Community of Interest Model Charter

Part 1: HSIN GOVERNANCE & THIS CHARTER

1.1 Purpose of the COI Model Charter

The purpose of this Community of Interest (COI) Model Charter is to ensure that there is consistent form and content in the governance of COIs across the Homeland Security Information Network (HSIN). This substance and consistency will ensure transparency and accountability for the whole HSIN enterprise. This COI Model Charter provides all COIs and the HSIN Program Management Office (PMO) with a common reference from which to develop a specific and final charter ("Charter") required to govern and manage each COI.

Each COI is entitled and empowered to modify and finalize, in close coordination with the HSIN PMO, this COI Model Charter, as it requires, to meet its particular, community's mission needs. The COI Model Charter is a baseline of terms for the governance and management of a COI. Any required changes to the primary terms of this charter, other than the addendum that documents architectural elements of the COI environment, will undergo a re-review and require a formal approval by the COI Sponsor in coordination with the PMO. HSIN Release 3 will be deployed using Microsoft SharePoint 2010 platform. This document may leverage terminology provided by Microsoft SharePoint 2010.

1.2 HSIN Information Sharing & Governance Philosophy

One of the major goals of HSIN Release 3 and all of its COIs is to ensure that sensitive but unclassified (SBU) information within the system does not become "stovepiped" and that full avenues for information sharing are in place across all mission areas, levels of government, and non-governmental partners in the advancement of the purpose of the national Information Sharing Environment.[1] The purpose of HSIN is to provide stakeholders across the Homeland Security Enterprise with the means for effective and efficient collaboration for decision making, tiered secure access to data, and accurate, timely information sharing and situational awareness. HSIN, as the designated information-sharing portal for the Department of Homeland Security (DHS) and its security partners[2], serves as the principal platform for consolidation and/or interoperability with DHS information-sharing portals. HSIN is the only federal portal that provides information sharing among DHS and its Federal, State, local, territorial, tribal, international, and private sector partners across the full spectrum of homeland security missions.

[1] ISE Business Model, http://ise.gov/ise-business-model (3/21/12)
[2] Secretary Michael Chertoff Memorandum, "Homeland Security Information Network Deployment," 1/9/6.

HSIN facilitates information sharing and coordination across all DHS mission areas and supports the Emergency Management Community, Critical Infrastructure Community, Law Enforcement Community, Intelligence Community, and the DHS relationship with the Department of Defense.

To achieve these ends, HSIN seeks only to create those governing bodies and documents required to achieve a network of trust and the efficient, effective management of all forms of HSIN policy. There are three forms of policy at work within HSIN: Enterprise policy, affecting and used by all elements of the HSIN enterprise; Program policy, effecting and used primarily by the HSIN PMO; and User policy, effecting and used primarily by HSIN users and their communities. The form of HSIN governance is a function of these three types of policy. The table below summarizes these policy types in greater detail, with examples.

Policy Type	Policy Consumer	Governing and Advisory Bodies	Governing Rules	Examples
Enterprise	All elements of HSIN	HSIN Executive Steering Committee (ESC) (primary) HSIN Advisory Council (HSINAC)[3]	ESC Charter; Policy on Policy Management; Policy Management Plan	COI Model Charter
Program	HSIN Program Management Office	Senior Leadership Team	Policy on Policy Management; Policy Management Plan	Policy on HSIN Connect Users and Uses
User & Requirements	Registers Users, COIs, Mission Areas	Combination – As Required – ESC, SLT, Change Control Board (CCB), HSIN User Working Group and Other User Working Groups	CCB Charter; Requirements Management Plan; Terms of Service COI Charter	Terms of Service; Internal COI Management

Table 1: HSIN Policy Types

To govern these three policy types, HSIN has established the following governance model, with each form of governance reflecting the function of each policy type.

[3] NOTE HSINAC is a FACA committee that provides recommendations to the HSIN PMO on requirements that the HSIN PMO considers in-depth because the committee represents the perspective of State, local, territorial and tribal (SLTT), which is the Federal government's full partner in homeland security across the US.

