

Fusion Center Civil Liberties and Privacy Officers (CLPO) Community of Interest Charter

Part 1: HSIN GOVERNANCE & CHARTER

1.1 Purpose of the COI Charter

The purpose of this Community of Interest (COI)¹ 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.

Each COI is entitled and empowered to modify and finalize, in close coordination with the HSIN PMO its own governing Charter as it requires, to meet its community's mission needs.

1.2 The Relationship of this COI Charter to HSIN Governance

This 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. When finalized, this COI Charter will be 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 Community. Nothing in this COI Charter, nor the architecture of HSIN shall be misconstrued 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.

¹ 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. A user is accountable to the rules of every COI that they are a part of.

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 HSIN Fusion Center Civil Liberties and Privacy Officers (CLPO) Community of Interest (COI).

a. **Authority:**

1. Title 6 U.S.C. Domestic Security § 345: Establishment of Officer for Civil Rights and Civil Liberties
2. Title 42 U.S.C. The Public Health and Welfare § 2000ee-1: Privacy and Civil Liberties Protection and Oversight
3. Title 6 U.S.C. Domestic Security § 124h(i)(6): Department of Homeland Security State, Local, and Regional Fusion Center Initiative
4. Title 6 U.S.C. Domestic Security § 111(b)(1)(G): Executive Department; Mission

- b. **Background, History, and Intent of the COI:** The HSIN Fusion Center CLPO COI is anticipated to be located within the Civil Rights and Civil Liberties HSIN Site Collection Path and sponsored by the Office of Civil Rights and Civil Liberties (CRCL). The COI will include HSIN Connect. The Fusion Center CLPO COI and Connect room are to be managed/administered by CRCL staff. The COI will have its own separate Charter and Privacy Threshold Analysis (PTA) governing this community.

The purpose of the HSIN Fusion Center CLPO COI is to share information and material about privacy, civil rights, and civil liberties protections and practices among the DHS Office for Civil Rights and Civil Liberties, the DHS Privacy Office, and state and major urban area fusion center personnel, specifically with Civil Liberties and Privacy Officers (CLPOs) at those centers; and to facilitate and support a mutual self-supporting network of CLPOs to share model policies, training material, best practices, and advice on the protection of privacy, civil rights, and civil liberties in the execution of fusion center operations.

HSIN Fusion Center CLPO COI membership includes CRCL staff, along with local, state, and federal from the following agencies:

- **Local:** Local and major urban area fusion centers, such as:
 - San Diego Law Enforcement Coordination Center, San Diego, CA
 - Los Angeles Joint Regional Intelligence Center, Los Angeles, CA

- Northern California Regional Intelligence Center, San Francisco, CA
- Central Florida Intelligence Exchange, Orlando, FL
- A full list can be found at: <https://www.dhs.gov/fusion-center-locations-and-contact-information> and <https://nfcausa.org/fusion-centers/>
- **State:** State and major urban area fusion centers, such as:
 - Alabama Fusion Center
 - Arizona Counter Terrorism Information Center
 - Arkansas State Fusion Center
 - California State Threat Assessment Center
 - A full list can be found at: <https://www.dhs.gov/fusion-center-locations-and-contact-information> and <https://nfcausa.org/fusion-centers/>
- **Federal - DHS:**
 - Office for Civil Rights and Civil Liberties (CRCL)
 - DHS HQ Privacy Office
 - Office of Intelligence and Analysis (I&A)
- **Federal - Other:**
 - Department of Justice (DOJ)

Access to the Fusion Center CLPO COI, Connect room, and content will be managed by CRCL staff. COI/Connect room membership will be granted to:

1. Federal employee or federal contractor supporting the DHS State, Local, and Regional Fusion Center Initiative (6 U.S.C. § 124h);
2. State and major urban area fusion center employee;
3. State or local government employee, including sworn law enforcement officers, with duties associated with a State and major urban area fusion center; or,
4. Member of the National Fusion Center Association.

The CRCL COI administrators will conduct a bi-annual audit of all COI users and remove users who no longer require access to the COI.

The Fusion Center COI will consist of a top-level site with a document library, list, event calendars, and discussion boards. The document library will contain training materials, best practice guides, request for information and model policies. Lists on the site will include contact lists and alert lists. Content will be uploaded by CRCL, PRIV, and the

NFCA Privacy/CL Sub-Committee members. The content will be sourced from Federal, State, local, tribal, and territorial entities. New content will be created and reviewed by the Sub-Committee and DHS offices.

