
Privacy Impact Assessment
for the

# Homeland Security Information Network (HSIN) Communities of Interest (COIs)

## Operations Directorate
## National Operations Center

June 22, 2007

UPrepared by
Theresa Philips
HSIN Program Manager
Department of Homeland Security
(202) 282-2000

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
703-235-0780

## Introduction

The National Operations Center (NOC) is a standing inter and intra-agency organization within the Department of Homeland Security (DHS) that fuses law enforcement, national intelligence, emergency response, and private sector suspicious activity reporting and serves as a focal point for natural and manmade crisis management and coordination.

The NOC established an information sharing and collaboration enterprise known as the Homeland Security Information Network (HSIN). HSIN is designed to facilitate the secure integration and interoperability of information sharing resources amongst federal, state, local, tribal, private sector commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as in undertaking incident management activities. HSIN is designed allow all relevant stakeholders access to the same relevant information set at the same time regardless of jurisdictional, geographic, or agency boundaries.

As part of the information sharing efforts HSIN supports, HSIN has established different communities of interest (COIs) within the HSIN network. HSIN COI are separate collaborative environments where users involved in the same subject matter area and/or industry may post and view potentially relevant news and information and utilize collaborative tools. The posting environment functions like an internet message board where threads (user posted subjects for discussion) are posted and users post replies within threads. Collaborative tools consist of document libraries (common resources), membership lists, and calendars. Additionally each COI has the option of using an instant message chat tool where users may discuss items of interest with other users. Each of these tools are available to each COI, although COIs may choose not to enable them.

These sources are comprised of the various HSIN COIs reflected through the HSIN Portals that include:

- **HSIN National Operations Center (NOC):** The NOC portal is the HSIN Portal designated for use by the National Operations Center and is restricted to NOC Watch Standers and members of the NOC.

- **HSIN Law Enforcement (LE**): The portal for all departments dealing with law enforcement sensitive data that meet the DOJ definition of law enforcement.

- **HSIN Government:** HSIN Government is for federal, state, and local government HSIN members with access to For Official Use Only (FOUO) or Sensitive But Unclassified (SBU) information.

- **HSIN Emergency Management (EM):** HSIN EM is the national hub for all HSIN members that have emergency management responsibilities, i.e., first responders, response planners, fire, and police assets

- **HSIN Information Analysis (IA):** The IA portal is the information sharing and collaboration environment designated primarily for members of DHS Office of Intelligence & Analysis.

- **HSIN National Capitol Region (NCR):** HSIN NCR provides members of government and representatives of the critical infrastructure providers in the greater Washington DC metropolitan area with an environment to share information and collaborate

- **HSIN International:** The International portal is for foreign partners to exchange information and collaborate during crises (Canada, the United Kingdom, and Australia).

- **HSIN State Portals:** Many of the states have requested portals for conducting state level operations to fuse information prior to entering into the national portals. Management of the state portals is done at the state level.

- **HSIN Critical Sector (CS**): HSIN CS is a collection of portals established to support and encourage information sharing in the critical infrastructure COI.

- **HSIN Congress:** HSIN Congress is the HSIN Portal designed for use by the United States Congress.

The COIs listed above may have a number of "sub-sites" or smaller COIs within them. For example, the Emergency Management COI (HSIN EM) has multiple sub-sites created for specific needs. Some of these sites include the American Red Cross Disaster Operations Center, FEMA Operations Center, the National Response Coordination Center, Fire Services, and a site for each of the nine FEMA Emergency Support Functions.

In order to gain access to the HSIN, potential users must submit biographical information and employment information so that they may be verified as legitimate potential users. A COI will initially establish membership criteria. A COI owner will nominate specific validating authorities within a single COI. Those validating authorities are responsible for verifying the legitimacy of the potential user. Once verified, the user is given access privileges to only his COI; however, a user can be a member of more than one COI if it is appropriate and the membership criteria are met.

As an additional feature, an HSIN user may elect to receive alerts and warnings that are then directed to the user's email address, telephone number(s), or fax lines. These alerts will be emergent real-time one-way communications that are geared to notice of ongoing activity status or to direct the user to a particular location within HSIN for additional information or detailed collaboration.

This privacy impact assessment covers the registration information required for access to the HSIN COIs. None of the substantive material discussed within HSIN COIs are covered by this PIA. DHS is not responsible for monitoring the specific content of HSIN; rather DHS provides the communication environment and user access controls. For all purposes, including the Freedom of Information Act (FOIA) and the Privacy Act, DHS is not the custodian of substantive information on HSIN. Federal, state and local HSIN users are bound by their own jurisdictional requirements.

## Section 1.0 Information Collected and Maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

## 1.1 What information is to be collected?

HSIN Registration Information. HSIN will collect registration information from each user that will be used to validate their status and qualifications for being a member of HSIN user groups. That information generally is name, contact information, employment information, and geographic data. Registration information may also include emergency resources that the submitter of the information maintains, which can be made available in emergency situations to permit incident managers to allocate those resources to those in need. The registration information collected is the same for all HSIN user groups and COIs, and does not vary for any prospective user, user group, portal, or for any other instance.