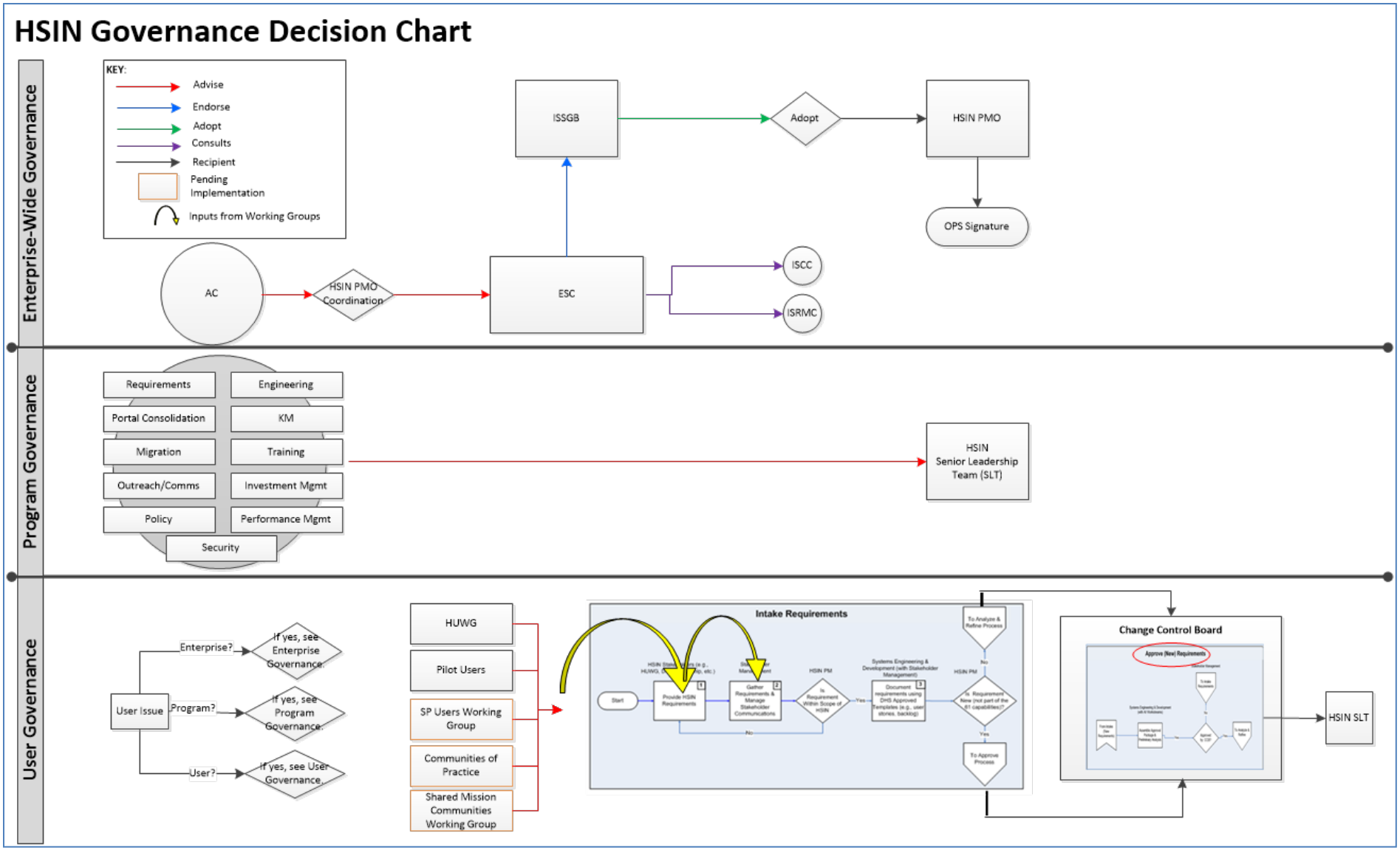

Figure 1: HSIN Governance Decision Model

HSIN users, through their COI Sponsors, have a right to engage with the HSIN PMO to address their new system requirements. To do so, Users may engage one of the major user working groups noted in the governance diagram above (See Figure 1), or, may utilize their Mission Advocate, Outreach team, or online feedback forms. These technical requirements are managed through the HSIN CCB and vetted, adopted or rejected through the HSIN SLT. Should COIs have issue with an SLT requirements decision, they may address them through the HSIN Outreach Team, the CCB and ultimately, the SLT and the ESC.

Full details of HSIN governance and policy management can be found in the HSIN Policy Management Business Plan, as kept on file by the HSIN PMO.[4]

1.3 The Relationship of this COI Model Charter to HSIN Governance

This COI Model Charter, and the specific missions and Charters of each COI, serve to advance the Mission of the national Information Sharing Environment (ISE) and of HSIN itself. This COI Model Charter is a function of HSIN Enterprise Policy – it is used and referenced by all elements of HSIN. When finalized, individual COI Charters will also be a function of Enterprise policy, used and referenced by the COI, its sponsors, users, the HSIN PMO and all other HSIN communities, to fully establish the terms on which the COI is established, managed, and governed, along with the rights and duties of users and the HSIN PMO in relation to the particular Community. Nothing in this COI Model Charter, any other Charter, nor the architecture of HSIN R3 shall be misconstrued so as to conflict with or infringe upon any mission operator authorities or goals, or create inappropriate or inaccurate authorities or relationships between jurisdiction types or COI sponsors.

