exchange remains in that application and is not associated with an individual's HSIN profile.

In HSIN Exchange, all groups are either in an originating or responding roles for an RFI. The originating group of the RFI will hereafter be referred to as the Originator and the recipients of an RFI will be referred to as the Responders.

Once an RFI is distributed, HSIN Exchange allows Originators and Responders to clarify the request and ask for additional information. All Responders are able to submit multiple responses if required. Only the Originator and responding group can see responses. Responders can only see their organization's response(s), not any other organizations' responses. Responses may include structured data (e.g., expiration date, case number, date submitted), a text description, and attachments. Responders can also attach standard office documents (e.g., Word, Excel), image files (e.g., JPEG, PNG), and geospatial files (e.g., KML).

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

Users are able to set up two notifications to prompt them to open HSIN Exchange when RFIs are sent, received, and updated: (1) pop-up windows in active browser sessions of HSIN Exchange; and (2) email notifications. In order to set up these notifications, a user inputs his or her own contact information PII. This PII is inputted because the only information that HSIN Exchange receives from HSIN is the individual's full name (i.e., first name and last name), HSIN user ID, and email address associated with the user's HSIN account.

HSIN Exchange for Flash Alerts

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

Flash Alerts uses the contact information provided by individual users who have opted-in to facilitate the creation and distribution of emergency notifications to users, who are notified through email/browser pop up and or text message.[5] At least one user from each group is expected to acknowledge the alert on behalf of their group in their next active session on HSIN Exchange. HSIN Exchange allows for reporting on how many users received an alert and how many users acknowledged the alert.

Prior to using the Flash Alerts capability, all HSIN Exchange users are required to take part in a mandatory, Flash Alert-specific training conducted via the HSIN Learning Management System

[5] Prior to opting-in, users are notified that standard text messaging rates apply to receiving Flash Alerts.

(LMS), which contains the curriculum found in the HSIN PII training. During this training, users will learn how to properly use specific functionality, learn how to properly manage PII and will be informed as to what specific information can and cannot be sent out via Flash Alerts. Once mandatory training has been completed via the HSIN LMS, all users will receive a certification of completion.

When creating a Flash Alert, users will manually confirm via a pop-up that no PII is in the notification prior to distribution. The HSIN PMO will conduct regular audits are performed on the information sent using Flash Alerts to ensure no PII was disseminated. Therefore, the HSIN PMO will run audits on a random sampling of pre-existing Flash Alerts content until an automated process can be implemented. During these audits, if it is found that a user sent out PII using Flash Alerts, the user's rights will be removed and he or she will not be able to distribute emergency notifications via Flash Alerts moving forward.[6]

Application User Roles and Responsibilities

The following defines the specific user roles and responsibilities on HSIN Exchange:

Content Owner

A Content Owner on HSIN Exchange will have all of same rights, duties, and permissions to manage content as a HSIN COI Content Manager, as defined in the HSIN ToS. In the context of HSIN Exchange, there will be one stakeholder who will: (1) hold the designation of Content Owner per group; and (2) be identified by name or position title in organization in their respective business rules to be filed with the HSIN PMO. In this role, a Content Owner on HSIN Exchange will: (1) manage membership within the stakeholder set(s) and/or the groups they oversee; (2) monitor and manage the PII that is being shared on the group(s) to which they are assigned; (3) respond to FOIA requests on behalf of the stakeholder set(s) and/or group(s) they oversee; and (4) provide for the deletion and archival of the content and records shared on the group(s) they oversee, to include setting automatic content purge timelines that do not to exceed the HSIN five-year record retention threshold. To further protect any PII shared on HSIN applications, HSIN Exchange Content Owners will also be responsible for ensuring that all application users, to include Group Administrators and all other permissioned roles, have taken the HSIN PII training and have obtained the necessary certification before access to the application is granted and roles are subsequently enabled.

Group Administrator

A Group Administrator will have the rights, duties, and permissions to control information on and membership in groups on HSIN Exchange. In this role, the Group Administrator will be able to: (1) view, export, submit, modify, forward, cancel, and close RFIs; (2) end conversations; (3) create responses; (4) run reports on requests, responses, users, and the group(s) over which they hold Administrator rights; (5) view and modify the group(s) over which they hold Administrator rights; (6) view, add, remove, and disable Member rights/access in the group(s) over which they hold Administrator rights; and (7) submit feedback on the system.

