Privacy Impact Assessment
for the

HSIN-Intelligence Portal

January 31, 2008

Contact Points
(b)(6)
Program Manager
Office of Intelligence and Analysis
(b)(6)

(b)(6)
CIO / Deputy Director, Information Sharing and Knowledge Management Division
Office of Intelligence and Analysis
(b)(6)

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

Abstract

The Office of Intelligence and Analysis (I&A) in the Department of Homeland Security (DHS) is implementing the Homeland Security Information Network-Intelligence Portal. The Portal is designed to foster information sharing, specifically with state, local, tribal, and private sector stakeholders. I&A has conducted this PIA because the portal may be used to communicate personally identifiable information (PII).

Introduction

The Department of Homeland Security, Office of Intelligence and Analysis (I&A), as the departmental lead component for communicating and collaborating with internal and external stakeholders on intelligence matters, has implemented the Homeland Security Information Network (HSIN)-Intelligence secure extranet portal, hereafter referred to as HSIN-Intelligence. The platform is used to share intelligence at the controlled, unclassified information (CUI) [1] level specifically with state, local, tribal, and private sector (SLTP) customers, and federal and international partners. The system also supports the sharing (collaboration) of intelligence within the DHS Intelligence Enterprise[2]. I&A has conducted this privacy impact assessment because of the collection of personally identifiable information (PII) during the user registration process and the sharing of PII among users within the HSIN-Intelligence platform.

Description

HSIN-Intelligence is the centralized mechanism for the DHS Office of Intelligence and Analysis to post and share intelligence information relating to the security of the homeland and the mission of the Department with other intelligence analysts at the Federal, State and Local levels. The security and functionality features implemented to support the mission requirements ensure:

- Appropriate security for exchanging sensitive intelligence information.
- Discretionary access to intelligence information.
- Information view capabilities managed by individual user and organizational roles
- A secure, single-access point to intelligence data which authorized stakeholders may access from anywhere at any time.
- Trust-enhancing functionality [redacted] (b)(2) High [redacted]

[1] Controlled Unclassified Information (CUI) is the emerging term across the federal government to encompass all unclassified information that needs to be protected.

[2] The "DHS Intelligence Enterprise" includes all those component organizations within the Department that have activities producing raw information, intelligence-related information, and/or finished intelligence.

The implementation of this platform will involve multiple phases. Currently, implementation has entered Phase One. (b)(2) High If this were to occur, such phases would be preceded by a revision to this privacy impact assessment.

The primary mission-driven platform configuration model is to divide the capability into two conceptually, and technically, separate areas:

- HSIN-Intelligence (General): This is the central hub for HSIN-Intelligence. (b)(2) High Management of the I&A content provided will be overseen by the I&A Production Management (PM) Division. (b)(2) High Subsequent and follow-on phases of implementation will address the potential need for policies and governance (b)(2) High Modification of this PIA to support those added capabilities will be addressed appropriately.
- HS SLIC Compartment: This refers to the restricted access area self-contained within the larger HSIN-Intelligence hub. It is designed specifically for targeted dissemination to and collaboration among authorized end-users within the Homeland Security – State and Local Community of Interest (HS–SLIC). (b)(2) High which is intended to enable participants to collaborate on the assessment of raw intelligence data and other relevant reporting, as well as the development of joint or collaborative products, that may contain the personally-identifiable information (PII) of U. S. Persons,[5] including U.S. Citizens and other Legal Permanent Residents of the United States.

Typical Transactions on HSIN-Intelligence

HSIN-Intelligence serves as a hub through which authorized users may receive appropriately sanitized and properly vetted intelligence products or reporting disseminated by I&A, and otherwise reach the I&A-provided internal collaboration spaces, including, when appropriate, the restricted HS SLIC Compartment. Users with general authorized access to only the HSIN-Intelligence hub would access basic intelligence related information, intelligence reports and other collaborative efforts that have either been sanitized to exclude or, by rule, will not include in the first instance, any PII. Certain authorized users would, (b)(2) High access the "restricted" HS SLIC compartment for

[3] Intelligence Oversight is the process of ensuring that all intelligence, counterintelligence, and intelligence related activities are conducted in accordance with applicable U.S. law, Presidential Executive Orders, and DHS Management Directives and policies (b)(2) High

[5] The definition of a U.S. Person includes a U.S. citizen, an alien known to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S. (except for a corporation directed and controlled by a foreign government).

viewing, and posting, and collaborating on intelligence products provided by, or for other authorized members of the HS SLIC.

To illustrate, when an authorized State or local agency end-user logs into the HSIN Intelligence portal, (b)(2) High

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

Information collected includes the following:

- Intelligence, law enforcement, and other information lawfully acquired and initially provided by a federal, state, local, or tribal government agency, or the private sector, to an authorized HSIN Intelligence participant, that is relevant to one of the specific functions of I&A in the context of the broad mission and associated responsibilities of the Department, including but not limited to the prevention of terrorism; the responsibilities of legacy agencies and entities originally transferred to the Department, including those responsibilities unrelated to terrorism; the preparation, response and recovery from natural and manmade crises and disasters; and ensuring that civil rights, civil liberties, and the overall economic security of the United States are not diminished by homeland security efforts.