PART 2: COI ESTABLISHMENT, ORGANIZATION & MANAGEMENT

2.1 Purpose of the COI

The purpose of this Charter is to establish the authority, scope, mission and goals, roles, responsibilities and functions for the Homeland Security Information Network (HSIN) [insert mission area/name][5] COI.

a. Authority: [insert]
b. Background, history, intent of the COI [insert]
c. Mission, Vision and Goals: [insert]

[4] HSIN PMO, "Policy Management Business Plan," 2012.
[5] Items highlighted in yellow are marked so as to indicate particular sections of this template where COIs shall be required to input their own, original content.

2.2 Organization, Governance and Management of the COI

The governance and management of this COI shall be organized and executed through the following form(s) and process(es):

[COI to insert a graphic summing up its governance, decision making and management structure(s), and to include language summarizing the graphic's contents, all related roles and their duties. A list of mandatory and optional COI roles is provided below in the COI Model Charter]

The following describes the COI Sponsor Roles, Permissioned Roles, and collateral roles that each Site Group within a COI will establish as the utilization of HSIN by the group requires for effective management of the Site. These roles leverage the standard Microsoft SharePoint 2010 language since HSIN will be utilizing that platform. All modifications to a Site design below a Site Collection[6], does not require permission from the HSIN PMO, but Sites must be listed in the addendum to a COI Charter to ensure clear governance is outlined. Additionally, modifications of COI and Site designs must adhere to Section 508 requirements and the standard template design guidance provided from the HSIN PMO.

2.3 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. Figure 2 illustrates the privileged roles within a COI.

[6] Site collection - A site collection is a group of Web sites that have the same owner and share administration settings. Source: http://technet.microsoft.com/en-us/library/cc263165.aspx

HSIN Privileged Roles

Community of Interest (COI)

COI Sponsor -
Primary authority over a COI and liaison between its COI and HSIN PMO.

Site Collection Administrator –
Granted "full control" of one or more Sites within a Site collection of a COI

Site

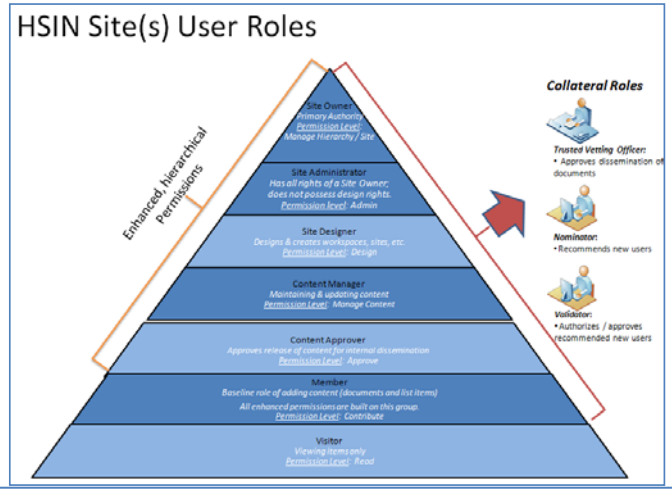

Figure 2: HSIN Privileged Roles

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 Trusted Vetting Official (TVO) or Content Manager, to ensure duplicate documents do not exist in or are posted from their COI, documents are appropriately tagged, by Federal, state/local jurisdiction for Privacy, Freedom of Information Act (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 Collection 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.

2.4 HSIN Site(s) User Roles[7]:

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.

[7] 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.