The registration information provided by the prospective user includes:

first name*, middle initial, last name*, email address*, mobile email address (i.e. Blackberry, Nextel, etc.), job title*, address name*, work address line 1*, work address line 2, city*, county, state*, postal code*, business phone*, mobile phone, pager, fax, other phone, first choice of contact*, second choice of contact*, third choice of contact, watch position (pertains to operations centers), choose a secret question*, answer to secret question*, sponsor/supervisor organization*, sponsor/supervisor name*, sponsor/supervisor job title*, sponsor/supervisor email address*, sponsor/supervisor business phone*, sponsor/supervisor fax, sponsor/supervisor first choice of contact*, sponsor/supervisor second choice of contact*, sponsor/supervisor third choice of contact, and completed verification*. The asterisk (*) denotes a required field.

## 1.2 From whom is information collected?

HSIN Registration Information. Information is collected from those individuals who express a desire to become users of one or more of the HSIN portals, or from individuals who are nominated for access by others into one or more of the HSIN portals. Information is also collected from the employers of potential HSIN users. This information is generally limited to confirmation of the data Information collection is limited to those individuals who wish to be granted access to HSIN. The process is the same for all COIs.

## 1.3 Why is the information being collected?

HSIN will collect registration information on each HSIN user so that the user may be validated as a member of the specific communities of interest the user was nominated for, and so the user may receive information and communicate using HSIN. HSIN users may be governmental officials, law enforcement personnel, international partners, and private sector individuals whose professional duties and interests make them stakeholders of the DHS mission.

As an example, registration information permits DHS to validate that an applicant is indeed a state or federal law enforcement officer and is thus eligible to access the criminal intelligence and law enforcement sensitive communication available via law enforcement areas of HSIN. Likewise, where HSIN has a specific communications and collaboration area available to owners and operators of critical infrastructure in the oil and gas sector of commercial industry, registration information permits DHS or representatives of the oil and gas sector to validate that applicants are owners and operators of critical infrastructure in that sector and may have access to proprietary communications and collaboration reserved for commercial entities within that sector of industry.

The sole purpose of collecting the registration information (for any COI) is to verify users for a particular COI.

### 1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The Homeland Security Act of 2002 as codified within the United States Code at 6 U.S.C. § 121(d)(1); 6 U.S.C. § 121(d)(4); 6 U.S.C. § 121(d)(11); 6 U.S.C. § 121(d)(12)(A); 6 U.S.C. § 121(d)(15); and 6 U.S.C. § 121(d)(17) provide DHS and the NOC with authority to establish HSIN and to collect the information in HSIN. As per the Paperwork Reduction Act of 1995, 44 U.S.C. 3507(d), the NOC has considered the impact of the information collection burden imposed on the public in the HSIN Registration process and is complying with the required processes for this new information collection. The HSIN Registration information is maintained in strict compliance with the notification, access, and amendment requirements of the Privacy Act of 1974 as amended, 5 U.S.C. 552a. This applies to and is the same for all HSIN COIs.

### 1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The personal and employment data collected for HSIN Registration is limited to the information necessary to validate the registrant's identity as a legitimate and approved validating authority of the respective COI, the qualifications of entry into particular HSIN collaboration spaces, or to access specific information within the HSIN Database. This is the same for and applies to all HSIN COIs.

HSIN registrant information may also include emergency resources that the HSIN registrant has and his geographic location. This feature will permit HSIN to serve as a resource identification and allocation tool to assist incident managers in identifying resources in proximity to particular events or incidents.

As noted above, only some of the information is required when a person applies to a COI. HSIN Program Management has found that users of HSIN have varying forms of primary contact methods; some users may use pagers as a primary communication device, and other users may have no pagers at all. Flexibility in registration information allows HSIN validating authorities in the COIs to approve users in the most appropriate and efficient way. Having limited and mandatory information fields would hamper the validation process.

## Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

### 2.1 Describe all the uses of information.

HSIN Registration information will be used by DHS to validate the registrant's identity and relate it to a legitimate stakeholder of the communication and collaboration resources available to HSIN, or the qualifications of entry into particular HSIN collaboration spaces. The registration information is used for this purpose for all HSIN COIs.

The supervisor/sponsor information specifically is collected for the purpose of validating the prospective HSIN user. The information provided by the prospective user must be sufficient to ensure the validating authority will be able to contact the supervisor/sponsor. When the supervisor/sponsor is contacted, the validating authority also needs to know the role of the prospective user and his/her relationship to the sponsor. This is the information the validating authority uses to contact the supervisor/sponsor, which is part of the process to guarantee the prospective user and supervisor/sponsor are who they say they are and determine if the prospective user requires access to the respective HSIN COI. Because users of HSIN have varying forms of primary communication, the required registration information is left open-ended. This accommodates all users' needs, as well as the validating authorities need for not just accurate information but the *appropriate* information.