The HSIN Fusion Center CLPO COI will use HSIN Connect for real-time information sharing about privacy, civil rights, and civil liberties protections. The Connect room may contain a file share pod, attendee list pod, chat pod, and share pod for presentations and live briefings. All COI members will be granted access to the HSIN Connect room. CRCL staff will be hosts for the room and will operate as its content managers while the room is active. Materials shared in the file share pod would be the same as what is shared on the corresponding COI.

Information shared on the HSIN Fusion Center CLPO COI and Connect room could contain personally identifiable information (PII) on:

(1) COI members.

The HSIN Fusion Center CLPO COI and Connect room is anticipated to contain list PII on COI members for the purpose of facilitating internal communication between Fusion Center members and DHS employees. PII shared on COI members could include the following:

- first names,
- last names,
- employing organizations,
- position in organizations,
- business email addresses,
- business office phone numbers, and
- business mobile phone numbers.

COI member PII will be voluntarily entered and provided by the individual to whom it pertains and made available in the contact list located on the COI and, possibly, within any of the other lists or libraries on the COI.

A PTA will be put on file with the DHS Office of Privacy to explain the proper use and storage of PII on the HSIN Fusion Center CLPO COI and Connect room. Per the COI governance model outlined in the HSIN Terms of Service, the submitting organization is responsible for and maintains ownership over the data they share on the platform. Prior to members of the Fusion Center CLPO COI sharing PII differently than what has been

identified, HSIN will work with the CRCL staff administrators to update this Charter and other governance documentation prior to any change in information sharing.

HSIN is a data steward, and the information shared on the HSIN Fusion Center CLPO COI and Connect room is the property of the submitting organization. HSIN does not share any of the information on the HSIN Fusion Center CLPO COI and Connect room with any other DHS platform or system.

c. Mission, Vision, and Goals:

1. **Mission** – Enhance the protection of privacy, civil rights, and civil liberties in the execution of homeland security and fusion center missions by facilitating communication and collaboration among federal, state, local, tribal, and territorial partners within and outside the National Fusion Center network.
2. **Vision** – A virtual community for open communication, collaboration, and development of privacy, civil rights, and civil liberties professionals and practices at fusion centers nationwide.
3. **Goal** – Provide access, capability, and content that enables the sharing of experiences, expertise, and training.

2.2 Governance, Management and Key COI Roles

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

The HSIN Fusion Center CLPO COI Advisory Group is comprised of designated CRCL staff to provide oversight of the development, implementation, training, and use of HSIN.

The HSIN Fusion Center CLPO COI governance and management roles are as follows:

- **COI Sponsor:** Brian Sterling, Section Chief, Security, Intelligence, and Information Policy Section, CRCL
- **Site Owner(s):** David Demski, Brian Sterling
- **Site Inviter(s):** Brian Sterling (CRCL), David Demski (CRCL), Gay Flumer (CRCL), Roy Frank (Co-Chair, NFCA Sub-Committee), and Jeff Dambly (Co-Chair, Sub-Committee)
- **Site Access Requester(s):** Brian Sterling (CRCL), David Demski (CRCL), Gay Flumer (CRCL), Roy Frank (Co-Chair, NFCA Sub-Committee), and Jeff Dambly (Co-Chair, Sub-Committee)

- **Site Access Approver(s):** Brian Sterling (CRCL), David Demski (CRCL), Roy Frank (Co-Chair, NFCA Sub-Committee), and Jeff Dambly (Co-Chair, Sub-Committee)

The above key roles (COI Sponsor, Site Owner/Administrator, Inviter, Access Requester, and Access Approver) are defined as follows:

Sponsor

The COI Sponsor role is the primary authority over the COI. COI Sponsors must hold a position from a public sector institution. Each COI must have at least one sponsor. 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 COI Sponsor(s) has enforcement authority over the COI. The 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, the HSIN PMO reserves the right to request a new COI Sponsor to manage the COI and to ensure the integrity of the HSIN enterprise.²

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)³ and the HSIN Privacy Impact Assessments (PIA).⁴ In addition, each COI Sponsor must work with the HSIN PMO to complete a Privacy Threshold Analysis (PTA) and submit the PTA for approval to the DHS Privacy Office before the launch of any COI. The COI Sponsor is also responsible for ensuring the PTA is kept up to date and accounts for any changes made to the COI.

Site Owner

The Site Owner is the primary manager of a COI's site infrastructure, site content and site information sharing activities occurring within the COI and associated HSIN Connect Room. The Site Owner is responsible for managing the content shared within their COI's document libraries, lists, and discussion boards by the COI's membership. The Site Owner can be granted full control of one or more sites within a site collection or COI. The Site Owner can audit all site content. The Site Owner will be required to take the HSIN Personally Identifiable Information

² For further information, please refer to the HSIN Policy on *Security Incident Response* and/or the *Security, Penalties, and Enforcement* section of this Charter.