HSIN Site(s) User Roles

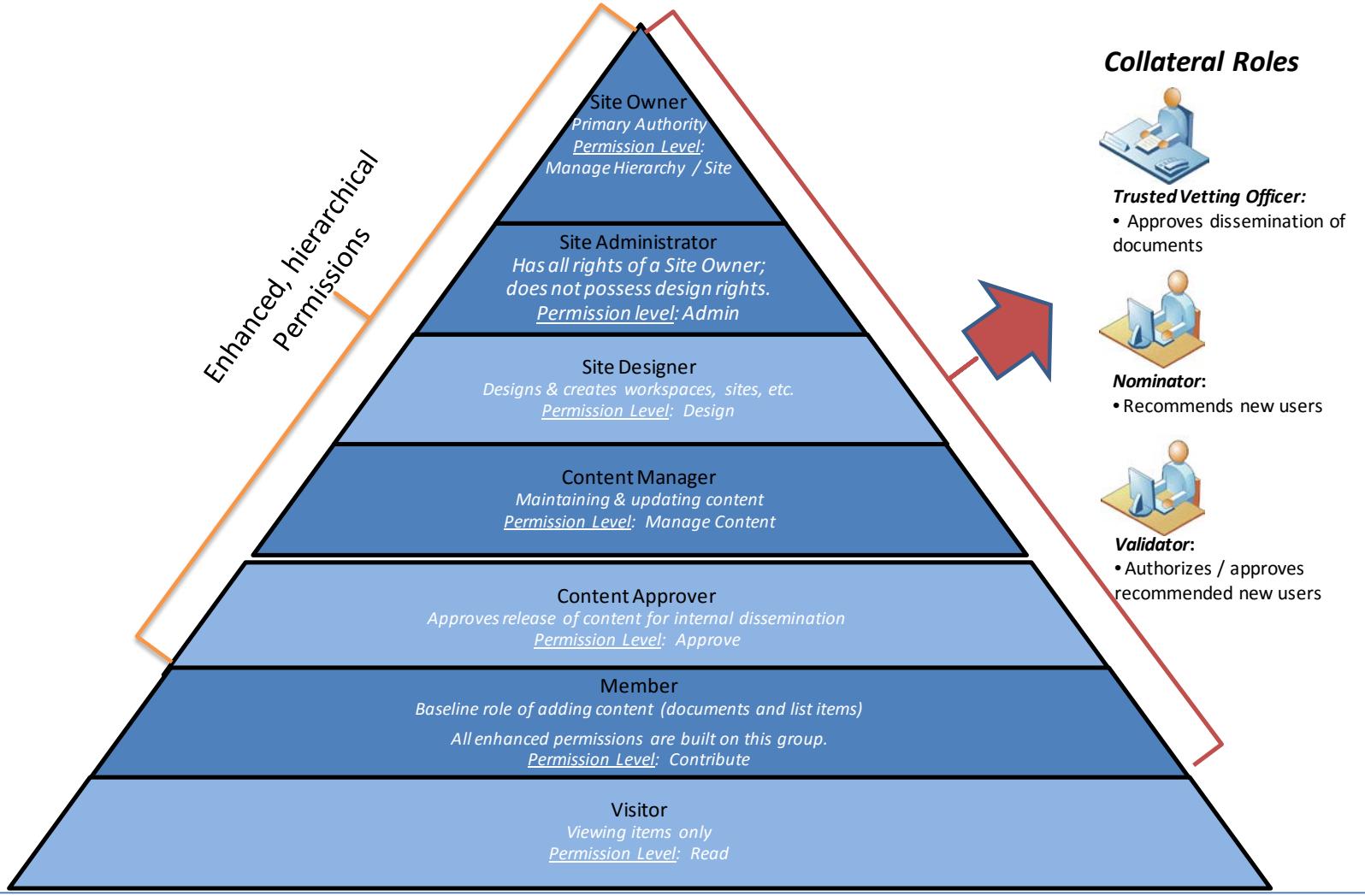

Figure 3: HSIN User Roles

Site Owner

A Site Owner will be granted the permissioned role of "Hierarchy Manager" and Site Owner at the Site level. 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 HSIN 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. "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.

2.5 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[8] 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

[8] 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.

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[9]; 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 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[10]:

- 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.

2.6 Modifications to, Enforcement and Recording of the COI Charter

If and when content within this Charter needs to be modified, other than the addendum which documents architectural elements of the COI's use of HSIN, the COI Sponsor, or its designee, shall consult and obtain agreement from the HSIN PMO of the modifications, formally approve and authorize the changes, and provide a copy to the HSIN PMO. This process will assure the modification's implementation is in compliance with all HSIN policy. In addition, any additions to addendums will require consultation and agreement from the PMO prior to modification by the COI Sponsor or delegated representative. Examples where this Charter may be modified include, but are not limited to: (1) authoritative role change; (2) revised governance / management structure; and/or (3) revised mission / vision / goals of the COI, and (4) addition and/or removal of Site and/or Site Collections within the COI.