## 2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No. HSIN enables communities of interest to gather and exchange relevant information, but does not utilize tools or programs that feature data mining or complex reporting functionalities. The tools that can be potentially enabled in each COI do not allow such features.

## 2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

A key component of the HSIN Registration verification process will be an inquiry/investigation to ascertain whether the eligibility information is accurate. Each COI designates trusted authorities, or validating authorities, with the responsibility and authority to conduct registration verification. The validating authority is a member of that COI, and is approved by DHS and the COI owner and stakeholders. Depending on the COI, the verification may include contacting employers, state agencies, or non-governmental trade associations to verify a registrant's status in their organization. The entities contacted vary by COI. For example, a registration application for a state or federal law enforcement officer would likely be coordinated with the state or federal law enforcement agency to verify an individual's identity and law enforcement credentials. HSIN Registration contact and geographical information collected directly from the registrant and not critical for determining eligibility will likely not be further checked. The accuracy of the information provided is dependent on the applicant which supports the need for the validation. The process of validation and the information provided to the validating authorities is the same for each COI. For specific criteria necessary to validate individuals into each HSIN COI, refer to section 8.5.

## 2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

HSIN has been developed in order to minimize the amount of personal information incorporated. For example, employment information and workplace contact information is collected in most cases, instead of home contact information. A mask is placed on the information so that it may only be viewed by appropriate, DHS approved HSIN administrative and registration personnel and is not available to all HSIN users. These controls are applied throughout HSIN for each COI. This ensures that privacy and

information safeguarding requirements are met by limiting access to personal information only to those users whose operational role and mission warrants such access.

## Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

### 3.1 What is the retention period for the data in the system?

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

### 3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes.

### 3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The retention period of six (6) years is adequate to satisfy the need to archive and document DHS operations. Because the registration information is not mission information the period of six (6) years does not create a significant privacy risk.

## Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

### 4.1 With what internal organizations are the information shared, what information is shared and for what purpose?

HSIN Registration information may be shared by any DHS entity or component that is involved in the process of validating the registrant's identity and relating it to a legitimate stakeholder of the communication and collaboration resources available to HSIN or the qualifications of entry into particular HSIN collaboration spaces. Additionally, limited amounts of data will be shared among internal members of the COI for the purposes of site maintenance (administration) and for supporting collaboration (notifying users of other members in their COI(s)). Information shared would be limited to name, email address, organization, and role within the COI.

### 4.2 For each organization, what information is shared and for what purpose?

HSIN authorities may share registration information with other organizations within DHS when they believe an opportunity exists for the information to permit greater communication and collaboration, including permitting HSIN users to receive alerts and warnings that are submitted to members of other DHS programs at the same time that those members receive the information. This general policy is true for all COIs: registration information may, but need not necessarily, be shared for the purposes outlined above.

### 4.3 How is the information transmitted or disclosed?

All information in the HSIN registration process will be either submitted via the internet by the HSIN registrant, or submitted *en masse* by a DHS agency, law enforcement entity, governmental agency, or non-governmental commercial or trade entity who seeks to register all of their members within HSIN.

### 4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Once maintained within HSIN, registration information will be maintained electronically and only disclosed within DHS for routine system administrative purposes or to integrate/interoperate with other DHS component communication and collaboration platforms that provide HSIN users additional features. It is anticipated that disclosures of submitted information may be released or used for governmental regulatory purposes in limited circumstances.

## Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

### 5.1 With what external organizations is the information shared, what information is shared, and for what purpose?

HSIN registration information may be shared with any external organization as required in the process of validating the registrant's identity and relating it to a legitimate stakeholder of the communication and collaboration resources available to HSIN. Additionally, limited amounts of data will be shared among the members of the COI external to DHS for the purposes of site maintenance (administrator review of users) and for supporting collaboration (notifying users of other users available in their assigned COI's). Information shared would be limited to name, email address, organization, and role within that COI.

### 5.2 How is the information transmitted or disclosed?

All information in the HSIN COI registration process will be either submitted via the internet by the HSIN registrant, or submitted *en masse* by a law enforcement entity, governmental agency, or non-governmental commercial or trade entity who seeks to register all of their members within HSIN. Once maintained within HSIN, registration information will not be shared with any external organization, unless

doing so is required in the process of validating the registrant's identity and relating it to a legitimate stakeholder of the communication and collaboration resources available to HSIN or the qualifications of entry into particular HSIN collaboration spaces.

### 5.3 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

HSIN users individually will have to certify knowledge of and the intent to comply with an End User Agreement (EUA) that incorporates their compliance with the laws and policies associated with their organization as well as the laws and policies of the jurisdictions in which they operate. The EUA, approved by DHS, does not differ from COI to COI. However, each user must accept the EUA for each COI. See Appendix B for the full EUA.

