Privacy Impact Assessment
for the

Homeland Security Information Network Database

April 5, 2006

Contact Point
Laura Manning
Deputy Director, Raw Data Fusion
DHS Office of Operations Coordination
(202) 282-8313

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

The Homeland security Operation Center (HSOC) is a component of the Department of Homeland Security that serves as the primary national hub for domestic incident management operational coordination and situational awareness. A key focus of the HSOC is the coordination and dissemination of terrorism-related information that is operationally significant for decisions and actions undertaken by stakeholder entities, such as governmental officials, law enforcement personnel, non-governmental organizations, and private sector individuals that have domestic situational awareness requirements. The HSOC also serves as a primary national level hub in domestic incident management; serving dually as an operational communications and information sharing hub, as well as the primary conduit to the White House and the Secretary of the Department for significant domestic events and incidents.

The Homeland Security Information Network is a secure internet-based system of integrated communication networks designed to facilitate information sharing between DHS and other Federal, state, county, local, Tribal, private sector commercial, and other non-governmental organizations involved in identifying and preventing terrorism as well as in undertaking incident management activities. The mission of HSIN is to enhance the communication of relevant information among all applicable domestic security actors regardless of jurisdictional, geographic, or agency boundaries. Additionally, HSIN enables these organizations to maintain voice and data communications with one another during incident management. The HSIN is managed by the HSOC.

The HSIN Database supports the HSIN user community by enabling approved users to research and analyze information with a "nexus to terrorism"[1]. The HSIN Database is populated with information from:

- suspicious activity reports from law enforcement, governmental agency, or private sector security officials;
- law enforcement bulletins and reports from Federal, state, county, local, and/or Tribal law enforcement, and
- relevant information from approved HSIN users communications.

Prior to inclusion in the HSIN Database, information will be reviewed by HSOC personnel to ensure a nexus to terrorism. After a nexus is established, the information is categorized based on sector, subject matter, geography, and need to know.

The HSIN Database focuses primarily on activities, rather than individuals. It is made up of reports about what individuals, either law enforcement or otherwise have observed that is out-of-the-ordinary based upon their judgment/experience and the circumstance of their observation. In most but not all cases, such observations will not include personally identifiable information, but rather the facts of a situation. In instances where the observation or incident led to personally

[1] A "nexus to terrorism" is defined as information important to the identification of terrorism planning and preparation and relevant to the nation's efforts to prevent acts of terrorism against the United States.

identifiable information being obtained, this information will be logged into the HSIN Database, and additional safeguards will be employed, including masking the information. The data including names would only be available to those whose roles authorize them to access/collect such information (primarily law enforcement and the intelligence community). Other users such as private sector security managers would only be able to access the activity-based information; the private and other sensitive data would be masked. If they have need for more information, private sector users will either contact the source entity (such as another private sector entity) or look to local law enforcement for additional information they might be eligible to receive.

The HSIN and the HSIN Database will enable DHS to build a "Common Operational Picture" (or "COP"), which relates critical operational information in a consolidated, user-defined format that is organized by event, incident, or potentially significant threat. COP enables key domestic security stakeholders to coordinate their prevention, mitigation, repose, and recovery activities and decision making.

This Privacy Impact Assessment describes the system, functions, data safeguards, and data integrity features of the HSIN Database.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

HSIN Database will collect relatively "raw" suspicious activity information. This type of information is generally provided by individuals who observe the activities of others and deem that activity suspicious based upon the totality of observable circumstances.

The HSIN Database will be limited to relevant information for which there is a nexus to terrorism. While the primary focus of the information will be on activities, the personally identifiable information accepted for retention as part of a particular submission may include: full name, address, date of birth, place of birth, citizenship, physical description (height, weight, eye and hair color), distinguishing scars, marks, or tattoos, automobile registration information, watch list information, intelligence information including links to terrorism, any criminal and/or incident activity, the date information is submitted, and the name of the contributing/submitting organization.

Limited data concerning the providers of information, including the means of transmission of the data, may also be retained where necessary. For example, where it is determined that maintaining the identity of the source of investigative lead information may be necessary to provide an indicator of the reliability and validity of the data provided and to support follow-on investigative purposes relevant and necessary to a legitimate law enforcement or homeland security matter, such data may likely warrant retention. Absent such a need, no information on the provider of the information would be maintained.

1.2 From whom is information collected?

Information is collected from:

- Private individuals submitting tips either directly to the HSOC or through law enforcement officials;
- Suspicious activity reports from law enforcement, governmental agency, or private sector security officials;
- Law enforcement bulletins and reports from Federal, state, county, local, and/or Tribal law enforcement; and
- Relevant information from communications between approved HSIN users, such as experienced critical infrastructure security managers.