[9] Mission areas: Emergency Management, Law Enforcement, Critical Infrastructure, Emergency Services, Intelligence, and Public Health – HSIN Program Plan 2012-2014 (Final)
[10] HSIN Release 3 User Story ID #348, 4/10/12

The COI Sponsor(s) has enforcement authority over this COI. HSIN PMO empowers the COI Sponsor to monitor activity in this COI, enforce the provisions of the COI's Charter, and report any suspicious behavior to the HSIN PMO. If suspicious behavior is dismissed or appropriate action is not taken, HSIN PMO reserves the right to request a new COI Sponsor to manage the COI and to ensure the integrity of the HSIN enterprise. For further information, please refer to the HSIN Policy on *Security Incident Response* and/or the *Security, Penalties, and Enforcement* section of this Charter.

HSIN PMO shall maintain a copy of the agreed upon Charter leaving the original with the COI. The HSIN PMO retains the right to unilaterally modify the terms of this Model Charter document, and must provide notice of such modifications to the entire enterprise.

2.7 Joining the COI

HSIN maintains strict permissioning controls for use when determining if an applicant for membership to HSIN can become a registered HSIN user. These controls are designed to uphold the security and integrity of HSIN. These controls provide users transparency on terms of service and make enforcing penalties easier. Users may decline to provide their information during this initial review process, but by doing so, their application for access will be rejected and they will not be provided an account. Upon successful review and authentication, each user will be assigned to a COI.

A user can belong to multiple COIs, and for that reason, he/she must be familiar with the terms of service associated with HSIN and be made aware of the rules governing each COI they are a member of by the Sponsors of the COIs they are a part of, including, but not limited to, their records management requirements, privacy standards, and their own responsibilities and obligations as a user of HSIN and as a member of a COI. 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. COI Sponsor(s) of this COI shall be responsible for all approving authority of nomination and validation procedures for the COI and its Sites. Nomination and/or validation duties must be approved 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 delegating Nom/Val authority to a Federal agency who is not a COI Sponsor of that COI, unless that person is a member of the COI). Nominations into COIs will expire after 60 days. After the 61st day, the HSIN user must be re-nominated. The COI Sponsor shall be responsible for accepting 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 COI Sponsor must 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 users making up the COI[11]. The table below illustrates the list of sample COIs.

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)

[11] The requirement that a Sponsor(s) 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 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.

	• United States Secret Service (USSS)
Departments & Federal Agencies	• Federal Bureau of Investigations (FBI) • Department of State (DOS) • Department of Interior (DOI) • Department of Energy (DOE) • Department of Veterans Affairs (VA) • Department of Defense (DOD) • Defense Information Systems Agency (DISA) • Defense Intelligence Agency (DIA) • Defense Security Service (DSS) • 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 • Arizona • Arkansas • California • Colorado • Connecticut • Delaware • District of Columbia • Florida • Georgia • Hawaii • Idaho • Illinois • Montana • Nebraska • Nevada • New Hampshire • New Jersey • New Mexico • New York • North Carolina • North Dakota • Ohio • Oklahoma • Oregon • Pennsylvania • Rhode Island

	• Indiana • Iowa • Kansas • Kentucky • Louisiana • Maine • Maryland • Massachusetts • Michigan • Minnesota • Mississippi • Missouri	• South Carolina • South Dakota • Tennessee • Texas • Utah • Vermont • Virginia • 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

In addition to these controls, this COI maintains additional criteria for admitting new users into its community. A user applicant into this COI, must possess the following credentials to become a user-member of this COI:

- User must support a mission that falls under the national and DHS Information Sharing Environment (ISE);
- Vetted to access For Official Use Only (FOUO) information;
- Adhere to and accept the HSIN Terms of Service
- [Insert COI's additional membership criteria.]

2.8 User Account Revocation

Please refer to the appropriate section of the HSIN R3 Terms of Service for full details.

2.9 Behavior on HSIN

COI Sponsors will take responsibility for user compliance to his/her behavior within their COI and throughout HSIN.[12]

2.10 COI & Site Inactivity

Please refer to the appropriate section of the HSIN R3 Terms of Service for full details.

2.11 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 via a web browser, mobile device or other application. Such users shall be subject to the rules governing a the HSIN Federated Users COI, including additional COI membership criteria, in the same way as any other registered, HSIN user. See *HSIN Federated User Rights Management Policy* for full details.

2.12 COI Management and Content Creation

The HSIN PMO shall review and vet the request for the creation of any new COI[13]. Such review and vetting is critical to ensure that a new COI does not duplicate the stated purpose of an existing COI. COI Sponsors are responsible for reevaluating 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

[12] Full description of 'Behavior on HSIN' is outlined in the HSIN Terms of Service.