### 5.4 How is the shared information secured by the recipient?

HSIN is an internet-based medium that is subject to 128 bit secure socket layer (SSL) encryption for all transactions. The HSIN information is presumptively sensitive but unclassified. Once accessed, HSIN information available to the recipient are subject to the recipient's compliance with the laws and policies of their agency/organization, their jurisdiction, and any limitations imposed by the source/originator of the information. At a minimum, that information obtained via HSIN must thus be safeguarded by the HSIN user per the same laws/policies/business rules as information otherwise used within their agency/organization.

### 5.5 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Currently, all prospective HSIN users are provided technical training to prepare them for using HSIN. That training includes training on the associated laws and policies of their agency/organization, their jurisdiction, and training on the requirement that they comply with all access and disclosure limitations imposed by the source/originator. The above principles are also generally included in the HSIN registrant's End User Agreement. Training teams are deployed to each community where training sessions are held to instruct and prepare them for using HSIN.

### 5.6 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Any sharing of registration information is limited to the discrete purpose for which it was shared, namely the validation of registration information submitted by an individual. The registration information may be used by the account creator and account validator for no other purpose than to approve or disapprove the person's HSIN COI membership. In the future, a HSIN global address list is planned, but only minimal fields, such as email and name will be mandatory. The global address list will not be operational for approximately one (1) year or later.

## Section 6.0 Notice

The following questions are directed as notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information. The only personal information solicited by DHS in HSIN is the HSIN Registration material.

### 6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Yes. The System of Records Notice for the registration information and subsequent user verification is covered by DHS ALL 004, General Information Technology Access Accounts. It is attached as Appendix A.

Because HSIN COIs are invitation only, i.e., users are nominated then validated, individuals are aware that they will be asked for personally identifying information. Specifically, the HSIN User License Agreement (ULA) gives specific notice of Privacy Act protections and the nature of the collection.

### 6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. However, without providing sufficient registration information upon which a DHS official can validate an HSIN registrant's identity or qualifications, the registrant may be denied access to HSIN.

### 6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Yes. However, without providing sufficient registration information upon which a DHS official can validate an HSIN registrant's identity or qualifications, the registrant may be denied access to HSIN.

### 6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Individuals will be provided notice through the System of Records Notice. Personal information will be collected only with the voluntary participation and knowledge of the individual or the individual's employer. When an employer provides the registration information, it is bound by its own policies and procedures and by the employment contract it has with its employee.

## Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

### 7.1 What are the procedures which allow individuals to gain access to their own information?

HSIN registration information will be available to the registrant at all times and may be updated to ensure the accuracy of the information maintained by DHS. This is especially important for the contact information used to provide real-time alerts to HSIN users. Should users have further questions they may contact the Office of Operations Coordination at 3801 Nebraska Avenue, NW, Nebraska Avenue Complex, Washington DC, 20393.

### 7.2 What are the procedures for correcting erroneous information?

HSIN Registration information will be available to the registrant at all times and may be updated via the internet to ensure the accuracy of the information maintained by DHS.

### 7.3 How are individuals notified of the procedures for correcting their information?

HSIN Registration information will be available to the registrant at all times. The procedures for correcting their information will be co-located within the user profile section.

### 7.4 If no redress is provided, are alternatives are available?

Not applicable.

### 7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

If an individual believes that his or her HSIN Registration information is incorrect, that individual will be able to provide any information that they deem relevant with a request that it be included within any record maintained in HSIN.

## Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

### 8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Certain NOC staff including watch and technical support personnel will have access to all HSIN communication and collaboration tools. Watch staff communicate and collaborate with other HSIN users and receive, research, and respond to requests for information regarding terrorism-related suspicious

activities. Authorized HSIN IT specialists and technical and operational program managers will access HSIN to ensure system performance that will also include auditing system usage.

## 8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes. Currently there are several technology contractors who have access to the system. The contractors that have access to the system fall into three categories.

The first category is account managers. The account managers are basically users of the system at the help desk. Their role is to solve problems for user having trouble with their accounts.

The second category is the systems engineering category. Systems engineers fix bugs in the system, add functionality, and design and improve system capacity and capability.

The third category is the user. This category has many different sub-categories, such as, other government agencies, US territories, tribal, state and local, critical sectors, and also private and public users. The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information systems usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system. As deemed appropriate, users may be required to sign a Non-Disclosure Agreement before beginning any work or accessing any information on HSIN. In addition, all users of the system are required to agree to the HSIN User License Agreement (ULA) before being provided access to the system.

## 8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. The access controls involve two basic components in addition to a general audit protocol designed to identify and sanction inappropriate access.

User/Data-defined Access Controls. The first of these controls are limitations based upon a user's administratively assigned categories and roles. Certain users will be restricted from classes of information that they are not authorized by law to receive. As an example, private sector users would not be permitted to access personal information, commercial proprietary information not provided directly to them by the source agency, or law enforcement sensitive information. Access to all personal information in the HSIN will be limited to only those law enforcement and governmental users with a need to know for the performance of their official duties. The agencies entering the data retain the responsibility for the accuracy of that data.