³ Defines a HSIN user's basic rights, duties, and privileges as a registered user of HSIN.

⁴ Available at www.dhs.gov/privacy. References the DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces On the Sensitive but Unclassified Network (July 25, 2012) and the DHS/ALL/PIA-061-1 HSIN 3.0 User Accounts (April 24, 2017) and preceding versions.

(PII) training and receive a HSIN PII certification before permissioned roles are enabled. A HSIN Community Site Owner can also have the permission roles: Inviter, Access Requester and Access Approver; however, to maintain two-person integrity, HSIN Policy requires two different individuals, (one being an Access Requester and the other an Access Approver) to give a user HSIN Community access.

Inviter

An Inviter will be granted the permission to invite new users who require a HSIN account to register and join the HSIN network. New users invited by the Inviter to the HSIN network will only have access to HSIN Central and not a HSIN Community of Interest (COI). Inviters must be from the same jurisdiction, jurisdiction-type (e.g., State, local, private), and/or mission type, as majority of the users within their associated COI (based on the stated purpose of the COI, as determined by the COI). Stakeholders trained and certified by the HSIN PMO will be assigned to the COI's Inviter group. Inviters are responsible for recommending potential new users to their COI who possess the following criteria:

- Performs a job function that meets at least one of the homeland security mission areas⁵; and
- Has a valid email address.

Access Requester

An Access Requester will be granted the permission to submit a user's request for access to their HSIN Community of Interest (COI). Access Requesters must be from the same jurisdiction, jurisdiction-type (e.g., State, local, private), and/or mission type, as majority of the users within the given COI (based on the stated purpose of the COI, as determined by the COI). Stakeholders trained and certified by the HSIN PMO will be assigned to the COI's Access Requester group. To maintain two-person integrity, HSIN Policy requires two different individuals, (one being an Access Requester and the other an Access Approver) to give a user HSIN Community access.

Access Approver

Once a user has requested access, an Access Approver will evaluate a user's access request for membership in their Community of Interest (COI). Access Approvers are responsible for granting or denying the access requesters nominee. Access Approvers 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 majority of the users within the given COI.

⁵ Mission areas – Emergency Management, Law Enforcement, Critical Infrastructure, Emergency Services, Intelligence, and Public Health – HSIN Program Plan 2012-2014 (Final)

Stakeholders trained and certified by the HSIN PMO will be assigned to the COI's Access Approver group. To maintain two-person integrity, HSIN Policy requires two different individuals, (one being an Access Requester and the other an Access Approver) to give a user HSIN Community access. Access Approvers are responsible for confirming a requested user meets the following:⁶

- The requested user meets the COI's membership criteria;
- The requested user has a valid reason for access; and
- The requested user has a valid community permission level identified.

2.3 Modifications to, Enforcement, and Recording of the COI Charter

If 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 on the modifications and the HSIN PMO shall approve and authorize the changes through a Charter update. This process will assure the modification's implementation follows all HSIN policy. Similarly, in certain situations with complex COIs an addendum may be necessary and will require consultation and agreement from the PMO prior to modification. Examples of how this Charter may be modified include but are not limited to: (1) authoritative role change; (2) revised governance / management structure; (3) revised mission / vision / goals of the COI, and (4) addition or removal of Site and/or Site Collections within the COI.⁷

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

2.4 COI Management and Content Creation

The HSIN PMO shall review and vet the request for the creation of any new COI. Such review and vetting are critical to ensure that the COI meets a purpose intended for HSIN and that a new COI does not duplicate the stated purpose of an existing COI. COI Sponsors are otherwise responsible for management and creation, to include 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

⁶ HSIN Release 3 User Story ID #348, 4/10/12

⁷ Additionally, modifications of COI and Site designs must adhere to the requirements outlined in Section 508 Awareness Training and the standard template design guidance provided from the HSIN PMO. *See Rehabilitation Act of 1973, as amended, § 508, 29 U.S.C. § 794d.*

COI to assist in its mission, in accordance with DHS co-branding policies and regulations, including the requirements of section 508 of the Rehabilitation Act of 1973, as amended.

2.5 Site Management

Refer to HSIN training for the guidelines for site management. Nothing in this section shall be construed to limit the ability of any COI to create workspaces and groups.