[13] 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.13 A user is accountable to the rules of every COI that they are a part of.

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.

2.13 Section 508 Compliance Requirements

Please refer to the appropriate section of the HSIN R3 Terms of Service for full details.

2.14 Site Management

A COI shall have the right to create new Sites and functional pages within the COI as required to fulfill its mission. COIs shall create such Sites in consultation with the HSIN PMO, primarily to avoid the creation of new Sites which may duplicate the purpose of other, existing Sites within the requesting COI or another COI. Each COI's Charter shall document Sites and functional pages, their purpose and structure, as an addendum to the Charter, and define the relationship, mission need, and membership rights of the new Site within the COI. The Site shall be subject to the same COI inactivity rules established above (See COI and/or Site Inactivity section above). In addition, Sites may not be created which would duplicate the purposes of an already created Site and the mission of its COI, without coordination with the potentially affected, COI and the HSIN PMO. Nothing in this section shall be construed to limit the ability of any COI to create workspaces and groups.

2.15 Sharing With Other COIs, Federated Users and Shared Space Activities

The HSIN Shared Space shall operate as a repository of approved finished products or relevant documents published by authorized stakeholders and members that are (1) permissioned and secured at the document level based upon prescribed document attributes and the permissions of a particular user; and (2) targeted to an audience. This COI's users shall create and submit content they desire to be shared in the Shared Space and with other COIs to the COI's TVO. The TVO shall be responsible for reviewing the content to ensure that it can appropriately be shared to the Shared Space and other COIs that are in compliance with the user content creator's

original content tagging's, inter-COI information sharing agreement, and all other COI and HSIN policies. The TVO will then either approve, reject, or modify the request for sharing and forward the content appropriately. All shared content must be tagged for "findability." No content shall be published to the shared space, another COI, or made available to Federated users in such a way as to violate this Charter's privacy policy, improperly disseminate PII, or be in contravention of any COI's rules and/or procedures regarding the proper handling and distribution of content with particular markings (e.g., the handling of Law Enforcement Sensitive or Protected Critical Infrastructure Information information). A COI shall be free to develop and implement any and all rules it requires to govern, manage and define the criteria, attributes and markings necessary for sharing content from the COI to the shared space, other COIs and Federated users.

PART 3: Applicable Laws, Regulations and Policies

3.1 Freedom of Information Act (FOIA)

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, local, 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 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, local, 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 this COI Charter, on the Federal, State, local, 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.

3.2 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.[14] 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.

3.3 Privacy

The COI Sponsor must ensure compliance with all HSIN privacy policies as required and appropriate, including those found in the HSIN Terms of Service (TOS)[15] and the HSIN R3 Privacy Impact Assessments (PIA).[16]

3.4 Records Management Responsibilities

HSIN is a Data and Content Steward and is not responsible for the management of the records[17] 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 user's 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

[14] HSIN 3.0 DHS Security Plan_draft_0.2, May 2, 2012
[15] Defines a HSIN user's basic rights, duties and privileges as a registered user of HSIN.
[16] Available at ww.dhs.gov/privacy. References the DHS/OPS/PIA-007 HSIN 3.0 Shared Spaces On the Sensitive but Unclassified Network (July 25, 2012) and the DHS/OPS/PIA-008 HSIN 3.0 User Accounts (July 25, 2012).
[17] 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).

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.[Insert what procedures keep this user in compliance with its state/local RM laws.]

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 tool are "steady state" (normal day-to-day) and are stored for five years and then destroyed.
- 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 4: ROLES, DUTIES, & PRIVILEGES OF THE HSIN PMO IN CONCERT WITH THE COI

4.1 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 whether or not the COI's site, 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 Central (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.

4.2 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 purpose of HSIN and of the DHS Information-Sharing Environment (ISE) and not for perfunctory, administrative matters with no relation to the missions 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 (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 HSIN 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; (2) contact the HSIN Help Desk to then send the request to the HSIN Outreach; or (3) directly contact the full-time, Federal employees of the HSIN Outreach staff. Upon receipt of the request for approval, the HSIN Outreach 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.

4.3 Customer Service and General Program Support

In general, HSIN PMO shall fulfill its duties as a Data and Content Steward and ensure a functioning, secure system for users and COIs. Please refer to the HSIN TOS for the full description of the HSIN PMO's responsibility to provide customer service and general program support to its users.