Prior to inclusion in the HSIN Database, information will be reviewed by HSOC personnel to ensure there is a nexus to terrorism. After the nexus is established, the information is categorized based on sector, subject matter, geography, and need to know.

1.3 Why is the information being collected?

The information in the HSIN Database is collected in order to provide key domestic security actors with information necessary to coordinate their prevention, mitigation, response, and recovery activities.

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 HSOC with authority to collect the information in the HSIN Database.

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.

In general, the information collected as part of suspicious reporting will not be personally identifiable. In instances where personally identifiable information is relevant and necessary to be collected, it will be protected with additional safeguards, including masking, so that only those individuals with appropriate access and a verifiable need to know will be able to review the personally identifiable information collected.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The information collected in the HSIN Database enables HSIN users to research and analyze activities with a nexus to terrorism. It allows users to draw links and patterns that might not otherwise be readily apparent.

As stated in the introduction, DHS uses the information to build the COP. The COP is a merger of all relevant and available information associated with emerging events or incidents in a consolidated format to facilitate decision makers.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (sometimes referred to as "datamining")?

Yes. The HSIN Database can be mined in a manner that identifies potential threats to the homeland or trends requiring further analysis. Access to sensitive information, including personal information, is limited to only those users with a verifiable need for that access.

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

The information contained within the HSIN Database will be provided by government or non-governmental personnel. Information from government entities will remain associated with the source government entity, which may be contacted by authorized law enforcement or government personnel accessing that information to question its accuracy or update its status. Those same source entities are expected to update information that they provide in the HSIN Database as investigative activity produces additional amplifying information or results in closure of the case.

Information from non-governmental entities is suspicious activity information that will be entered into the HSIN Database and that will, generally, be concurrently addressed to a law enforcement agency for investigation. Updated information will be entered by authorized users and remain associated with the initially submitted information.

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.

The HSIN Database has been developed in order to minimize the amount of personal information incorporated. In instances where personal information is required, a mask is placed

on the information so that it may only be viewed by appropriate personnel with the correct user roles and verifiable need to know. This ensures that privacy and information safeguarding requirements are met by limiting access to sensitive information, such as personal information, only to those users whose operational role and mission warrants such access. This limitation is further enforced by ensuring that the data is distinctly segregated into sections based upon its sensitivity.

Section 3.0 Retention

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

HSOC personnel plan to request records disposition schedules and coordination of those schedules with the National Archives and Records Administration (NARA) for ten years from the time of inclusion in the HSIN Database. Not all records will remain active during this time; rather, it is anticipated that the HSIN Database will maintain both active and inactive records. HSIN users will be required to change the status of their submissions from active to inactive if an incident is determined to have no nexus to terrorism. The system will provide HSIN users with reminders for active reports that have not been resolved after a certain period of time.

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

HSOC personnel plan to request records disposition schedules and coordination of those schedules with the National Archives and Records Administration (NARA) for ten years from the time of inclusion in the HSIN.

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

Given that most contemporary knowledge of terrorist planning indicates long periods of pre-operative activity, and that some seemingly innocuous criminal and surveillance activity could signal terrorist planning, a 10-year retention period is deemed necessary for law enforcement investigative activities, governmental, and other subject matter experts to link the information with known terrorist activity or to identify the activity as benign and unrelated to terrorist activity. HSOC has developed the "active" and "inactive" records in order to minimize the impact of information being maintained for this time period, and access to inactive records will be more closely controlled.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Initial access to the HSIN Database will only permit access to activity-based information; personal information will be masked. The activity-based information in the terrorism-related suspicious activity reports contained within the HSIN Database will be shared with the DHS components whose legitimate law enforcement or governmental terrorism-related missions require access to the information. Where access to sensitive information, such as personal information, is determined to be necessary, access will be based on a verifiable need to know and will be subject to any restrictions placed on that data by the submitter.

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

All information that is relevant and necessary to an HSIN user will be made available, but personal information is only provided in instances where the HSIN user has the appropriate clearance and a verifiable need to know.

4.3 How is the information transmitted or disclosed?

HSIN users are able to query the HSIN Database directly over a secure network.

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

In order to minimize the number of individuals with access to information while maximizing the usefulness of the information provided, HSIN Database masks personal information and other sensitive information. HSIN Database then uses role-based access to enforce these rules.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Because the purpose of the HSIN Database is to increase information sharing for homeland security purposes, HSIN users may be governmental officials, law enforcement personnel, non-governmental organizations, and private sector individuals whose professional duties and interests make them stakeholders of the DHS mission. HSIN users will only be provided access to information that is relevant to their official duties.