This information may include the PII of specific U.S. Persons, such as name, date of birth, nationality, place of birth, or some other specific PII. However, such PII shall be made visible within HSIN Intelligence, if at all, only to and by authorized members of the HS SLIC, within the restricted HS SLIC compartment, in accordance with all applicable procedures or guidelines on the collection, use, retention, and dissemination of PII, and only when necessary and relevant to the purpose for which it is to be maintained and shared within HS SLIC. While much information otherwise collected into and contained within the HSIN Intelligence portal is either derived from or, as in the case of a finished intelligence product or report re-posted from elsewhere into HSIN Intelligence, would have originally contained PII of

specific U.S. Persons, it is the policy of HSIN Intelligence that no such PII shall be visible in any intelligence, law enforcement, or other information product or report posted into the general access areas of HSIN Intelligence.

(b)(2) High

User registration information is also collected from nominated and approved HSIN-Intelligence end users, including those specifically nominated and approved for access within the restricted HS SLIC compartment. (b)(2) High

Separate to the technical platform, (b)(2) High

With respect to information providers and users within the HS SLIC compartment, such collected information will also (b)(2) High

1.2 From whom is information collected?

Information collected is obtained from federal, state, local, or tribal government organizations, including law enforcement agencies, participating in HSIN Intelligence. This information may include relevant information originally collected by any one of these participating organizations, consistent with their respective missions and authorities to do so, as well as by foreign government organizations and the private sector.

Registration Information: (b)(2) High

1.3 Why is the information being collected?

HSIN-Intelligence enables authorized end users to access, receive, analyze, and, where appropriate, disseminate relevant intelligence, law enforcement, and other information, on behalf of their represented agencies, and in accordance with all applicable laws, regulations, and guidelines. The collection of this information into HSIN Intelligence enables participating agencies at the federal, state, local, tribal, and local level to assess the information in the context of their individual agency missions and responsibilities, and to make informed decisions concerning rapidly evolving threats to homeland security by using the best data available.

Registration Information: (b)(2) High

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

Among the legal authorities, arrangements and agreements that define the information collection are:

- **The Homeland Security Act of 2002** (Title II – Information Analysis and Infrastructure Protection, as amended): Authorizes DHS, among other things, through the Under Secretary for I&A and Chief Intelligence Officer of the Department (collectively, I&A),: (1) to access, receive and analyze law enforcement information, intelligence information, and other information from agencies of the federal government, state and local government agencies (including law enforcement agencies), and the private sector, and to integrate such information to aid primarily in the collection, analysis, and sharing of terrorism information and related threats to the homeland; (2) to integrate relevant information in order to identify priorities for protective and support measures (including those unrelated to the prevention of terrorism) by the Department, other agencies of the federal government, state and local governments agencies and authorities, the private sector, and other entities; (3) to provide intelligence and information analysis support to other elements of DHS engaged in authorized DHS missions (including those unrelated to the prevention of terrorism); and (4) to perform such responsibilities as directed by the Secretary in furtherance of an authorized mission of DHS, as derived from statutory, regulatory, and executive authorities. Also authorizes I&A:
    - to consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, and other elements of the federal government, as well as with state and local governments and private sector entities, as appropriate, to establish priorities and strategies for the collection of relevant information, and to ensure that appropriate exchanges of that information are occurring;
    - to request additional information from other federal agencies, state and local governments, and the private sector, relating to threats of terrorism or relating to other areas of responsibility assigned by the Secretary; and
    - to establish and utilize a secure communications and information technology infrastructure, in order to access, receive, analyze, and disseminate data and information acquired by the Department, in furtherance of I&A's responsibilities therein, and to ensure information contained therein is treated in a manner which complies with applicable federal law on privacy.
- **Executive Order 12333, as amended,** recognizes I&A as a member of the National Intelligence Community (IC), and authorizes all agencies within the IC, in accordance with applicable law and other guidance, to collect information needed by the President and other Executive Branch officials for the performance of their duties and responsibilities, including but not limited to information concerning international terrorist and narcotics activities, and other hostile activities directed against the U.S. by foreign powers, persons, organizations, and their agents; and to produce and disseminate intelligence. The Order also authorizes IC agencies to collect, retain, and disseminate such information and intelligence which concerns specific and identifiable U.S. Persons, but only

in accordance with subsequently issued procedures that are both consistent with the authorities provided in law and this Order, and limited to specific types or categories of U.S. Persons information.

  - This Order also authorizes IC agencies to cooperate and participate in law enforcement activities, unless otherwise precluded by law or this Order, related to counterintelligence, counterterrorism, or international counternarcotics investigations, as appropriate, and to otherwise provide, with the approval of the agency General Counsel, expert assistance, including, but only where lives are endangered, in support of local law enforcement agencies.

- **The Homeland Security Presidential Directive (HSPD-5)(February 28, 2003)** designates the Secretary of Homeland Security as the principal federal official for domestic incident management, and facilitates pertinent information sharing between the Department of Homeland Security and other agencies.

- **Homeland Security Presidential Directive 7 (HSPD-7)(2003**) orders the Secretary of Homeland Security to establish appropriate systems and mechanisms for sharing relevant homeland security information within and among the various sectors, and with those agencies and organizations primarily responsible for coordinating the protection of, our nation's critical infrastructure and key natural resources.

- **The Intelligence Reform and Terrorism Prevention Act (IRTPA)(2004), as amended,** directs the establishment of an information sharing environment, or ISE, to facilitate the sharing of terrorism, including pertinent law enforcement, weapons of mass destruction-related, and homeland security information among all appropriate Federal, state, local, and tribal entities, and the private sector, utilizing, among other things, existing systems and networks, and incorporating mechanisms (e.g., audits, authentication, access controls) for protecting the security of the information and individual's privacy and civil liberties. While the IRTPA created a government-wide program for sharing information in the ISE, it specifically preserved within DHS its existing authorities with regard to the exchange, use and dissemination of information to state, local, and private entities.