4.4 Security, Penalties, and Enforcement

The HSIN PMO has the right to uphold the integrity of the HSIN system. The COI Sponsor

acknowledges the HSIN PMO's roles and responsibilities pertaining to the security, penalties, and enforcement processes in protecting HSIN. Therefore, if a security breach 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.[18] 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 are not 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[19]";
- 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 platform 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

[18] NIST 800-53, PS-8

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

this network is used.[20] 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;
- 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.

4.5 Training[21]

The HSIN PMO shall offer baseline training regarding the topics below, however COI Sponsors and users have the duty and responsibility to pursue applicable training required to meet their own missions. Training topics provided from the HSIN PMO include:

1. Classifications and Markings--Personally Identifiable Information (PII), Sensitive Security Information (SSI), For Official Use Only, etc. (FOUO)
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
7. Mobile Device Access
8. Nomination / Validation Authorization
9. Privacy
10. Records Management

[20] A user's 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.

[21] 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.

11. Rules of Behavior[22]
12. Section 508 Guidance
13. Shared Space Activities
14. Templates
15. Tools (Jabber, HSIN Connect, My Site, et al.)

To the greatest extent possible, the COI Sponsor acknowledges that the 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 guides (QRGs), and computer based training (CBTs). These modules would also include best-practice guidance on topics such as document management and content dissemination.

PART 5: ADDITIONAL PROVISIONS

5.1 Standard Operating Procedure (SOP) References

A COI shall develop any and all SOPs required to fully implement its Charter. Such SOPs must be cataloged and regularly reviewed for accuracy and relevance, at a minimum, on an annual basis. The COI shall list in this section the procedures it shall follow to develop, implement, review, amend, and if necessary eliminate SOPs. The COI shall also provide, if possible, a listing

[22] 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)

of its SOPs in this section. If such a listing is impractical due to the sheer volume of such SOPs, or content sensitivity, then the COI may simply record in this section where a full catalog of SOPs may be found.

5.2 Terms of Service (TOS) in relation to this COI Model Charter

All COI Sponsors agree to comply with the HSIN TOS in addition to the rules provided in this COI's Charter. Any violations, or suspicions of violation of the TOS may result in termination of the COI. Nothing in this Model Charter shall be interpreted as limiting or contradicting the TOS.

5.3 User Directory

The User Directory shall only be used to network among other professionals and to leverage best practices from existing users. This directory may not be used as a contact list for mass email deliveries and or any other unsuitable activities. COI Sponsors shall assure compliance within its COI.

5.4 Expiration / Renew Date of Charter

The COI shall establish rules governing the adoption of its Charter by the Community. It shall establish rules governing the regular (at least annual) review of the Charter's provisions for modification and/or update, and shall set a date of expiration for the Charter, as well as rules governing the renewal of the Charter for an additional, prescribed period of time, as required.

This Charter shall become effective on Month/Day/Year.

This Charter shall expire on Month/Day/Year.

[insert date]

5.5 Signatures

COI Sponsor(s)

Signature(s)

Date

HSIN Program Manager

Signature(s)

Date

Appendix

Definitions[23]

a. **Community of Interest (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.[24] A user is accountable to the rules of every COI that they are a part of.

b. **Critical Infrastructure Information (CII)** - Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. [25]

c. **Data and Content Steward** – 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 and Content Steward ensures development of an information sharing platform/capability that allows the content on a system to be used to its fullest capacity.

d. For Official Use Only (FOUO) - The marking instruction or caveat "For Official Use Only" will be used within the DHS community to identify sensitive but unclassified (SBU) information that is not otherwise specifically described and governed by statute or regulation.[26]

e. **Homeland Security Information Network (HSIN)** – HSIN is the Secretary's designated platform for sharing of SBU/Controlled Unclassified Information (CUI) information between DHS and all homeland security missions, partners and jurisdictions. This Model Charter and the related HSIN Terms of Service apply to a user's and COI's use of HSIN, on HSIN, while accessing HSIN.

[23] These definitions are intended as a baseline of common, critical terms. A COI shall be free to add additional terms for definition as required in coordination with the PMO.
[24] HSIN Memorandum of Understanding Template 12-27-09
[25] MD 11042.1
[26] DHS Directive 4300A 19Mar2012, pg. 106