Source/Originator Access Limitations. Originators placing information that they deem to be sensitive into the HSIN Database may also place release restrictions on the data. For example, a law enforcement agency may identify that a particular piece of information is of such sensitivity to an ongoing investigation that it may be viewed for situational awareness, but may not be officially used or referenced without contacting that agency. Similarly, a business may restrict access or use of commercial proprietary information, so that particular law enforcement agencies may access it, but may not release it publicly or

distribute it to regulatory entities unless it demonstrates a violation of law relevant to a Federal, state, municipal, or tribal law enforcement agency.

Audit Controls and Sanctions. All information will also remain linked with records of who/when that information was accessed and subjected to a periodic audit to ensure that information in the HSIN Database is used in accordance with the above described policies. Currently, the NOC is investigating the use of intelligent software analytical tools that will produce reports of questionable information access patterns of particular users in order to complement the random audit controls that will be in place. Access to personal information will always be preceded by a user record of certification that requires the user to detail his identity, the data sought, and the legal/regulatory predicate authorizing access to the data. Any user found to be falsely making such a certification will be referred to the Federal Bureau of Investigation or other entities within the Department of Justice for investigation and possible prosecution. They will also be referred to their law enforcement (governmental and/or commercial agencies) where they may also be subject to the appropriate disciplinary and legal actions.

## 8.4 What procedures are in place to determine which users may access the system and are they documented?

HSIN Registration information will be available to the DHS Operations personnel and registered users who are required to validate the registration information.

## 8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

All HSIN Portals contain information that is Sensitive But Unclassified (SBU), For Official Use Only (FOUO), or Law Enforcement Sensitive (LES). The information is derived from multiple Federal, State, local, tribal, private sector, and International sources including:

- Law enforcement organizations;
- Emergency managers and first responders;
- Intelligence analysts;
- Entities involved in maintaining the Nation's critical infrastructure:
- International partners

After ensuring each potential member may appropriately access sensitive information, each COI establishes its own membership criteria. For example, HSIN Law Enforcement (LE) COI grants access to persons who are 1) the member is a sworn law enforcement officer; 2) the member is an analyst working in direct support of law enforcement officers; and 3) the member is required to have access to LES information in the routine performance of his/her duties. These criteria are regularly verified by the COI owners and validating authorities.

## 8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Misuse of the information is subject to disciplinary action. This policy is largely controlled by supervisory efforts. However, as a technology safeguard, the Baseline 2 system has software proposed

called the Oracle COREid suite for this purpose. This identity and access management package provides a logging functionality that also tracks the activities of document generation. Control of access to only authorized users includes the effective implementation of password and account management in accordance with the provisions stipulated in the DHS 4300A Sensitive Systems Policy. This functionality, once fully implemented supports the following controls:

* passwords must expire after 90 days and cannot be one of the last four passwords used

* temporary or emergency accounts are terminated after 30 days

* accounts with no login activity for more than 30 days are deactivated

* account lock-out will occur after three consecutive unsuccessful login attempts

* session lock/termination of account by user will occur when inactive after 10 minutes

The technical level of effort coupled with resource and schedule constraints as well as system functionality release dates are factors in determining when all of the automated security controls will be implemented. In order to mitigate operational and mission risks until automated solutions are deployed, and achieve immediate compliance with the required security controls, effective immediately COI Administrators will ensure that temporary or emergency accounts are terminated after 30 days, and that accounts with no login activity for more than 30 days are deactivated monthly. The system will require that users change their passwords at least once every 90 days. The remaining automated security controls are already in place.

## 8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Training will include aspects of 28 Code of Federal Regulations (CFR) Part 23 (Criminal Intelligence Operating System Policies) compliance, discussions as to what can be put on the system, and the process of sharing of information, including a discussion of what 28 CFR Part 23 actually is and the limitations of shared information usage.

## 8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. The HSIN Certification and Accreditation (C&A) has been completed and approved on June 9, 2006.

## 8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The NIST 800-53 risk level for Confidentiality is "Moderate" per guidance from the DHS Operations Information System Security Officer (ISSO) during the HSIN C&A process. The formal risk assessment was submitted on June 1, 2006. Appropriate management, technical, and operational controls have been or will be implemented as need arises to address risks to confidentiality in general, but not to personally identifiable information in particular.

# Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

## 9.1 Was the system built from the ground up or purchased and installed?

HSIN was designed and built from the ground-up.

## 9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The registration protocol and the need for accurate registration and up-to-date contact and emergency resource registry information drove the need to ensure that HSIN Registration information maintained its validity. This requirement resulted in HSIN providing a user-friendly method for data access and amendment by co-allocating that information within an easily accessible user profile section. Further system improvements will include a "Federated ID Management System," which will carry a user's identity profile for cross-identification to other systems and accessibility to other information sources.