- **The Privacy Act of 1974** outlines the notice, use, access, and disclosure procedures which govern the I&A system of records within which HSIN Intelligence, and the specific intelligence and other user-related registration information containing covered PII contained therein, is maintained.

1.5 Privacy Impact Analysis

I&A posts intelligence information products and other related reporting products which contain visible PII only to those discrete restricted-access areas of the HS SLIC compartment within HSIN Intelligence where content and access management of the information in that area is either controlled exclusively by I&A or, when such control belongs to another HS SLIC member organization, where I&A has in advance determined specifically that the release of PII to that organization is authorized and otherwise consistent with I&A's obligations and procedures concerning the treatment and handling of U.S. Persons information, as discussed further below in this section. Similarly, other participating HS SLIC member

organizations post information, including that which may contain PII, into those areas of the HS SLIC compartment where content and access management of the information in that area is either controlled exclusively by that organization or, when such control belongs to another HS SLIC member organization, where that posting organization has in advance determined specifically that the release of PII into that organization's area is authorized and otherwise consistent with its own obligations and procedures concerning the treatment and handling of U.S. Persons information.

As discussed above, and consistent with the governing HS SLIC Charter, (b)(2) High [redacted]

All PII posted onto the HS SLIC compartment by I&A personnel, including the purpose for which it was collected into HSIN Intelligence and the manner in which it is maintained and shared with other agencies within the HS SLIC compartment, conforms to the requirements of the Privacy Act insofar as public notice of the collection, use, and maintenance of PII by I&A has been properly published, along with specific instructions for or claimed exemptions from, *see* 6 CFR Part 5, subpart B, Access and Amendment of Covered Records by Record Subjects.

Moreover, I&A, as a member of the National Intelligence Community, also conducts its mission in conformance with the requirements of Executive Order 12333, as amended, and has established procedures to govern the collection, retention, and dissemination of information concerning U.S. Persons in a manner which protects the privacy and constitutional rights of U.S. Persons. Specifically, I&A intelligence personnel may collect information which identifies a particular U.S. Person, retain it within and or disseminate it from I&A information sharing platforms such as HSIN Intelligence, as appropriate, only when it is determined that the PII is necessary for the conduct of I&A's authorized functions and otherwise falls into one of a limited number of categories which reflect the discrete types or activities of U.S. Persons for which information on such individuals would be utilized by the Department in the overall execution of its mission. Even where the collection and retention by I&A personnel of PII within HSIN Intelligence is appropriate under these procedures, there is nevertheless an additional requirement imposed whereby, prior to disseminating or making available any such PII outside of I&A, I&A personnel must also undertake a "minimization" process; that is, evaluating whether inclusion of the specific U.S. Person information or identity within that particular intelligence product or report, in the context of the intended recipient's need for the specific PII to understand or utilize the product, is necessary. Where disclosure of the actual PII is not necessary, the identity information must be "masked" by redacting or deleting it and replacing it with "a U.S. Person," "USPER", or some similar generic identifier. When an I&A product includes U.S. person identifying information, that PII must also be properly marked or tagged as "a U.S. Person" or "USPER," as appropriate, and the product or report itself must carry a warning stating that "This document contains U.S. Person Information and should be handled accordingly," or words to that effect.

I&A "Information Handling Guidelines" further complement the protections already afforded, respectively, by I&A's Privacy Act and Intelligence Oversight frameworks, described above, by explicitly prohibiting in all circumstances the collection and maintenance of U.S. persons information "solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights

secured by the Constitution or laws of the United States." These same guidelines also require I&A personnel to honor other restrictions/controls that may apply to information previously acquired by I&A, and which may limit or, in some cases, entirely prohibit, the use of certain information such as PII on platforms such as HSIN Intelligence. Such restrictions might include, as appropriate, classified or other sensitive information controls, statutory restrictions on the use of certain data, and 3rd party controls (e.g., ORCON, 3rd Agency Rule, Trusted Agents, etc.).

Other participating HS SLIC member organizations post information, including that which may contain PII, into those areas of the HS SLIC compartment where content and access management of the information in that area is controlled exclusively by that organization. Similar to the obligations of I&A personnel to protect information concerning U.S. Persons, State and Local HS SLIC members, whose users post intelligence and related reports into the HS SLIC compartment, have also agreed, as a condition both to participation within HS SLIC and access to relevant information containing PII, to be bound by the obligations and requirements concerning the treatment of PII applicable within "Criminal Intelligence Systems," pursuant 28 CFR Part 23. This imposes upon them obligations to protect the privacy interests of the subjects and potential subjects of these activities. These protections are achieved by requiring, among other things, that law enforcement intelligence information which identifies an individual be collected, retained, and disseminated only when there is reasonable suspicion that the individual identified is involved in criminal conduct and the information is relevant to that conduct or activity.

Furthermore, while each State and Local member, as a matter of policy and business process within the HS SLIC compartment of HSIN Intelligence, retains originator control over its own postings and is individually responsible for its users' compliance with the requirements of 28 CFR Part 23, as well as all other laws, regulations or directives which may apply uniquely or otherwise to that State or Locality's activities within HSIN Intelligence, appropriate I&A personnel may nevertheless review every HS SLIC user posting and, at their discretion, request minimization of any U.S. person identifying information contained therein where it is determined to be necessary in the interest of protecting the privacy and civil liberties of individuals.