f. **HSIN Program Management Office (PMO) –** The administrative agency responsible for the management, operation and maintenance of all aspects of HSIN in coordination with the whole community of HSIN stakeholders.
g. **HSIN Program Manager –** The leader of the HSIN PMO.
h. **HSIN User -** An individual that, based on his or her credentials and other attributes, has been granted membership to HSIN and one or more HSIN COIs.
i. **Law Enforcement Sensitive (LES)[27] –** Information that is unclassified information originated by agencies with a law enforcement mission that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigate activity, evidence, or the integrity of pretrial investigative reports. Any law enforcement agency employee or contractor in the course of performing assigned duties may designate information as LES if authorized to do so pursuant to department specific policy and directives.[28]
j. **My Site (aka My HSIN)** – An individual user's profile page within HSIN, not requiring a governance structure, management structure, nor formal relationship to any COI.
k. **Open Source** - Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (Public Law 109-163, January 6, 2006. National Defense Authorization Act FY 2006, Subtitle D, Section 931, sub-section (a)(1))
l. **Personally Identifiable Information (PII)[29]** - 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. (Examples: Name, office phone, biography, business card.)
m. **Portal –** HSIN and its network of consolidated, migrated, interoperable information sharing platforms, designed to answer the information sharing requirements of the whole community of HSIN stakeholders.
n. **Protected Critical Infrastructure Information (PCII)** - Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor[30]. PCII will be shared only for the Homeland Security purposes specified in 6

[27] This definition is referenced at the direction of DHS Security. Should a COI have an alternative definition of LES, it should consult with the HSIN PMO regarding its potential inclusion.
[28] ODNI CAPCO Register of Markings
[29] Handbook for Safeguarding Sensitive Personally Identifiable Information (PII) at the Department of Homeland Security, 10-06-2011, http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf
[30] MD 11042.1

U.S.C. 131(3) (Section 212(3) of the Homeland Security Act), and in no event for other collateral regulatory purposes.

o. **Publish –** The act of posting, delivering, uploading or otherwise enabling the display of content to and within HSIN by a user, COI or other authorized party**.** Publication in HSIN can occur in a variety of forms, including by a User within a COI, by a COI's TVO[31] into the Shared Space, and other forms.

p. Records – "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)"[32].

q. Sector

i. Federal - The national, central government of a federated state, such as that of the United States of America.[33]

ii. International - Transcending national boundaries or viewpoints, beyond the international border of a home-state.[34]

iii. Private - The area of the nation's economy under private rather than governmental control.[35]

iv. State/Local/Territorial - The public, governing authorities of jurisdictions below that of the national, central government of a federated state.[36]

v. Tribal - The organ of internal self-government of a recognized U. S. Indian tribe, since the Indian Reorganization Act of 1934.[37]

r. Sensitive but Unclassified (SBU) – "Sensitive Information" - Information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal Government programs or other programs or operations essential to the national interest.[38]

---

[31] TVO – A collateral duty of a registered HSIN user, whose responsibilities include approving and disseminating documents outside of the original Site and/or work area.
[32] Defined in 44 U.S.C. 3301
[33] Collins English Dictionary, 2009
[34] Collins English Dictionary, 2009
[35] Random House Dictionary, 2012
[36] Random House Dictionary, 2012
[37] OED.com, 2012
[38] DHS Directive 4300A 19Mar2012, pg. 108

s. **Sensitive Personally Identifiable Information (SPII)** - PII which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples include Social Security numbers, Alien Registration Numbers, criminal history information and medical information.[39]

t. Sensitive Security Information (SSI) - Information obtained or developed in the conduct of security activities, including research and development**.**[40]

u. Site – A digital environment within HSIN intended to support information sharing between and amongst individual users and a COI. A Site is a technical solution that consists of a data repository, visual elements, administration, and every other core element of the functionality and experience for the user. Visually, a Site is represented as one or more Web pages, lists, and Web Parts. Organizationally, a Site is a sub-unit of a COI. Thus, a Site within HSIN, shall not require a formal Charter, nor its own formal governance structure. However, a Site shall have a clearly defined relationship to a governing COI. That relationship must be described in full in the governing COI's Charter, including a description of the Site's purpose, how it advances the mission and purpose of the governing COI, and how it is to be managed.[41] A Site, in and of itself, shall not be confused with a larger, socially-based, COI.

v. Site Collection(s) - A Site Collection is a group of web sites that have the same owner and share administration settings within a COI.

w. **Unclassified** - Any information that has not been properly classified as intelligence pursuant to Executive Order 13526, "Classified National Security Information," the Atomic Energy Act of 1954, as amended, or any predecessor or successor issuances.

[39] DHS 4300a 1.4.17 & 1.4.18
[40] 49 CFR 1520.5, pertaining to Transportation sector
[41] Cardarelli, Mauro, Susan Hanley, Scott Jamison. Essential Sharepoint 2010. Pearson Education. 2011. Pg. 65.

Signature Page

HSIN COI Model Charter

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