Member

A Member will be granted the permissioned role of "Contribute," resulting in the ability to submit and review RFIs. All users on HSIN Exchange are eligible to be assigned to the Member role, regardless of their enhanced role. More specifically, users assigned as "Member" on HSIN Exchange will be able to: (1) view, export, submit, modify, forward, cancel, and close RFIs; (2) end conversations; (3) create responses; and (4) submit feedback on the system. This role is the baseline

[6] *See* DHS/ALL/PIA-061-1(e) HSIN R3 User Accounts: HSIN Exchange Flash Alerts PIA (April 24, 2017), *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-pia-all061-1-hsinr3accounts-april2017_0.pdf.

role to create, cancel, or close RFIs.

Reader
A Reader will be granted the permissioned role of "Read." This role is intended to have limited operational use. On HSIN Exchange, a Reader can only view and export RFIs, as well as submit feedback on the system.

Annual Filing With the HSIN PMO
Stakeholder set business rules, group-specific business rules, and content purge deadlines for Fusion Centers, the Terrorist Screening Center (TSC), and other HSIN Exchange application users shall be filed addendums to the HSIN ToS directly with the HSIN PMO annually. The filing and review of this documentation will be conducted on a sliding basis throughout the year, the exact timing of which will be set by the HSIN PMO. The HSIN PMO will notify all Fusion Centers, the TSC, and other application users of their respective deadlines for submission and work with the Content Owners to ensure that the needed documentation has been reviewed for accuracy and is revised and filed by the deadline set by the HSIN PMO.

Rights Specific to Defined Stakeholder Sets

I. Stakeholder Set: Fusion Centers

- **a. Business Description:** The National Network of Fusion Centers (NNFC) will enable one group for each DHS-recognized center for the purpose of Fusion Center-to-Fusion Center RFIs, and to respond to encounter notifications from the Terrorist Screening Center. Each Fusion Center is responsible for defining and enforcing these business rules among the users who compromise their respective stakeholder set(s) and group(s).
- **b. Stakeholder Set Business Rules:** Fusion Centers may accept RFIs internally within the Fusion Center stakeholder set, as well as externally from the Terrorist Screening Center stakeholder set. The groups may make individual decisions to further refine these business rules about who they will accept RFIs from.
- **c. Stakeholder Set Purge:** The stakeholder will set purge decisions, not to exceed HSIN's five-year record retention threshold; purge decisions will then be further defined at the group level. Each group under the Fusion Center stakeholder set will identify a Content Owner by name or position title on behalf of their group who shall be responsible for setting the purge timeframes for their respective group(s).
- **d. Number of Groups in the Stakeholder Set:** The Fusion Center stakeholder set is comprised of 79 groups, one for each DHS-recognized Fusion Center. Each Fusion Center will designate one or more Group Administrators. Each Fusion Center will also identify one Content Owner to ensure business rules and purge deadlines are set and documented accordingly.
    - **i. Group:** FUSION CENTER (FC) NAME (to be completed for each of the 79 Fusion Centers)
        1. **Group-specific business rules:**
            1. FC ACRONYM will accept RFIs from the Fusion Center stakeholder set
            2. FC ACRONYM will accept RFIs from the Terrorist Screening Center stakeholder set
        2. **Group-specific purge:** Groups to define individual purge decisions, which will be set by their respective Content Owner, not to exceed the HSIN five-year record retention threshold:

1. FC ACRONYM content will be automatically purged from the system every X days from the date of submission to recipient groups.
2. The FC ACRONYM Content Owner will be a DEFINED NAME OR POSITION TITLE IN ORGANIZATION. It is the Content Owner's responsibility to manage the PII that is being shared and to ensure FC ACRONYM Group Administrator(s) and all members have taken HSIN PII training. Additionally it is the responsibility of the FC ACRONYM Content Owner to set purge timelines (not to exceed HSIN's five-year record retention threshold) and to manage the membership of the group.