Notwithstanding the implicit protections to privacy and civil liberties contained in the applicable frameworks described above, it is important to note also that the HS SLIC Steering Group regularly steers discussion and information posting activities occurring within the HS SLIC compartment to fit current issues and concerns of its member organizations, DHS, and the Intelligence Community. Thus, in most circumstances, user posted information must, in addition to complying with the policies, procedures, and guidelines described above, be relevant to issues and concerns specifically defined by the Steering Group.

Finally, significant technical safeguards have been implemented to further ensure the consistent and constant protection of PII. Primary among them, [redacted] This primary safeguard ensures that only those individuals actually nominated, verified and validated as authorized users are provided access to PII, as appropriate, at any time.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

I&A uses of HSIN Intelligence include:

(b)(3) High

[redacted]

Registration Information [redacted] (b)(2) High

[redacted]

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

[redacted] (b)(2) High

[redacted]

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

The information contained within HSIN-Intelligence will be provided by I&A and other authorized member organizations. Beyond those mechanisms actually in place, applied, or otherwise required by law, when the information was originally collected by the relevant agency, the information posted to HSIN Intelligence, including PII within the restricted spaces of the HS SLIC compartment, is not checked for accuracy, but assumed to be accurate as coming from a trusted system user and organization in the ordinary course [redacted (b)(2) High]

[redacted (b)(2) High]

[redacted]

2.4 Privacy Impact Analysis

The HSIN-Intelligence portal access and accountability controls, including those specifically designed for and implemented within the HS SLIC compartment where PII resides, are the primary guarantors of the accuracy, appropriate protection and integrity of the information stored within the system. As gatekeepers for determining who holds access and to what information, these rules and controls involve two basic components. The first of these are the technical limitations [redacted (b)(2) High] Secondly, users are administratively restricted from information that they are not authorized by policy or law, or otherwise permitted, to receive.

[redacted (b)(2) High]

Registration Information: [redacted (b)(2) High]

Any user found to be falsely making such a certification will be immediately denied continued access to the portal, referred to the appropriate law enforcement or other entity responsible for investigating such misconduct, and the matter will also be referred to the user's parent and/or sponsoring organization for consideration of any additional disciplinary or other legal actions that may be taken against that individual.

Section 3.0 Retention

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

I&A maintained data contained within HSIN-Intelligence, including any PII of U.S. persons contained within the HS SLIC compartment, is retained for periods of time in accordance with applicable law, regulation, and other directives or guidance, including relevant provisions of the Federal Records Act, and specifically with respect to PII, those rules and procedures for the retention of such information required under Executive Order 12333, and as implemented through DHS Memorandum, *Intelligence Oversight Basics*, dated March 27, 2006, discussed more fully in section 1.5, above, which requires review of U.S. person information placed into I&A's records system, including relevant portions of HSIN Intelligence, on a periodic[6] basis to see if the PII itself is still needed and otherwise meets the standards for its original collection, also discussed above. If not, the PII will be deleted from the record. Under these rules, the obligation to review and assess PII in I&A controlled records for continued retention belongs to each employee, contractor or other official assigned to I&A, or over whom it is determined that I&A policies and procedures concerning the treatment of PII within HSIN Intelligence will apply, and who is responsible for posting the covered content.

Data maintained, and otherwise posted into restricted HS SLIC spaces where content management is exclusively controlled by HS SLIC member organizations other than I&A, is retained in accordance with whatever retention period the individual State or locality requires – to be clear, information posted into those restricted access areas of the HS SLIC compartment control over which belongs exclusively to organizations other than I&A or other federal agency participants are not considered federal records. This is so, notwithstanding the fact that I&A or another member organization is provided access to that particular space for purposes of viewing and assessing the content.

Registration Information: [redacted] (b)(2) High [redacted]

[6] At a minimum, PII is to be reviewed annually to determine the need and authority for continued retention.

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

No, a records retention schedule currently has not been reviewed or approved by NARA. I&A is coordinating separately a records retention schedule for approval in parallel to this HSIN-Intelligence project. I&A, as the system owner, will default to retaining all records indefinitely (or five years in accordance with 28CFR, Part 23) until such time that the retention schedule has been approved and implemented within I&A.

3.3 Privacy Impact Analysis

The retention rules concerning information within HSIN Intelligence generally, and specifically those concerning PII posted and maintained within I&A controlled HS SLIC spaces which require, among other things, annual reviews of PII and deletion when no longer needed or permissible to retain under applicable guidelines and procedures, help to mitigate significantly the risk that personally identifiable information will be retained any longer than actually needed.

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 which internal organizations is the information shared?

Information is generally shared with any DHS component with an intelligence element (e.g., CBP, ICE, I&A, TSA, Coast Guard, etc.), and any other DHS component where the information is relevant to the performance of an official function. Since DHS intelligence information sharing and collaboration is the purpose of the HSIN-Intelligence system, and because DHS policies require the sharing of certain information in the possession of any one DHS organization – including I&A – with any other DHS organization, those DHS employees who are otherwise eligible and have validated user accounts can access information within HSIN Intelligence in accordance with applicable HSIN Intelligence rules and procedures. This internal access specifically includes access to information by both law enforcement and non-law enforcement organizations within DHS for purposes consistent with the authorized functions of those DHS organizations and personnel, and the DHS mission.

Registration Information: User registration information is not shared outside of HSIN-Intelligence or, for the HS SLIC portions, outside of the respective HS SLIC community.

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

Any information within HSIN Intelligence capable of being collected by I&A may be generally shared with any other DHS component where the information is relevant to the performance of an official function which belongs by statute or other authority to that DHS component, appropriate information security safeguards exist and are in place (e.g., system eligibility and access by the component user), and

the sharing is not itself otherwise prohibited by law. Since the scope of I&A's intelligence information sharing mission is consistent with that of the mission of DHS and all of its constituent components, the information shared with those components does not, generally speaking, differ from the type of information already described in 1.1.