PART 3: Applicable Laws, Regulations and Training

3.1 Freedom of Information Act (FOIA)

The manner in which the HSIN PMO, COI Sponsors, and other users should respond to a request made pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552, is based on the circumstances of the FOIA request and the applicable laws. HSIN users are responsible for the content that they publish to any element of HSIN or for which they retain custody and control at any location within HSIN. HSIN users may be subject to the FOIA in addition to any other applicable Federal, State, local, territorial and tribal information management, privacy, public disclosure requirements (“Sunshine laws”). Likewise, they should comply with the applicable records management statutes and regulations of their jurisdiction(s) for the content that they publish and for which they retain custody and control.

The HSIN PMO is a Data and Content Steward and is not responsible for the content that HSIN users and COIs post to any element of HSIN, nor does the HSIN PMO have custody, responsibility, or control over such content for FOIA or other Sunshine law purposes. Therefore, the HSIN PMO will not release in response to a FOIA or other Sunshine law request any records HSIN users exclusively control and post on HSIN. In the event the HSIN PMO also maintains a copy of a record posted on HSIN (e.g. HSIN COI charters), the HSIN PMO will coordinate any legally required release with the appropriate COI personnel. The HSIN PMO will work to facilitate the direction of FOIA and other Sunshine law requests to the department, agency, organization, or other entity with control over the records as appropriate.

In accordance with 6 U.S.C. § 482(e), when responding to a FOIA or other Sunshine law request, HSIN COI Sponsors and other users will coordinate the release of any information originating with the Federal government with the Department of Homeland Security prior to release in order to protect from unlawful disclosure any information that (A) relates to the threat of terrorist activity, (B) relates to the ability to prevent, interdict, or disrupt terrorist activity, (C) would improve the identification or investigation of a suspected terrorist or terrorist organization, or (D) would improve the response to a terrorist act. In addition, HSIN COI Sponsors and other users will coordinate with the Department of Homeland Security on the release of information

originating with the Federal Government to ensure that information that is subject to any exemptions from disclosure under the FOIA is appropriately protected. A COI Sponsor may provide additional information, at its discretion, within this COI Charter, on Sunshine laws and records management statutes and regulations that it believes 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 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.⁸ The HSIN PMO has 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;
- Acting dishonestly or unprofessionally by engaging in unprofessional behavior by posting inappropriate, inaccurate, or objectionable content;
- "Bad Actors"⁹;
- Maliciously publishing inaccurate information; and
- Harassing or causing harm to another person including sending unwelcomed 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 user's account to ensure that the integrity of the system is upheld. Additionally, the HSIN PMO reserves the right 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, or change information on this web site is strictly prohibited and may be subject to criminal prosecution under the Computer

⁸ NIST 800-53, PS-8

⁹ Bad actor – including but not limited to, fraudulent access with malicious intent.

Fraud and Abuse Act, the National Information Infrastructure Protection Act, Title 18 of the United States Code, sections 1001 and 1030, and other applicable Federal and state laws and regulations governing the jurisdictions where this network is used.¹⁰ 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:

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

3.3 Records Management Responsibilities

HSIN is a Data and Content Steward and is not responsible for the management of the records¹¹ created, posted or shared by HSIN users, nor is it responsible for the compliance of users and COIs with the records management laws and regulations that apply to their published content 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 or over which they retain custody and control, 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 to the extent applicable.

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. If a user becomes inactive, his or her content shall be retained under the COI's records management policy and procedure. Content owners and COIs may contact the HSIN PMO to set up alerts for COI Sponsors regarding expiring data that may be up for deletion. After

¹⁰ 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, the National Information Infrastructure Protection Act, Title 18 of the United States Code, sections 1001 and 1030, and other applicable Federal and state laws and regulations governing the jurisdictions where this network is used.

¹¹ Defined in 44 U.S.C. 3301 as including "all recorded information, regardless of form or characteristics, made or received by a Federal agency 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 United States Government or because of the informational value of the data in them." (See also 36 C.F.R. § 1222.10 for an explanation of this definition).

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, the HSIN PMO may offer additional services to COIs regarding data transfer prior to purging when requested by a COI or user. However, ultimately records management is the responsibility of content owners and/or the content controlling COI. Per the HSIN Terms of Service, "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's item's last modification date." The CRCL records retention policy does not conflict with HSIN's five (5) year record retention policy and procedure. In the event information is no longer relevant to support the mission of the HSIN Fusion Center CLPO COI or is needed longer than permitted by HSIN's five-year record retention policy, it is the responsibility of the HSIN Fusion Center CLPO COI Site Administrator(s) to remove that information from HSIN and provide additional storage capacity for data, as needed. The Fusion Center CLPO COI HSIN site administrators will conduct a review of all content on the COI on a bi-annual basis to purge content that is no longer needed and/or remove content that exceeds the retention period for a HSIN's system/database.