Initial access to the HSIN Database will only permit access to activity-based information. Sensitive information such as personal information will be excluded from the activity-based

information that is subject to analytical processes and shielded from those conducting analysis. In no case will non-law enforcement or non-governmental users be afforded access to personal information in the HSIN Database.

5.2 What information is shared and for what purpose?

All information that is relevant and necessary to an HSIN user will be made available, but personal information is only provided in instances where the HSIN government or law enforcement user has the appropriate clearance and verifiable need to know. Personal information will never be provided to private sector HSIN users.

5.3 How is the information transmitted or disclosed?

HSIN users are able to query the HSIN Database directly over a secure network.

5.4 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 comply with an End User Agreement that requires their adherence to the rules and policies associated with their organization as well as the laws and policies of the jurisdictions in which they operate. Additionally, all entities collaborating and communicating using HSIN or maintaining access to the HSIN Database will be bound by Memoranda of Understanding that will detail all aspects of their access, use, security, and permissible further dissemination of the data within the HSIN Database.

5.5 How is the shared information secured by the recipient?

In order to access to the HSIN Database users must have appropriate encryption capabilities; essentially, the ability to access web sites whose addresses begin with "https". In addition, entities collaborating and communicating using the HSIN Database or maintaining access to it will be bound by Memoranda of Understanding governing all aspects of their access, use and further dissemination. These agreements will include information security provisions.

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

DHS and external users of HSIN who access law enforcement sensitive information must be credentialed members of law enforcement agencies or designees who receive training in the protection of personal information. Similarly, government entities who partner with DHS and are HSIN users or maintain access to information with a nexus to terrorism in the HSIN Database must receive similar training from their employers.

Currently, all prospective HSIN users are being provided technical training to prepare them for using HSIN, including training on the associated laws and policies of their agency/organization, their jurisdiction, and on the requirement that they comply with all access and disclosure limitations imposed by the source/originator of the HSIN communication or the HSIN Database information. The above principles are also generally included in the HSIN registrant's End User Agreement and any Memorandum of Understanding for entities/organizations that partner with DHS for the use of HSIN resources or access to the HSIN Database.

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

Categorizing the information when it is included in the HSIN Database, in coordination with enforced role and rule-based access, minimizes the number of people with access to personally identifiable information.

Section 6.0 Notice

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?

A system of records notice for this system was published in the Federal Register on April 18, 2005, under the title "HSOC Database" to provide notice. DHS intends to publish a final SORN for the HSIN Database which will be more limited and refined in scope than originally published in the April 18, 2005 notice. Beyond this, in instances where personal information is provided as part of the suspicious report, the individual is unlikely to have knowledge that his/her information has been submitted to the system.

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

When an individual is submitting information to the HSIN Database, he/she has the right to decline providing personal information. As an example, an anonymous caller contacts a law enforcement agency with a report of suspicious activity. The information may be submitted to HSIN without capturing the callers identifying information. For personal information that may be associated with suspicious activity reports, there is no opportunity to decline to provide information.

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?

Although HSIN information may have originator controls that govern particular uses of it, in general, individuals will not be able to consent to particular uses of the information. For suspicious activity reports received directly from individuals, however, such individuals may be protected as confidential sources.

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. Given that in some instances personal information will be collected without the knowledge of the individual, the HSIN Database masks the personal information so that only those individuals with appropriate clearance and a verifiable need to know are able to see the information.

Section 7.0 Individual Access, Redress and Correction

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

Individual access to information in the HSIN Database is available through the provisions of the Freedom of Information Act and the procedures for submitting FOIA requests are available in 6 C.F.R. Part 5.

7.2 What are the procedures for correcting erroneous information?

Because personal information is likely to be in the HSIN Database based on a suspicious activity report, which is, in essence, the opinion of an observer, no procedures will be established to allow for correction of this opinion information. If an individual believes that he or she has suffered an adverse consequence related to the HSIN Database, 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 the HSIN Database regarding a particular incident, activity, transaction, or occurrence. That correspondence will be directed to the DHS HSOC Watch Floor, and a member of the watch will research the HSIN Database to ascertain whether any record correlates to the information provided. If there is correlative information, the watch officer will enter the information provided into that record and indicate it as First-Party Amplifying information.