4.3 How is the information transmitted or disclosed?

Authorized users with specifically assigned rights and attributes are able to access HSIN-Intelligence spaces, including, as appropriate, the restricted HS SLIC compartment, directly over an unclassified web-based (i.e., remote) secure network interface.

4.4 Privacy Impact Analysis

All HS SLIC members who access PII via the HSIN-Intelligence system must (inclusive):

- Be a full-time, current employee (government or contractor personnel) of a law enforcement, criminal justice, or homeland security Federal, State, Territorial and Protectorate, Tribal, or local government agency engaged in seeking to detect, defeat, or deter terrorist acts and thereby engaged in law enforcement activities for purposes of 28 C.F.R. Part 23; exceptions to full-time status must be approved by both the respective State HS SLIC point of contact and the DHS HS SLIC PM;

- Be a U.S. Citizen;

- Be currently employed in homeland security information and intelligence analysis functions for that government agency, as verified by (1) the DHS HS SLIC PM or their Government supervisor for federal employees, or (2) the respective State, Territory, or Urban Area HS SLIC point of contact or their designee for State and local intelligence employees;

- For State and Local members, be formally associated — either via management chain of command, Memorandum of Understanding, or some other formal mechanism — with a State and Local Fusion Center, or centralized intelligence fusion capability in the absence of a center, recognized as such by the HS SLIC Steering Group Voting Member appointed by the respective Homeland Security Advisor;

- Accept a HS SLIC user agreement that includes, to specifically include a third party non-disclosure agreement; any HS SLIC End User violating this user agreement shall have their access to the HS SLIC terminated on an immediate basis; and

- Have a government email address (or other email address approved by the State, Territory, or Urban Area POC and the HS SLIC PM).

In addition, each participating State, Territorial, or Urban Area HS SLIC Sponsoring Organizational representative is required to:

- Verify the HS SLIC eligibility status of sponsored employees (including contractors) on an annual basis, ensuring that each employee they sponsor (1) meets the eligibility requirements and (2) uses the system within these rules; and

- Maintain the user roster for the organization, and remove from the system any sponsored employee no longer eligible.

Finally, each HS SLIC member must:

- Be part of a single Sponsoring Organization approved by the associated Voting Member;
- Revalidate their position, title, and email address at least annually; and
- Change their system password and agree to user rights and responsibilities every 90 days or their access will be terminated.

The HS SLIC mitigates privacy risks caused by inappropriate access and/or sharing by limiting who has access to PII and defining proper use of system information. (b)(2) High This ensures internal and external access to the HS SLIC restricted portion of HSIN-Intelligence is tightly controlled. Coupled with usage restrictions detailed in Section 2.0 and Section 8.0, this ensures that risks associated with internal sharing are mitigated as much as possible.

Internal and external sharing is governed by these same access, control, and accountability procedures.

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 which external organizations is the information shared?

As of January 3, 2008, those external organizations who are members of the HS SLIC and have sponsored user accounts for eligible personnel to access the HS SLIC compartment include:

39 States:

Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, New Hampshire, New Jersey, New Mexico, New York, Ohio, Oregon, Rhode Island, South Carolina, Tennessee, Texas , Vermont, Virginia, Washington, West Virginia, Wisconsin

Federal Agencies:

DOJ, Drug Enforcement Administration
Department of Interior
Federal Bureau of Intelligence, National Security Branch
Office of Director of National Intelligence, Program Manager-Information Sharing Environment
Department of Defense, Northern Command

All users granted access to the HS SLIC compartment, who are employed by any organization (to include all listed above,) have been granted access through the eligibility criteria described in Section 4.4 above, and have accepted to be bound by the handling restrictions, HS SLIC governance policies and laws of their jurisdictions.

Users granted access to the HSIN-Intelligence (General) areas are granted via policies determined by the I&A Production Management Division for intelligence dissemination products that do not contain PII.

All HSIN-Intelligence information is stored in virtual spaces accessible only through the HSIN Intelligence portal. Individual users will be able to send external emails and alerts to other users from within the system, though emails or alerts originating on the system are retained in the system.

Registration Information: User information is contained in a global directory. Users may alter their information themselves, within the portal.

5.2 What information is shared and for what purpose?

Homeland security-related law enforcement, intelligence, and other information from federal, State and local government agencies (including but not limited to terrorism and related threat reporting, assessments of suspicious activity reports, and other reports or exchanges concerning activities that users consider germane to the homeland security mission) is shared among and between the external organizations listed above in order to enable those organizations to identify criminal and other related activities associated with terrorist actions, planning, or preparations. (b)(2) High [redacted]

5.3 How is the information transmitted or disclosed?

Authorized users with specifically assigned rights and attributes are able to access HSIN-Intelligence spaces, including, as appropriate, the restricted HS SLIC compartment, (b)(2) High [redacted]

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?

Individual HSIN-Intelligence users, including and especially those end users with access to restricted spaces within the HS SLIC compartment, must read, acknowledge, and comply with an End User Agreement that references and incorporates their obligations to comply with the laws and policies associated with their sponsoring organization, the jurisdictions in which they operate, and that of the overall HSIN Intelligence program, as applicable. In addition, and in order to enter any spaces within the HSIN-Intelligence portal, users must acknowledge an on screen system use agreement.