HSIN COIs were designed around the need for an information sharing and collaboration capability to span across a multitude of parties of the same community (e.g. emergency management, electricity sector, individual states) and to parties of other communities in effort to enhance and improve situational awareness to prevent, deter, detect, and respond to all natural and man-made events. Close coordination between DHS and COI representatives occurs to identify each COI's need so that the COI site is designed and constructed to proper specifications and capabilities.

## 9.3 What design choices were made to enhance privacy?

The role-based and situation-based access limitations are defined by the user's status as well as the nature of the information that the user can receive and the situations when the user can receive that data. This was a design choice that is directly related to the commitment to fully accomplish the NOC information sharing mission while fully protecting the privacy and protecting the commercial proprietary and law enforcement sensitivities associated with the HSIN communication and collaborations.

# Conclusion

The NOC performs a critical role in information sharing and communications, especially during periods when the nation's critical infrastructure is particularly vulnerable to or compromised by an attack or major incident. In order to fulfill its vital role and carry out the Nationally significant functions apportioned to it, the NOC must establish and sustain a complex information system that is capable of coordinating among many individual systems; that is automated, integrated, adaptable, and scalable; that is able to accommodate rapidly evolving threat capabilities; and that is able to leverage advances in technology to counter all emerging threats to the security of the American homeland. The HSIN was defined to fulfill those requirements. It was envisioned as an internet-based platform to ensure compatibility and interoperability with a host of communication and collaboration tools. The registration protocol for HSIN

was identified as a critical function for ensuring that HSIN members are capable of validation. It also served as a key component in the development of business rules for access to the NOC Database.

## Responsible Officials

Theresa Philips
HSIN Program Manager
Department of Homeland Security

## Approval Signature Page

Original signed and on file with the DHS Privacy Office. June 22, 2007

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

# APPENDIX A

**BILLING CODE 4410-10**

**DEPARTMENT OF HOMELAND SECURITY**

**Office of the Secretary**

**[Docket No. DHS-2006-0076]**

**Privacy Act of 1974; System of Records.**

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of Privacy Act System of Records.

**SUMMARY**: In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it proposes to add a new system of records to its inventory of record systems for Department of Homeland Security General Information Technology Access Account Records System.

**DATES**: Written comments must be submitted on or before January 29, 2007.

**ADDRESSES:** You may submit comments, identified by DOCKET NUMBER DHS-2006-0076 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-572-8727 (not a toll-free number).
- Mail: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

**FOR FURTHER INFORMATION CONTACT:** Please identify by DOCKET NUMBER DHS-2006-0076 to request further information by one of the following methods:

- Mail: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528
- Facsimile: 202-572-8727 (not a toll-free number).
- E-Mail: privacy@dhs.gov

**SUPPLEMENTARY INFORMATION:**

As part of its efforts to streamline and consolidate its record system, the Department of Homeland Security (DHS) is establishing a new agency-wide systems of records under the Privacy Act of 1974 (5 U.S.C. 552a) for the Department of Homeland Security General Information Technology Access Account Records System (GITAARS). This system of records is part of DHS's ongoing record integration and management efforts. This system will consist of information collected in order to provide authorized individuals with access to DHS information technology resources. This information includes user name, business affiliation, account information and passwords.

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the U.S. Government collects, maintains, uses and disseminates personally identifiable information. The Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act requires each agency to publish in the Federal Register a description of the type and character of each system of records that the agency maintains, and the routine uses for which such information may be disseminated and the purpose for which the system is maintained. Individuals may request their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

In accordance with 5 U.S.C. 552a(r), a report on this system has been sent to Congress and to the

Office of Management and Budget.

**DHS-2006-0076**

**System name:**

General Information Technology Access Account Records System, DHS/ALL 004.

**Security classification:**

Unclassified but sensitive.

**System location:**

Records are maintained by the Department of Homeland Security at the DHS Data Center in Washington, DC, and at a limited number of remote locations where DHS components or program maintain secure facilities and conducts its mission.

**Categories of individuals covered by the system:**

A. All persons who are authorized to access DHS Information Technology resources, including employees, contractors, grantees, private enterprises and any lawfully designated representative of the above and including representatives of Federal, state, territorial, tribal, local, international, or foreign government agencies or entities, in furtherance of the DHS mission;

B. Individuals who serve on DHS boards and committees;

C. Individuals who have business with DHS and who have provided personal information in order to facilitate access to DHS Information Technology resources; and

D. Individuals who are facility points of contact for government business and the individual(s) they list as emergency contacts.

**Categories of records in the system:**

DHS/ALL 004 contains names, business affiliations, facility positions held, business telephone numbers, cellular phone numbers, pager numbers, numbers where individuals can be reached while on

travel or otherwise away from the office, citizenship, home addresses, electronic mail addresses, names and phone numbers of other contacts, the positions or titles of those contacts, their business affiliations and other contact information provided to the Department that is derived from other sources to facilitate authorized access to DHS Information Technology resources.