II. Stakeholder Set: Terrorist Screening Center

a. Business Description: The Terrorist Screening Center (TSC) will enable one group synonymous with the organization for the purpose of sending encounter notifications to the Fusion Center stakeholder set and managing responses and associated metrics in HSIN Exchange. The TSC is responsible for defining and enforcing these business rules among the users who compromise their respective stakeholder set and/or group.

b. Stakeholder Set Business Rules: The TSC group may send RFIs to the Fusion Center stakeholder set for response. The TSC will not receive RFIs originating from the Fusion Center stakeholder set. Individual group decisions do not apply.

c. Stakeholder Set Purge: The stakeholder will set purge decisions, not to exceed HSIN's five-year record retention threshold. TSC information shall be automatically purged from the system 90 days from the date of submission to recipients for response. Individual group decisions do not apply. The TSC will identify a Content Owner by name or position title on behalf of their Group. The TSC Content Owner shall be responsible for setting purge timeframes.

d. Number of Groups in the Stakeholder Set: The TSC will enable one group, synonymous with the organization. The TSC will designate one or more Group Administrators. The TSC will also identify one Content Owner to ensure business rules and purge deadlines are set and documented accordingly.

i. Group: Terrorist Screening Center (TSC)

1. Group-specific business rules:

I. TSC will not accept RFIs from the Fusion Center stakeholder set

II. TSC will only have one group and therefore will not accept RFIs from the Terrorist Screening Center stakeholder set

2. Group-specific purge: Groups to define individual purge decisions, which will be set by the TSC Content Owner, not to exceed the HSIN five-year record retention threshold:

I. TSC content will automatically be purged from the system every 90 days from the date of submission to recipient groups.

II. The TSC Content Owner will be A DEFINED NAME or POSITION TITLE IN ORGANIZATION. It is the TSC Content Owner's responsibility to manage the PII that is being shared and to ensure TSC Group Administrator(s) and all members have taken HSIN PII training. Additionally, it is the responsibility of the TSC Content Owner to set purge timelines

(not to exceed HSIN's five-year record retention threshold) and to manage the membership of the group.

III. **Stakeholder Set:** [NAME OF STAKEHOLDER SET] (Includes future stakeholder sets, such as RISSNET, HIDTA, EPIC, etc.)

a. **Business Description:** [This should contain a short description of the business conducted by the stakeholder set in HSIN Exchange and how they are defining groups. The [NAME OF STAKEHOLDER SET] is responsible for defining and enforcing these business rules among the users who compromise their respective stakeholder set(s) and group(s).]

b. **Stakeholder Set Business Rules:** [This should address sending/receiving RFIs for each stakeholder set enabled in HSIN Exchange, as well as within the stakeholder set. This should also address if groups may make individual decisions.]

c. **Stakeholder Set Purge:** [This should address when information should be automatically purged, and if the decision is made at the stakeholder set level or if each group may individually define.]

d. **Number of Groups in the Stakeholder Set:** [This should address how many groups are in the stakeholder set. It will also state that each group will designate one or more Group Administrators. Groups will also need to identify a Content Owner by name or position title in organization on behalf of their group to ensure business rules and purge deadlines are set and documented accordingly.]

i. **TEMPLATE Group:** NAME (ACRONYM) (to be completed for each group in the stakeholder set)

1. **Group-specific business rules:**
   I. ACRONYM will/will not accept RFIs from the Fusion Centers stakeholder set
   II. ACRONYM will/will not accept RFIs from the Terrorist Screening Center stakeholder set
   III. ACRONYM will/will not accept RFIs from NEW STAKEHOLDER SET NAME
2. **Group-specific purge:** Groups to define individual purge decisions, which will be set by their identified Content Owner, not to exceed the HSIN five-year record retention threshold:
   I. ACRONYM content will be automatically purged from the system every X days from the date of submission to recipient groups.
   II. The ACRONYM Content Owner will be A DEFINED NAME or POSITION TITLE IN ORGANIZATION. It is the ACRONYM Content Owner's responsibility to manage the PII that is being shared and to ensure ACRONYM Group Administrator(s) and all members have taken HSIN PII training. Additionally, it is the responsibility of the ACRONYM Content Owner to set purge timelines (not to exceed HSIN's five-year record retention threshold) and to manage the membership of the group.

PART 5 - HSIN PROGRAM MANAGEMENT OFFICE SPECIFIC TERMS AND CONDITIONS

User Account Revocation

HSIN PMO, through its Outreach and/or Security Offices, may at any time, without notice, disable a HSIN user's account, or eliminate a user's membership in a given COI, to ensure that the integrity of the system is upheld. As stated in Section 2.3 *Operational Roles*, during normal operations, the COI Sponsor of a particular community, has the validating authority to disable its user members' accounts, without consultation or approval from the HSIN PMO. The COI Sponsor, or surrogate, must conduct a thorough analysis of all access points the user must be blocked from, and then engage their COI's Administrator, who in turn shall work with the Systems Administrators (the HSIN Help Desk) to eliminate a user's membership in the particular COI in question. If necessary, the COI Administrator may also recommend to the HSIN PMO, or the HSIN PMO may determine unilaterally, that the user's complete HSIN registered account should be eliminated. Alternatively, a COI Sponsor may also communicate with the HSIN Outreach and/or Security Offices to request that the HSIN PMO, through its Outreach or Security Offices, disable a particular account.

