Privacy Impact Assessment Update
for the

HSIN R3 User Accounts:

Manual Identity Proofing Process

DHS/OPS/PIA-008(a)

January 15, 2013

Contact Point
James Lanoue
DHS Operations
HSIN Program Management Office
(202) 282-9580

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Homeland Security Information Network (HSIN) is maintained by the Department of Homeland Security (DHS), Office of Operations Coordination and Planning (OPS). HSIN is a user-driven, web-based, information-sharing platform that connects all homeland security mission partners within a wide spectrum of homeland security mission areas. This Privacy Impact Assessment (PIA) Update is being conducted to document a new process for certain registrants who may need an alternative manual solution to the standard online, electronic identity proofing (IdP) process.

Overview

HSIN is a user-driven, web-based, information-sharing platform that connects homeland security mission partners, consisting of DHS and its federal, state, local, tribal, territorial, private sector, international, and other non-governmental partners within a wide spectrum of homeland security mission areas. DHS OPS maintains HSIN. HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector, international, and other non-governmental partners involved in identifying and preventing terrorism and in undertaking incident management activities. HSIN is designed to allow all relevant, vetted stakeholders access to the information regardless of jurisdictional, geographic, or agency boundaries, so long as it has been determined that the information is appropriate to be shared.

DHS mission partners rely on HSIN as an environment that promotes trust and sharing, and HSIN supports the DHS and Information Sharing Environment (ISE) missions by: (1) providing timely and accurate information related to detecting, preventing, responding to, and recovering from terrorist attacks and natural disasters; (2) providing timely and accurate information regarding vulnerabilities and threats, managing incidents to mitigate risks, and reducing post- incident loss of life and property; (3) providing near-real-time collaboration and incident management; (4) facilitating information exchange for emergency management response and recovery operations; and (5) connecting disparate information users in a dynamic and diverse information exchange environment.

The HSIN platform allows these diverse communities to work together to perform investigations, identify terrorist activities, respond to areas affected by natural disasters, and provide coordination during recovery operations.

Identity Proofing Service

When registering for a new account with HSIN, all registrants must undergo an identity authentication process. The identity authentication process uses a third-party Identity Proofing (IdP) service to generate knowledge-based questions based on commercial identity verification information collected by third-party companies from financial institutions, public records, and other service providers. The information accessed by the IdP may include information such as the individual’s commercial transaction history, mortgage payments, and past addresses. An individual must correctly answer the knowledge-based questions generated by the IdP in order to authenticate his or her identity and enable access to use HSIN.

In order to generate these knowledge-based questions, the IdP service collects basic personally identifiable information (PII) from the individual including name, address of residence, date of birth and, on an optional basis, the individual's Social Security number (SSN); however, the SSN will not be stored by the HSIN Program Management Office (PMO).[1] Each individual will be asked a minimum of two and a maximum of four knowledge-based questions. The identity authentication process uses a third-party Identity Proofing (IdP) service to generate knowledge-based questions based on commercial identity verification information collected by third-party companies from financial institutions, public records, and other service providers. The information accessed by the IdP may include information such as the individual's commercial transaction history, mortgage payments, and past addresses. If there is not enough data to generate at least two questions, (i.e., the person lacks sufficient information to generate an adequate number of questions), then the individual's identity cannot be authenticated and he or she will not be able to continue through HSIN online registration.

The fact that an individual was unable to use the IdP service will be sent to HSIN, but no other information. HSIN PMO will receive aggregate reports on such failure rates. The IdP will send a transaction number, the fact that knowledge-based questions could not be generated, and the date and time of the transaction. This information will allow HSIN PMO to gather statistics on how many individuals are unable to use the IdP service.

If there is sufficient information to generate two to four questions, the IdP service will evaluate the answers to the questions and return a pass/fail indicator to HSIN PMO. If the individual does not successfully answer the questions generated by the IdP, he or she will not be authenticated and he will not be able to continue through the HSIN online registration process. If and when the registrant fails identity authentication, the system will provide the registrant with a limited number of opportunities to retry identity proofing. Should these retry attempts also fail, the system will present the registrant with the appropriate help desk phone number to call, based on the reason code of their failure.

The IdP service will send a transaction number, the date and time of the transaction, and an error code to HSIN PMO. This information will facilitate troubleshooting and system management and improvement so that HSIN PMO can maintain statistics of how many individuals are unable to authenticate through the IdP service. All PII entered by the individual during the IdP session and any questions generated by the IdP are deleted at the end of the session.

If the individual is able to answer the questions correctly, his or her identity is authenticated, a pass indicator is returned to HSIN, and the individual will continue through the HSIN online registration process. The next steps include aligning the registrant's personal and professional attributes collected from the HSIN account request form to specific Communities of

[1] HSIN will require individuals to authenticate their identity through the IdP and providing a SSN enhances the ability of the IdP to generate knowledge-based questions.