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

If an individual feels that the information maintained in the HSIN Database is inaccurate, there will be three methods available to provide accurate information to the HSOC Watch. The DHS FOIA page, accessible through the DHS public website, will contain a link permitting any individual to send information to the HSOC via a designated email address reserved for that purpose. The FOIA page will also contain a fax number and a mailing address for the same purposes for those who prefer to use those means to contact to the HSOC. All communications received, regardless of method, will be entered into and remain on record within the HSIN Database pursuant to its general record retention schedule and will be subject to audit.

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

The development of the HSIN Database and the processes governing its use included detailed consideration of the impact of erroneous data on individuals as well as on the official users of the information with the Database. Information in the HSIN Database is, by definition, raw suspicious activity information. The HSIN Database is simply a pool of unvetted, reported "as-is" information that is maintained in a manner making it accessible to appropriate official entities for further investigation and analysis predicated upon reasonable suspicion of a terrorism nexus.

Having verified and accurate information is the ultimate goal of all of the law enforcement, intelligence community, and other governmental officials using the system. The redress indicated in 7.2, above, will help to ensure that the information is accurate.

HSOC Watch-standers will ensure the integrity of the HSIN information based upon information provided by individuals, as well as any updates received from law enforcement and other government authorities.

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.

The HSIN Database focuses on collecting activity-based information rather than personally identifiable information. Any personal information included in an activity report is masked so that the number and type of individuals with access to the information is minimized. If an individual believes that he or she has suffered an adverse consequence related to the HSIN Database, 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 the HSIN Database regarding a particular incident, activity, transaction, or occurrence.

Section 8.0 Technical Access and Security

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 HSOC staff including watch and technical support personnel will have access to all HSIN communication and collaboration tools and the HSIN Database. Watch staff communicate/collaborate with other HSIN users and receive, research, and respond to requests for information regarding terrorism-related suspicious activities. IT specialists and HSOC technical and operational program managers will access HSIN and the HSIN Database to ensure system performance and to audit the use of the system. Analysts throughout law enforcement, government, and in some cases private sector security management may have access to the activity-based informational areas of the HSIN Database. All of these analyst users and other registered users, whose identity and need for access have been validated, will have varying levels of access to HSIN Database.

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 as they build the information network and the database. Such contractors or other IT professionals will be registered and managed using the same auditing and controls as every other HSIN user.

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 Database 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 HSOC 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 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?

The registration process will verify registrant eligibility for specific communication tools and collaboration spaces within HSIN and for information within the HSIN Database. The HSIN Database access control is role-based. Controls and access limitations are in place to ensure that sensitive information is protected from unauthorized access or exchange. Additional controls may be established to further define access to emergent, incident, and event-based information as required. In all cases access will be in accordance with applicable law and policy.

Role-Based Access Limitations. As an example of the role-based access, only a law enforcement officer will have access to law enforcement tradecraft and other sensitive information such as how information was acquired and what technical and operational means and methods were applied.

Situation-Based Access Limitations. As an example of additional controls, in order for a law enforcement officer to obtain personal information associated with a particular matter, the law enforcement officer must also meet the threshold of reasonable suspicion of criminal activity that may lead to terrorism. Without meeting that threshold, the officer will only have access to activity-based information minus the names and contact information of all involved (other than the source/originating agency). Prior to such information being accessed or displayed the officer will be prompted to certify he has a verifiable need-to-know the information and has met the reasonable suspicion standard. Once having so certified, the officer will be able to access all

pertinent information based upon his certification. All sensitive information requiring such a certification will always be displayed with a banner defining it as subject to the certification requirement and to audit. Similarly, intelligence community personnel will be subject to certification requirements prior to access of applicable information based upon intelligence oversight requirements defining their access to and retention of United States Person information.

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

Role Security. Roles are assigned and verified within the account management process. Nomination, registration, validation, and account update procedures ensure that HSIN Database user roles are verified as accurate. These roles define access to information based upon its sensitivity.

Rule Security. The rules associated with information access are defined by the laws and regulatory policies that govern the release of information. These laws/policies are identified within stated limitations in Memoranda of Understanding as well as in limitations built into the database technology. The Memoranda of Understanding will generally include limitations on public release of information, requirements for coordination prior to use of information from other source agencies, and the general "ownership custody and control" of information found within the database. The database technology further safeguards sensitive database information by ensuring that information placed in particular fields or tables is only accessible by individuals based upon their validated roles.

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

Role-Based Access Safeguards. The HSIN Database technology will safeguard information by limiting a user's ability to view or update particular fields of information based upon the user's role. The HSIN registration system currently groups those users into five roles as follows; 1) Law Enforcement, 2) Intelligence Community, 3) Federal government non-law enforcement, 4) State/Municipal/Tribal government non-law enforcement, and 5) Private Sector. Those roles were defined based upon the sensitivities associated with the information.