Security, Penalties, and Enforcement

The HSIN PMO has the right to uphold the integrity of the HSIN system. Therefore, if a breach of security is suspected and/or realized, HSIN reserves the right to take such actions required to ensure system integrity and to enforce discipline on relevant parties in the action of suspension, termination, or other means necessary.[30] The HSIN PMO holds the duty to report breaches to the affected parties once such information is determined creditable. Violations of HSIN security and/or system integrity may include, but not be limited to:

- Improper marking of content based on violation of document handling rules as established by an investigation by, for example the DHS Inspector General;
- Act dishonestly or unprofessionally by engaging in unprofessional behavior by posting inappropriate, inaccurate, or objectionable content;
- "Bad Actors[31]";

[30] NIST 800-53, PS-8

[31] Bad actor – including but not limited to, fraudulent access with malicious intent.

- Maliciously publish inaccurate information; and
- Harass or cause harm to another person including sending unwelcoming communications.

Intrusion detection mechanisms exist that detect unlawful activities, users, etc. The HSIN PMO, through its Outreach and/or Security Offices, may at any time, without notice, disable a HSIN users account to ensure that the integrity of the system is upheld. As stated in Section 2.3 *Operational Roles*, during normal operations, the COI Sponsor of a particular community, has the validating authority to disable its user members' accounts, without consultation or approval from the HSIN PMO. Alternatively, a COI Sponsor may also request that the HSIN PMO, through its Outreach or Security Offices, disable a particular account. HSIN provides service capabilities on a SharePoint 2010 platform. This technology allows for transparency and accountability for when a user posts or publishes content. Furthermore, the "created by" function on SharePoint, allows all users who have access to this content, to be able to see who has posted it. Additionally, HSIN PMO reserves the right to use this functionality to hold users accountable for unlawful activity. COI Sponsors may request that the HSIN PMO or HSIN Help Desk disable a user for any suspicious activity. If the HSIN PMO identifies that a user is in violation of such policies, their account may be revoked, terminated and/or suspended. The HSIN PMO will notify the COI Sponsor(s) of all COI(s) to which the offender belongs. Unauthorized attempts to gain access, upload, and/or change information on this web site is strictly prohibited and is subject to criminal prosecution under the Computer Fraud and Abuse Act of 1986, the National Information Infrastructure Protection Act, Title 18 United States Code Sections 1001 and 1030,
and other applicable Federal and State laws and regulations governing the jurisdictions where this network is used.[32] HSIN will be managed in accordance with DHS Management Directive 11042.1 (Safeguarding Sensitive but Unclassified Information), DHS Management Directive 4300.1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and other relevant policies, regulations, and laws.

Any violations of such policy can result in one or more of the following:

- Suspended or terminated access to HSIN;

[32] Your further use of the HSIN system shall be upon notice that the U.S. Government may monitor and audit the usage of this system to ensure the security of the network and to prevent its use for any purpose that constitutes a violation of law. Further use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to gain access, upload, and/or change information on this web site is strictly prohibited and is subject to criminal prosecution under the Computer Fraud and Abuse Act of 1986, the National Information Infrastructure Protection Act, Title 18 United States Code Sections 1001 and 1030, and other applicable Federal and State laws and regulations governing the jurisdictions where this network is used.

- Suspension, demoted roles and/or rights, transfer, or termination of the user(s) responsible for the violation(s);
- Escalation of issues to the appropriate authorities, outside of the HSIN PMO, for criminal investigations and/or prosecution.

Customer Service and General Program Support

In general, HSIN PMO shall fulfill its duties as a Data and Content Steward[33] and ensure a functioning, secure system for users and COIs. Such duties shall include development, management, monitoring, and maintenance of all aspects of the HSIN system, including portal development, testing, and production environments, Enterprise hardware, operating system software, and application software.