**Authority for maintenance of the system**:

5 U.S.C. 301; 44 U.S.C. 3101.

**Purpose(s):**

This system will collect a discreet set of personal information in order to provide authorized individuals access to DHS information technology resources. The information collected by the system will include full name, user name, account information, citizenship, business affiliation, contact information, and passwords.

The system enables DHS to maintain: a) account information for gaining access to information technology; b) lists of individuals who are appropriate organizational points of contact for the Department; and c) lists of individuals who are emergency points of contact. The system will also enable DHS to provide individuals access to certain programs and meeting attendance and where appropriate allow for sharing of information between individuals in the same operational program to facilitate collaboration.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses**:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3), limited by privacy impact assessments, data sharing, or other agreements, as follows:

A. To DHS contractors, consultants or others, when necessary to perform a function or service related to this system of records for which they have been engaged. Such recipients are required to comply with the Privacy Act of 1974, as amended (5 U.S.C. 552a).

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

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

D. To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the written or attested to request of the individual to whom the record pertains.

E. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. Sections 2904 and 2906.

F. To the Department of Justice (DOJ), or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS; (b) any employee of DHS in his/her official capacity; (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation.

**Disclosure to consumer reporting agencies:**

None.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Records in this system are on paper and/or in digital or other electronic form. Digital and other electronic images are stored on a storage area network in a secured environment.

**Retrievability:**

Information may be retrieved by an identification number assigned by computer, by facility, by business affiliation, e-mails address, or by the name of the individual.

**Safeguards:**

Information in this system is safeguarded in accordance with applicable laws, rules and policies, including the DHS Information Technology Security Program Handbook. Further, GITAARS security protocols will meet multiple NIST Security Standards from Authentication to Certification and Accreditation. Records in the GITAARS will be maintained in a secure, password protected electronic system that will utilize security hardware and software to include: multiple firewalls, active intruder detection, and role-based access controls. Additional safeguards will vary by component and program. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include: restricting access to authorized personnel who have a "need to know;" using locks; and password protection identification features. Classified information is appropriately stored in accordance with applicable requirements. DHS file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

**Retention and disposal:**

Records are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, "User Identification, Profiles, Authorizations,

and Password Files." Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

**System manager(s) and address:**

For Headquarters components of the Department of Homeland Security, the System Manager is the Director of Departmental Disclosure, U.S. Department of Homeland Security, Washington D.C. 20528. For operational components that comprise the U.S. Department of Homeland Security, the System Managers are as follows:

- United States Coast Guard, FOIA Officer/PA System Manager, Commandant, CG-611, U.S. Coast Guard, 2100 2nd Street, S.W., Washington, DC 20593-0001.
- United States Secret Service, FOIA/PA System Manager, Suite 3000, 950 H Street, N.W., Washington, DC 20223.
- Under Secretary for Federal Emergency Management Directorate, FOIA/PA System Manager, 500 C Street, S.W., Room 840, Washington, DC 20472.
- Director, Citizenship and Immigration Services, U.S. Citizenship and Immigration Services, ATTN: Records Services Branch (FOIA/PA), 111 Massachusetts Ave, N.W., 2nd Floor, Washington, DC 20529.
- Commissioner, Customs and Border Protection, FOIA/PA System Manager, Disclosure Law Branch, Office of Regulations & Rulings, Ronald Reagan Building, 1300 Pennsylvania Avenue, N.W., (Mint Annex) Washington, DC 20229.

- Bureau of Immigration and Customs Enforcement, FOIA/PA System Manager, Office of Investigation, Chester Arthur Building (CAB), 425 I Street, N.W., Room 4038, Washington, DC 20538.
- Assistant Secretary, Transportation Security Administration, FOIA/PA System Manager, Office of Security, West Building, 4th Floor, Room 432-N, TSA-20, 601 South 12th Street, Arlington, VA 22202-4220.
- Federal Protective Service, FOIA/PA System Manager, 1800 F Street, N.W., Suite 2341, Washington, DC 20405.
- Federal Law Enforcement Training Center, Disclosure Officer, 1131 Chapel Crossing Road, Building 94, Glynco, GA 31524.
- Under Secretary for Science & Technology, FOIA/PA System Manager, Washington, DC 20528.
- Under Secretary for Preparedness, Nebraska Avenue Complex, Building 81, 1st floor, Washington, DC 20528.
- Director, Operations Coordination, Nebraska Avenue Complex, Building 3, Washington DC 20529.
- Officer of Intelligence and Analysis, Nebraska Avenue Complex, Building 19, Washington DC 20529.

**Notification procedure:**

To determine whether this system contains records relating to you, write to the appropriate System Manager(s) identified above.

**Record access procedures:**

A request for access to records in this system may be made by writing to the System Manager, identified above, in conformance with 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS.

**Contesting record procedures:**

Same as "Records Access Procedures" above.

**Record source categories:**

Information contained in this system is obtained from affected individuals/organizations/facilities, public source data, other government agencies and/or information already in other DHS records systems.

**Exemptions claimed for the system:**

None.

Dated:

Hugo Teufel III,

Chief Privacy Officer.