The HSIN PMO is responsible for ensuring retention of records for the content which the HSIN PMO 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 National Archives and Records Administration (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.

3.4 Training¹²

The HSIN PMO shall offer baseline training; however, COI Sponsors and users have the duty and responsibility to pursue applicable training required to meet their own missions.

¹² 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.

PART 4: ADDITIONAL PROVISIONS

4.1 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 the Model Charter shall be interpreted as limiting or contradicting the TOS.

4.2 Customer Service and General Program Support

In general, the 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.

4.3 Expiration / Renewal 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. The Charter expires three years from the date of the last signature below and may be renewed for an additional three years every three years thereafter.

This Charter shall become effective on the date of the last signature.

4.3 Signatures

COI Sponsor: Brian Sterling, Section Chief, Security, Intelligence, and Information Policy

Signature:

Date:

HSIN Program Manager: James "Jim" Lanoue

Signature:

Date:

Appendix

Definitions¹³

- 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.¹⁴ 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.¹⁵
- 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 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. The Data and Content Steward does not have responsibility for the content that users and COIs post to any element of HSIN or retain custody and exclusive control over at any location within HSIN, under their relevant and applicable Federal, State, local, territorial and tribal information management, privacy, public disclosure (or “Sunshine laws”) and records management statutes, and/or regulations.
- 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.¹⁶
- e. **Homeland Security Information Network (HSIN)** - HSIN is the Secretary’s designated platform for sharing of SBU/Controlled Unclassified Information (CUI) information

¹³ 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.

¹⁴ HSIN Memorandum of Understanding Template 12-27-09

¹⁵ See 6 U.S.C. § 671(3).

¹⁶ DHS Sensitive Systems Policy Directive 4300A, , Version 13.1, July 27, 2017, at 159. The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).

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.

- 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 head of the HSIN PMO.
- h. **HSIN User** - An individual that, based on his or her credentials and other attributes, has been granted access to HSIN and membership in one or more HSIN COIs.
- i. **Law Enforcement Sensitive (LES)**¹⁷ - Information that is unclassified information originated by agencies with a law enforcement mission that 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 while performing assigned duties may designate information as LES if authorized to do so pursuant to department specific policy and directives.¹⁸
- 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 Intelligence** - 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 addressing a specific intelligence requirement.¹⁹
- l. **Personally Identifiable Information (PII)**²⁰ - 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 that individual regardless of whether the individual is a U.S. Citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department (examples: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account number)
- 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.

¹⁷ 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.

¹⁸ ODNI CAPCO Register of Markings

¹⁹ National Defense Authorization Act FY 2006, Public Law 109-163, § 931(a)(1).

²⁰ DHS Instruction Manual 047-01-007, Revision #3, Handbook for Safeguarding Sensitive Personally Identifiable Information (PII), December 4, 2017

- 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 requestor²¹. PCII will be shared only for the Homeland Security purposes specified in 6 U.S.C. 673 (Section 2224 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 Trusted Vetting Official²² into the Shared Space, and other forms.
- p. **Records** - All recorded information, regardless of form or characteristics, made or received by a Federal agency 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 United States Government or because of the informational value of the data in them.²³
- q. **Sensitive Information (formerly Sensitive but Unclassified (SBU))** - Any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy.²⁴
- r. **Sensitive Personally Identifiable Information (SPII)** - a subset of 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.²⁵
- s. **Sensitive Security Information (SSI)** - Information obtained or developed in the conduct of security activities, including research and development.²⁶

²¹ DHS Management Directive 11042.1.

²² Trusted Vetting Official (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.

²³ 44 U.S.C. § 3301. *See also* 36 C.F.R. § 1222.10 for an explanation of this definition.

²⁴ DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017, at 163. The term *sensitive information* as well as others will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).

²⁵ DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017, at 163.

²⁶ *See* 49 CFR § 1520.5.

- t. **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. A Site, in and of itself, shall not be confused with a larger, socially-based, COI.
- u. **Site Collection(s)** - A Site Collection is a group of web sites that have the same owner and share administration settings within a COI.
- v. **Unclassified** - Information that is not classified pursuant to Executive Order 13526 or any predecessor or successor orders. Unclassified information includes uncontrolled information and controlled unclassified information (i.e., information marked as CUI, SBU, FOUO, or other accepted markings for controlled unclassified information).