HSIN PMO shall provide HSIN Help Desk support, Mission Advocate (MA) support, and communications support to users and COIs. The Help Desk is a 24-hour support line offering technical and operational support to the HSIN users and COIs. Such support may include but is not limited to: issue resolution, general use questions, user account creation requests, user account lockouts, password resets, and other associated questions or issues within the HSIN system. Monthly reviews of the Help Desk support staff shall be conducted by the HSIN PMO. The Help Desk support staff shall be held accountable to meet strict performance criteria in order to maintain user and COI satisfaction levels.

While COI Sponsors and Managers are considered the first source of technical and subject matter expertise for users, HSIN Mission Advocates shall also be available to provide subject matter and technical expertise on all aspects of HSIN. They shall provide training, technical, and operational support for users in their assigned regions.

Important communications from the HSIN PMO will be displayed on the landing page, or "HSIN Central." Examples of these communications include, but are not limited to, expected technical outages, program announcements, alerts, newsletters, surveys, policies, etc.

[33] "The party responsible (HSIN PMO) for acting as the conduit between an information technology solution and the business portion of an enterprise that actually owns, consumes and shares content on the system, with both decision support and operational help. The data steward ensures development of an information sharing environment that allows the content on a system to be used to its fullest capacity.", HSIN COI Model Charter, 2012, pg. 4

Any enterprise-wide media or public relations communications intended for an audience external to HSIN, drafted by a COI, shall be submitted for consultation with the HSIN PMO prior to public dissemination. Such communications may include, but are not limited to press releases, formal testimony, or any major speaking engagements for the HSIN enterprise at large, or the HSIN PMO. Such communications such as internal COI communications to COI members, nor COI-specific marketing materials, do not require prior HSIN PMO approval. Likewise, the HSIN PMO will not speak on behalf of a COI without the appropriate consultation of the COI Sponsor.

HSIN PMO will annually review all COI and Site activity reports and consult with HSIN Outreach to identify any and all COI's and/or sites that should be found to be inactive. It will then use the process above to purge the site.
HSIN PMO personnel shall comply with all established information sharing security and safeguarding policies and procedures, and shall be subject to formal program sanctions should they be found to breach any such policies and/or procedures, ensuring compliance with DHS 4300A 5.1.1.c and NIST PS-8.

Design Standards

HSIN PMO will provide standard design templates that coincide with DHS co-branding policies and regulations, and which adhere in full to Section 508 requirements, for use by COIs based on their basic Site development requirements. These templates contain the minimum design requirements put forward from the HSIN PMO. Each Site Designer may configure additional webparts, functionalities, etc., to assist in the COI's mission, but must do so in coordination and consultation with the HSIN PMO and not in breach of any relevant, existing HSIN policy. The HSIN PMO is not responsible for a COI's 508 compliance. The HSIN PMO is responsible for ensuring that HSIN's design standards, and documents and media-uploads that it, itself posts and controls, are 508 compliant. (See *Section 508 Compliance Requirements*.) HSIN R3 will be organized in a new, updated manner that complements the SharePoint 2010 technological features. Therefore, all HSIN users should understand that the Site design architecture does not define the governance relationship between a COI and/or Sites. A COI Charter will identify its own governance requirements and authorities. Any Site created under a COI must be reviewed and approved by the COI's Sponsor.

Section 508 Compliance Requirements

HSIN PMO acts only as a Data and Content Steward and is not responsible for the 508 compliance of the content and/or multi-media posted by its users or COIs. The HSIN PMO is responsible for ensuring 508 compliance of HSIN's design standards and those elements of

HSIN that are controlled and managed directly by the PMO. Per DHS MD 4010.2, and to ensure content is usable by all users, each COI, must work with the HSIN PMO to ensure that its site design(s) are 508 compliant, fully conforming with the Section 508 Electronic and Information Technology (EIT) Accessibility Standards. COI Sponsor's must ensure that its members are aware of, and if applicable, receive the appropriate 508 compliance awareness training (SEE roles and duties section, and SEE training requirements section). All members of the HSIN enterprise may contact DHS Office of Accessible Systems & Technology, (202) 447-0440, accessibility@dhs.gov with questions or for information on training available related to Section 508 accessibility requirements.

Modifying HSIN Functions/Features

HSIN may regularly change and improve its services including adding or removing functionalities or features. Additionally, HSIN may suspend or stop a service altogether. HSIN PMO will work with users to ensure modified services are communicated in a timely manner.