All organizations that are eligible and vetted for membership into the HS SLIC, in coordination with their applicable sponsoring organizations and approval authorities are initially bound, as a condition of membership, by the policies, rules and processes outlined in the HS SLIC Charter. In addition, all HS SLIC end users, as a condition of their participation in and access to the HS SLIC compartment of HSIN-Intelligence, operate under a firm "no third party dissemination without explicit authorization" handling rule – that is, each HS SLIC user organization that posts information on HS SLIC retains the right to restrict further dissemination by any other HS SLIC member to whom access has already been granted, unless and until the original provider of the information explicitly permits further dissemination to any non-HS SLIC (3rd Party) entity.

5.5 How is the shared information secured by the recipient?

HSIN-Intelligence [redacted (b)(2) High] Once accessed, data available to the recipient is subject to the recipient's obligation to comply with the laws and policies of their respective agency/organization and applicable jurisdiction as well as the laws and policies associated with intelligence information and the HSIN-Intelligence system rules of conduct. The HSIN-Intelligence system complies with all appropriate DHS security policies. In addition, [redacted (b)(2) High]

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

The following training will be provided to users of this system:

- User Technical Training: The HSIN-Intelligence secure portal service vendor offers each of the users training on how to use the system. Training will be given at both HS SLIC user locations as well as through system-based training accessible from the system itself. Under section 201(d)(16) of the Homeland Security Act, DHS has a statutory responsibility "to coordinate training and other support to the elements and personnel of the Department, other agencies of the federal government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department."

- User Legal/Regulatory Training for HS SLIC: HS SLIC users granted access to PII receive formal vetting prior to physical access, and then receive training regarding the legal/regulatory predicate authorizing access to the data as also described in Section 2.4 above. DHS I&A members are subject to Intelligence Oversight training as well as other Privacy related training over the course of their assignment to the position. A majority of the HS SLIC members are State and Local authorities (or sworn Law Enforcement officers) who are bound to comply with 28 CFR Part 23, and receive the appropriate privacy training to properly conduct their duties.

5.7 Privacy Impact Analysis

HSIN-Intelligence mitigates privacy risks caused by inappropriate external access and/or sharing by prohibiting the use of PII except in certain areas of the platform, limiting who has access to HSIN-Intelligence generally, and specifically with respect to those restricted areas of the HSLIC compartment, and defining terms for the proper use of system information. This is particularly true for the HS SLIC compartment of HSIN-Intelligence, where all intelligence products containing U.S. person information or PII will reside. Through the auditing and technical measures of the system, the potential for misuse of data is minimized ((see section 8.6, below). The HSIN-Intelligence portal, in restricting the disclosure of sensitive PII information only to authorized HS SLIC members with the statutory responsibility and a mission need to know such information, further ensures the necessary privacy protections. These protections are further reinforced by the minimization process through which I&A, prior to dissemination within the HS SLIC compartment, assesses all information, including intelligence and other relevant products and reports, concerning U.S. Persons to determine whether disclosure of the PII is necessary in order for the recipients to otherwise understand and use the product or report.

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?

General notice to the public of information collected, maintained, used in, and disclosed from, all platforms within the collective records system within which I&A currently operates was published in the Federal Register on April 18, 2005, under the title "HSOC Database". The collection of information into HSIN Intelligence is covered by that SORN. Publication of notice for a new stand alone Privacy Act records system framework for I&A, including notice of exemptions to be claimed, is imminent. Among other things, this new I&A SORN will reflect the intervening reorganization of offices formerly within the DHS Information and Analysis and Infrastructure Protection Directorate, including both I&A and what had previously been known as the Homeland Security Operations Center, or HSOC (the conduit through which I&A and other IAIP offices had historically exchanged information with relevant stakeholders).

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

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

Information collected on individuals in support of an intelligence support mission does not include an opportunity for said individuals the right to decline the collection of this information. Information may be collected arbitrary of knowledge by the individual and the collection, retention, dissemination and

destruction of that information is bound by the laws, policies and regulations described further within this Privacy Impact Assessment.

User Registration Information [redacted] (b)(2) High [redacted] Additionally, authorized users may decline to provide intelligence information collected by their specific agency however the HS SLIC community strives to foster a level of trust among users, and choosing to withhold information has the potential to hinder and impact vital intelligence related collaboration.

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?

No. There does not exist a mechanism for individuals to consent or contest the uses of their personal information. The safeguards for the proper handling and protections of that information lie only within the laws, regulations and policies of the HSIN Intelligence user organization that collects the information.

6.4 Privacy Impact Analysis

General notice is provided through the published System of Records Notices, as required by the Privacy Act of 1974, and which govern the records systems within which information accessible through the HSIN Intelligence portal exist. Although individuals who may be the subject of or mentioned in a report or product may neither have been able to decline to provide information about themselves nor consent to certain uses when it was initially acquired, the HSIN-Intelligence portal mitigates privacy risk to individuals by controlling the nature of the information posted, the purposes for and manner in which it can be used and further shared, and access to it, so that only those individuals with a need-to-know that information in the performance of authorized functions, and subject to additional restrictions and limitations concerning access and use, are allowed to view it. Providing more robust notice than that discussed above would hinder the activities of the Department and its participating stakeholders in the conduct of intelligence and law enforcement investigations and other activities undertaken for the purposes of securing the homeland.

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?

Opportunities and instructions for individuals seeking access to information about them, and maintained by I&A within those restricted areas of the HSIN-Intelligence portal where PII may be present, are explained in provisions of the applicable Privacy Act System of Records Notice which covers that particular information. Additionally, any person may request access to any federal records maintained by I&A or any other federal agency through the Freedom of Information Act. The specific procedures for

submitting Privacy Act and FOIA requests for information maintained by I&A and accessible through the HSIN Intelligence portal are available in 6 C.F.R. Part 5.