# Appendix B

HSIN User License Agreement

---

Registration Notice:
You are entering an official United States Government system, which may be used only for authorized information coordination conducted within HSIN to include (but not be limited to) functions such as information gathering, processing, dissemination, sharing, archiving, and the general business records management practices associated with Federal, state, municipal, tribal, and private sector information management and exchange. HSIN may not be used for lobbying, advertising, or product endorsement purposes. 18 U.S.C. § 1030 prohibits unauthorized or fraudulent access to government computer systems. If the registration information associated with this action is not your correct information, you are in violation of this law and should exit this system immediately. Completing this action may subject you to a fine of up to $5,000 or double the value of anything obtained via this unauthorized access, plus up to five years imprisonment.

Monitoring and Auditing:
Your further use of this 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.

Compartmented Access to Information:
The information within HSIN is limited to particular communities whose users are vetted through detailed registration, identity verification, and access validation protocols approved and in some cases monitored or conducted by the U.S. Government. Information available to those communities of users is presumptively For Official Use Only (FOU), Law Enforcement Sensitive (LES), Protected Critical Infrastructure Information (PCII) or the proprietary information of non-governmental owners/operators of critical infrastructure or their agents. CLASSIFIED INFORMATION SHALL NOT BE PLACED OR MAINTAINED ON THIS SYSTEM.

Privacy Data and Criminal Intelligence Information:
HSIN governmental users involved in information coordination processes are subject to the Federal, state, municipal, and tribal information management, privacy, and public disclosure (or "sunshine") statutes and regulations of their jurisdictions. Compliance with all applicable Federal, state, municipal, and tribal laws and regulations is a nondelegable responsibility of the individual users and the agencies to which they belong. Some representative examples of the types of statutes and regulations applicable would include but are certainly not limited to 5 U.S.C. 552, The Freedom of Information Act; 5 U.S.C. 552b, The Privacy Act of 1974 (as amended); 28 C.F.R. Part 32, Criminal Intelligence System Operating Policies; Executive Order 12333, United States Intelligence Activities; and DoD Directive 5240.1R, Procedures

Governing the Activities of DoD Intelligence Components That Affect United States Persons. Again, these laws and regulations are only applicable to the extent that they apply to a particular agency or individual using HSIN. The Department of Justice has defined the HSOC as a law enforcement activity that is 28 C.F.R. Part 32 compliant for information sharing with law enforcement agencies and activities operating criminal intelligence systems through support under the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. §§ 3711). The HSOC and all LE communities operating within the HSIN system shall be governed by the provisions of 28 C.F.R. Part 32 and operated in a manner that conforms with or respects all agency/jurisdiction-specific law enforcement regulations and policies.

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

Private sector information that may be proprietary, submitted as protected critical infrastructure information, or otherwise law enforcement sensitive will be managed in compliance with all security and safeguarding provisions imposed by law and agreed upon between the applicable private sector entities and the source agency. Private Sector information posted into HSIN by non-governmental entities and labeled, "Proprietary Information of [posting Private Sector entity]" is the proprietary information of the posting Private Sector entity and is presumed to include material contributed or licensed by individuals, companies, or organizations that may be protected by U.S. and foreign copyright laws or the release of which may subject the posting Private Sector entity to commercial harm, competitive injury, or regulatory action. All persons/entities/agencies seeking to exploit, reproduce, redistribute, or making any use of such information that could possibly result in non-governmental or regulatory disclosure shall strictly adhere to the terms and conditions asserted by the copyright holder, and any transmission or reproduction of protected items beyond that allowed by fair use as defined in Title 17, Section 107 of the United States Code requires the written permission of the copyright owners.

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

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

DISCLAIMER

This site is maintained by the U.S. Government. The information available from this site may include law enforcement sensitive information; material contributed or licensed by individuals, companies, or organizations that may be protected by U.S. and foreign copyright laws; or material that is otherwise not subject to public release under or due to the Freedom of Information Act or the Privacy Act. Because much of the information that may be communicated on this system may be pre-analytical (raw) suspicious activity information from numerous Federal and state governmental, law enforcement, and many private sector sources; the U.S. Government does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or processes disclosed through this system. The U.S. Government does not endorse or recommend any products, processes, or services of non-federal or commercial entities. The views and opinions of authors expressed within products on HSIN web sites do not necessarily state or reflect those of the U.S. Government, and they may not be used for lobbying, advertising, or product endorsement purposes. Some HSIN web pages may provide links to external internet sites for the convenience of users. The U.S. Government is not responsible for the availability or content of those external sites, nor does the U.S. Government endorse, warrant, or guarantee the products, services, or information described or offered at those other internet sites. Users should be aware that external sites referenced by links within HSIN do not necessarily abide by the concept of operations, policies, or rules to which HSIN adheres. The compliance policies and rules concerning information coordination required for access to HSIN are not intended to create or confer any right, privilege, or benefit to any private person including any person in litigation with the United States or any agency or individual using HSIN.