Auditing Measures. Whenever data is entered, updated, or viewed a record of that activity is captured and maintained within the system and can be retrieved based upon the user or the record.

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

Currently, all HSOC personnel reviewing material being submitted to the HSIN Database must review the HSOC's U.S. Person Privacy Guidelines prior to operating the system. Those

guidelines as well as other information handling requirements are being incorporated into computer-based training modules that will be required for HSIN Database access. The business rules associated with the protection of the information, and the basis for those rules will be a component of all computer based training modules associated with HSIN and the HSIN Database.

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

The HSIN Authorization to Operate was granted on July 21, 2005, for a period of one year. The HSOC Information Security Officer (ISO) is coordinating efforts and preparing for the re-certification and accreditation of HSIN and the HSIN Database in advance of the June 1, 2006 expiration of the current authorization. The HSIN Database is and will continue to evolve in accordance with FISMA and the DISA assessment guidance.

Section 9.0 Technology

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

Both HSIN and the HSIN Database applications were developed from the ground up under a government contract vehicle. They were built upon specific previously accredited commercial-off-the-shelf (COTs) software applications. Those COTs applications are Microsoft Windows Server 2003™ and SQL Server 2000™.

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

System developers of the Homeland Security Information Network recognized from the beginning the need to ensure the integrity, privacy, and security of the sensitive information to be collected, used and disseminated in the HSIN Database. Initial decisions about system design were therefore based on the need to ensure data integrity, embed strong privacy controls, and implement robust security features. HSIN also developed policies requiring role-based access controls and auditing procedures to facilitate oversight of system operations. These policies are dynamic and will be modified when improvements are identified that will increase the integrity, privacy and security of the system.

9.3 What design choices were made to enhance privacy?

Role-based access system design choices. The HSIN Registration system software development is now government-off-the-shelf (GOTs) software named the Account Management System (AMS). It was built specifically to address the need to ensure and enforce role-based access controls for the sensitive data in the HSIN Database as well as throughout the HSIN network. The design decision to use AMS was made to ensure privacy protections would be supported in the

HSIN Database. The application of the HSIN Registration software to the HSIN Database ensures that only those with access that is authorized by law and policy are permitted access to sensitive data including personal information. This design choice evidenced the Department's commitment to fully accomplish its homeland security information sharing missions while also fully protecting the privacy, commercial proprietary, and law enforcement sensitivities associated with the information being communicated.

Perimeter-based network security design choices. Per the HSIN and HSIN Database contract requirements; network firewalls, intrusion detection systems (IDS), and secure internet communication (secure socket layer or SSL) were selected for the HSIN and HSIN Database. These design choices were made in light of government and industry-wide best practices to ensure system integrity and enhance privacy for public-facing web-based systems.

Component selection design choices. The selection of industry-standard products with proven track records and globally available support mechanisms were determined to be a key design factor in our efforts to ensure privacy and data security requirements would be met. The selection of such products provides benefits such as automated patch management, privacy and security update notification, and robust dedicated support and security staffs.

Conclusion

The HSOC 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, the HSOC 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. HSIN fulfills those requirements for the HSOC as well as a host of communities with similar requirements.

HSIN was deployed as an internet-based platform to ensure compatibility and interoperability among interrelated communities of users securely exchanging critical sensitive information relevant to their official domestic security missions while ensuring that the integrity and privacy of individual's data was maintained. The registration protocol for HSIN was identified as a critical function for ensuring that HSIN members are properly validated. It serves as a key component in role-based access to the HSIN Database.

The HSOC and other similar domestic security stakeholders will accomplish their vital information sharing missions when the scope of their information intake and retention is focused on information that is relevant to their mission. In order to accomplish that, all suspicious activity information received is logged for accountability, filtered to ensure that it is terrorism-related information, and is tracked for operational significance and appropriate information sharing. While appropriately safeguarding the privacy of individual information, the HSIN Database

supports the information gathering process by enabling a host of authorized state and Federal law enforcement, governmental, and private sector users to communicate and collaborate regarding suspicious activities and incidents that pose a threat to critical infrastructure and domestic security. The architects of the HSIN Database defined a database concept predicated on limiting access to particular fields of sensitive information rather than on limiting access to the database itself. We will continue to track developments in policy and technology that can be applied to improve the data integrity, privacy, and security of the HSOC and HSIN Database systems.