Tools

HSIN shall provide tools for users and COIs such as virtual teleconferencing, instant messaging, "My Site", and geospatial functionalities that support real-time, virtual collaboration among HSIN users. All of these tools must be used in support of the desired outcomes and purposes of the missions supported by HSIN and of the DHS ISE, and not for perfunctory, administrative matters with no relation to the mission of HSIN and the ISE.

HSIN Connect is a HSIN capability that supports real-time, virtual collaboration among HSIN users. HSIN Connect sessions are intended to support the purpose and goals of the national and DHS ISE, be hosted by registered HSIN users. HSIN Connect sessions related to the national and DHS ISE purpose and goals will have priority. HSIN Connect sessions involving the communication and/or use of types of Sensitive But Unclassified (SBU) information, shall ensure compliance with all related handling requirements, as required. If a HSIN Connect Session Host needs to conduct a session with more than four-hundred (400) users, the host must request approval from the HSIN PMO, as outlined below (See "Exceptions Under Special Circumstance").

The HSIN PMO may consider requests for potential use of the Connect feature outside of activities that serve the national or DHS ISE purpose and goals, and/or requests for use of the feature involving more than 400 participants. To consider a request, a registered HSIN user may either: (1) contact their appropriate Mission Advocate to then send the request to the HSIN Outreach Office; (2) contact the HSIN Help Desk to then send the request to the HSIN Outreach

Office; or (3) directly contact the full-time, Federal employees of the HSIN Outreach staff. Upon receipt of the request for approval, the HSIN Outreach Office shall promptly consider the request in direct consultation with appropriate representatives of HSIN Systems Engineering, obtain the technical opinion of Systems Engineering, and make a decision on whether to make an exception. The decision will then be promptly communicated to the user making the request. A HSIN user shall have the right to edit/modify their profile in their HSIN My Site (aka My HSIN) profile, viewable by other HSIN users. A HSIN user, prospective and otherwise, 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. A user who believes they have been misidentified through the third-party validation service as part of the normal identity proofing process, shall be required to contact the HSIN Help Desk to address their issue.

Additionally, users are reminded that content on these tools are archived and can be retrieved at any time. The posting of any unprofessional, false, misleading, profane, or defamatory material will not be tolerated. Complaints and/or posts that include threatening, harassing or discriminatory content; a suspected or actual breach of national security; or involve other similarly serious matters will be reported to appropriate authorities for action. These conditions, and all related guidelines, apply to all actions and posts using these tools, including, but not limited to video, audio, chat pods or conversations and file share pods.

Use of Soft Tokens

HSIN supports a soft token authentication method in alignment with industry security standards. A soft token is a cryptographic key that is typically stored on disk or some other media. [34] User authentication is accomplished by proving possession and control of the data provided via soft token, or "key". Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.[35] Additionally, HSIN will also require a one-time passcode upon entry. The system generates a unique identifier for each session and may allow a user to be logged on for up to 12 hours from that unique identifier. That passcode will be delivered in one, or more, of three ways: (1) email; (2) SMS; or (3) landline.

Personal Identity Verification (PIV) Card Access

[34] NIST 800-63
[35] NIST 800-63

HSIN will, at a point in time in the future, accept and be able to verify Personal Identity Verification (PIV) credentials issued by other Federal agencies as proof of identity.[36] HSIN PMO will fully adopt PIV authentication and soft tokens as the primary methods of identity proofing, replacing the need for hard tokens. This change will be communicated in advance and is expected to be implemented during a future development phase.

Separation from Duty

HSIN access is revoked for a user who no longer works for a supported mission area or is reassigned to other duties. Additionally, if a user's original criteria for membership in HSIN changes, they must repeat the registration process for HSIN access.

Social Media

Under no circumstances shall sensitive information be posted to social media sites by or through HSIN, its users or COIs.

System Availability

HSIN PMO will use its best efforts to provide system availability 24 hours a day, 7 days a week, 365 days a year, excluding time for routine off-line system maintenance, periodic backups, or outages caused by factors beyond control. HSIN PMO will notify COI Sponsors and Site Owners and to the greatest extent possible users, in advance of any disruptions of scheduled service maintenance.

[36] DHS 4300a 1.6.d

Signature Page

HSIN Terms of Service

Homeland Security Information Network

Approved by:

Original signed and on file with the HSIN Policy Office

_____ _____

Program Director, HSIN Date

Original signed and on file with the HSIN Policy Office

_____ _____

OPS Director, or Appointed Surrogate Date