Registration Information: (b)(2) High [redacted]

7.2 What are the procedures for correcting erroneous information?

Because personal information likely to be accessible through the HSIN-Intelligence portal, while not classified for national security purposes, includes or is based on highly sensitive intelligence or other threat reporting, no specific procedures have been established by the HSIN Intelligence program officials to allow for correction of this information. The System of Records Notice (SORN) that applies to this platform contains provisions that allow discretion in receiving PII correcting requests, if necessary. As a practice, as new information is obtained, old information accessible through HSIN-Intelligence will be updated or deleted. In addition, with respect to all information concerning U.S. Persons maintained by I&A, PII will be periodically reviewed by the poster of the information to determine if it is still needed, and if it is not, it will be removed.

State, local, and other government agency postings to the HS SLIC compartment of the HSIN-Intelligence are not maintained by I&A, nor considered to be I&A documents unless I&A chooses to re-post them into the I&A controlled spaces of the HS SLIC compartment, or in another location within I&A's system of records not accessible through the HSIN Intelligence portal. In those situations where PII is posted by a State, local, or other government organization, and into spaces whose content is under the management and control of that State, locality, or other government agency, individuals desiring to correct records which may identify them must contact that specific agency for more information on the procedures that may be available.

Registration Information: (b)(2) High [redacted]

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

The DHS FOIA page, available through the DHS public website, contains instructions for correcting information within DHS systems of records generally, but there are no specific provisions for correcting the highly sensitive law enforcement and related intelligence information in the HSIN-Intelligence system. Question 7.1 discusses the procedures for accessing information through the Privacy Act/FOIA process.

Registration Information: Upon completion of registration, users are informed of the correction procedures.

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

Basic access and correction procedures are discussed in Sections 7.1, 7.2, and 7.3 above.

7.5 Privacy Impact Analysis

During development of the HSIN-Intelligence information sharing platform, and the processes governing its use, significant consideration was given to the impact of erroneous data on individual record subjects, including official users of the information. Since most information within the restricted HS SLIC compartment of HSIN-Intelligence, where all PII resides (b)(2) High [redacted] Nevertheless, and given the sensitive nature of the information in HS SLIC and the intelligence missions it supports , (b)(2) High (b)(2) High and every effort is made to correct information and provide access to information in accordance with DHS guidance and other legal requirements, as applicable. (b)(2) High [redacted] This ensures accountability for information shared and made available to others within the HSIN-Intelligence platform.

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.)

HSIN-Intelligence has a separate Program Office that generally reviews portal content; this program office also manages the HS SLIC in its entirety, including overseeing the administration of the HS SLIC Steering Group and the technical portions of both the outer HSIN-Intelligence hub, as well as the restricted spaces of the HS SLIC compartment. As explained elsewhere, all users with access only to the outer HSIN-Intelligence hub will have similar access to all communication and collaboration tools accessible and functional capabilities within that general area. Users with access to the inner HS SLIC compartment will have such access to all communication and collaboration tools and functionality as are specifically made available to them, in accordance with any additional rules, permissions, or restrictions that may apply, therein.

All HS SLIC end users who are provided access to PII via the restricted HS SLIC compartment of HSIN-Intelligence must (inclusive):

- Be a full-time, current employee (government or contractor personnel) of a law enforcement, criminal justice, or homeland security Federal, State, Territorial and Protectorate, Tribal, or local government agency engaged in seeking to detect, defeat, or deter terrorist acts and thereby engaged in law enforcement activities for purposes of 28 C.F.R. Part 23; exceptions to full-time status must be approved by both the respective State HS SLIC point of contact and the DHS HS SLIC PM;

- Be a U.S. Citizen;

- Be currently employed in homeland security information and intelligence analysis functions for that government agency, as verified by (1) the DHS HS SLIC PM or their Government supervisor for federal employees, or (2) the respective State, Territory, or Urban Area HS SLIC point of contact or their designee for State and local intelligence employees;

- For State and Local members, be formally associated — either via management chain of command, Memorandum of Understanding, or some other formal mechanism — with a State and Local Fusion Center, or centralized intelligence fusion capability in the absence of a center, recognized as such by the HS SLIC Steering Group Voting Member appointed by the respective Homeland Security Advisor;

- Accept a HS SLIC user agreement that includes, to specifically include a third party non-disclosure agreement; any HS SLIC End User violating this user agreement shall have their access to the HS SLIC terminated on an immediate basis; and

- Have a government email address (or other email address approved by the State, Territory, or Urban Area POC and the HS SLIC PM).

In addition, each participating State, Territorial, or Urban Area HS SLIC Sponsoring Organizational representative is required to:

Verify the HS SLIC eligibility status of sponsored employees (including contractors) on an annual basis, ensuring that each employee they sponsor (1) meets the eligibility requirements and (2) uses the system within these rules; and

Maintain the user roster for the organization, and remove from the system any sponsored employee no longer eligible.

Finally, each HS SLIC member must

- Be part of a single Sponsoring Organization approved by the associated Voting Member;

- Revalidate their position, title, and email address at least annually; and

- Change their system password and agree to user rights and responsibilities every 90 days or their access will be terminated.

8.2 Will contractors to DHS have access to the system?

Yes. Both the HSIN-Intelligence portal and, within it, the HS SLIC compartment, is administered by a mix of both I&A government officers and contractors and all contractor work is overseen by DHS contracting officers and assigned I&A government staff. The number of contractors is minimized to only those needed. I&A contractors, specifically, may be utilized in a role to support directly the analytical intelligence functions and activities for which this platform serves, and/or may support directly the management/administration of the platform in support of the HSIN-Intelligence system in general or directly for the HS SLIC. In addition, 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 information technology professionals are registered and managed using the same auditing and controls as every other HSIN-Intelligence user. All contractors are required by contract provisions to sign non-disclosure agreements, and while serving in any role are bound by the same policies, laws, rules, and obligations that apply for any other individuals that have been vetted and authorized access to the platform in addition to the limitations included or contained within the contract or Statement of Work that applies.

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

[redacted] (b)(2) High [redacted]

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

[redacted] (b)(2) High [redacted]

Sharing with foreign partners are a critical part of fulfilling our mission of defending the homeland. [redacted] (b)(2) High [redacted]

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

(b)(2) High

[redacted]

- [redacted]
- [redacted]
- [redacted]

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

(b)(2) High

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

(b)(2) High I&A does not include U.S. person information in this metadata.

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

All DHS personnel having access to HS SLIC must conduct their activities in accordance with the guidance provided in DHS memorandum, Intelligence Oversight Basics, dated March 27, 2006. The memorandum describes core concepts related to I&A's mission, and the collection, retention, and dissemination of information about U.S. persons. DHS users also have access to system training that includes discussion of privacy aspects of the system, including required I&A annual training on EO 12333. Non-DHS intelligence professionals within the HS SLIC, who are also employed elsewhere within the Intelligence Community, have similar requirements for intelligence oversight training in accordance with Executive Order 12333. State and local authorities have their own training programs that are used to teach staff how to comply with issued guidance (see above at 5.6).

8.8 Is the data secured in accordance with FISMA requirements? If

The Certification and Accreditation process is currently being conducted. An Authority to Operate is expected to be granted before January 31, 2008. The platform will not be utilized in operational form until that approval to operate is obtained.

8.9 Privacy Impact Analysis

Access to the portions of HSIN-Intelligence containing sensitive PII is controlled and protected by a number of technical, procedural, and policy-based safeguards, including, (b)(2) High Access is role-based, and eligibility is reviewed for accuracy. Auditing is used to monitor system use. Overall, these safeguards adequately protect against inappropriate access to and use of information in the system.

Auditing was a major portion of the need for an infrastructure solution separate from the legacy HSIN technology platform. Using the (b)(2) High technology, I&A will be able to perform its mission with a robust compliment of tools to maintain user access control and ensure appropriate conduct by users on the HSIN-Intelligence platform.

Section 9.0 Technology

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

HSIN-Intelligence was developed by (b)(2) High The majority of the system was base capability provided to all (b)(2) High customers. However, the I&A secure portal Statement of Work required the contractor to build additional features.

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

System developers of HSIN-Intelligence recognized from the beginning the need to ensure the integrity, privacy, and security of the sensitive information to be collected, used, and disseminated on the system. All decisions about system design were based on the need to ensure data integrity, embed strong privacy controls, and implement robust security features. (b)(2) High

9.3 What design choices were made to enhance privacy?

(b)(2) High, in order to bolster privacy protections, HSIN-Intelligence requires that a "minimization" process be employed whereby all reports, analyses, assessments, and other products, prior to dissemination by I&A (i.e., posted onto the HS SLIC compartment), are reviewed to assess and determine whether the specific U.S. person identity information is necessary for the use of or understanding of the product by the intended recipients. Thus, for documents disseminated by I&A within the HS SLIC where the U.S. Person information or identity is not necessary to understand the product, the identity information will be "masked" by removing and replacing it with "a U.S. Person," "USPER," or some similar marking, as appropriate. Where an I&A product on the HS SLIC will include U.S. person identifying information, the product itself will carry a warning stating that "This product contains U.S. Person Information" or words to that effect. This is done in accordance with I&A's Intelligence Oversight obligations and policies, and the I&A Information Handling Guidelines.

As discussed above, (b)(2) High technology was selected because it provides the program management staff the tools necessary for I&A to comply, not only with the Intelligence Community's oversight responsibilities uniquely applicable within HSIN Intelligence to I&A, but to facilitate compliance with the Privacy framework (e.g., 28 CFR Part 23) for any other organization with access to, including the capability to post and exchange its own information within, certain portions of the portal. This was a specific design choice made to enhance accountability surrounding the possible use of personally identifiable information in the HS SLIC portion of HSIN-Intelligence.

Conclusion

HSIN-Intelligence 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 also ensuring that the integrity and privacy of individuals' data was maintained consistent with their own applicable standards, laws, policies, and procedures. For the HS SLIC compartment of the portal, U.S. person identifying information is routinely minimized unless the information is required for understanding the specific intelligence report, analysis, assessment or other product. This significantly mitigates the privacy risks for information accessible through HSIN Intelligence. For those documents that do contain personally identifiable information, a number of safeguards are in place to protect the privacy and integrity of the information. The registration

protocol for HSIN-Intelligence is identified as a critical function for ensuring that members are properly validated; this is particularly true for HS SLIC compartment access, the only portion of HSIN Intelligence which contains PII. It serves as a key component in role-based access to HSIN-Intelligence and mitigates the risk of inappropriate access to information. Basic auditing capabilities are implemented in all areas of HSIN-Intelligence. I&A will continue to track developments in policy and technology that can be applied continually to improve the privacy and security of the system.

Responsible Officials

(b)(6)
Program Manager
Office of Intelligence and Analysis
(b)(6)

(b)(6)
CIO and Deputy Director for Information Sharing and Knowledge Management
Office of Intelligence and Analysis
(b)(6)

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security