Interest (COI) that support their job function. These immediately aforementioned steps are intended to automatically streamline and identify an applicable relationship between a registrant and COI(s). Once a recommended COI relationship has been identified, the validator of that COI will either reject or approve the registrant's membership in the COI. All COIs operate under customized charters and may have specific membership criteria that a registrant must meet to qualify for entry.

Reason for the PIA Update

After publication of the July 2012 PIA for HSIN User Accounts,[2] further system requirements determined that HSIN registrants who were unable to complete the electronic IdP process must undergo a manual IdP process. Therefore, a PIA update is required to document the privacy risks for the registrants who may need an alternative, manual solution to the online, electronic identity proofing (IdP) process. This PIA update covers the manual identity proofing process for new user account registration required for access to the HSIN Release 3 (R3).

The HSIN PMO has implemented strict identity authentication controls in order to verify a registrant's identity. As stated above, if the registrant does not successfully answer the questions generated by the IdP service provider, he or she will not be authenticated and will not be able to continue through the HSIN online registration process.

Manual Identity Validator (MIV)

Registrants who use the manual IdP due to one of the scenarios below will require a face-to-face meeting with a Manual Identity Validator (MIV). The MIV role operates as the primary point of contact during the manual IdP process. All MIVs will receive required training from the HSIN PMO in order to transact the necessary duties of identity verification and confirmation for qualified registrants. The MIV must have a homeland security supported mission and be an active HSIN user. The MIV role is intended to coordinate in-person meeting sessions with HSIN registrants to review required documentation and confirm registrant identity.

During the manual IdP process, the MIV will personally verify and validate the registrant's identity by reviewing at least one form of a government-issued photo ID. The MIV will then submit the manual IdP online form to the HSIN Security Office.

All MIVs will be recruited and trained by the HSIN Outreach and Security offices. MIVs will be identified as qualified validators, meaning they will be registered HSIN users with a valid Department of Homeland Security mission and COI membership. They will then be provided basic training in the reading of identity credentials by HSIN Outreach, as overseen and approved by HSIN Security. When a MIV completes training, an auditable record of the completion of training will be recorded in their user profile. Training of MIVs will be developed from DHS best practices leveraged from DHS components that routinely review identity credentials. HSIN

[2] For a detailed description of the HSIN user accounts registration and access processes, please see DHS/OPS/PIA-008 HSIN R3 User Accounts (July 25, 2012) available at http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_ops_hsin_r3useraccounts_07252012.pdf.

Outreach will review best practices from such components as DHS Immigrations and Customs Enforcement (ICE) and DHS U.S. Citizenship and Immigration Services (USCIS). Every time a MIV manually validates a new user, he or she will record this validation using an online form, checking a series of boxes that document his or her sign-off on the manually validated user (see Figure 1 manual IdP form below).

Manual IdP Scenarios

If and when a registrant fails identity authentication, the system will provide the registrant with a limited number of opportunities to retry identity proofing. Should these retry attempts also fail or should the registrant determine he or she prefers to use the manual IdP instead of the electronic IdP process, the HSIN PMO has developed three scenarios for a non-standard manual IdP process depending on the type HSIN registrant:

- Scenario (1) A HSIN registrant who has failed the online, electronic IdP process three times;
- Scenario (2) A HSIN registrant who has a time-sensitive, mission-critical role requiring timely admission to HSIN; and/or
- Scenario (3) An international registrant[3].

Scenario (1): A HSIN Registrant who has failed the online, electronic IdP process three times

This scenario is followed when a qualified registrant fails the online, automatic IdP three times.

After a third failed attempt to gain access through the online, electronic HSIN IdP process, the registrant will receive an on-screen error code preceding the IdP quiz. The registrant is asked to call the HSIN Help Desk to request additional guidance. The HSIN Help Desk representative cannot interpret the error code; however, he or she will be able to provide the registrant with contact information for a local MIV. The registrant has the option to contact the MIV to proceed with the manual IdP process requiring an in-person meeting. These error codes are provided by the IdP and are purposefully nebulous for the privacy protection of the registrant. If the registrant requires further information on why he or she failed the online, electronic IdP service, then he or she will be instructed to directly contact the HSIN Help Desk.

When the HSIN Help Desk representative grants the registrant privilege to process through the manual IdP process as a result of the three (3) failed online attempts, he or she will receive an email with a letter from the HSIN PMO. The HSIN Help Desk representative will provide the registrant with a list of local MIVs. The MIV will personally verify and validate the

[3] The registration process to admit an international user falls within the manual IdP category but is completely separate from the processes outlined in this document. It involves rigorous oversight by the HSIN Information System Security Manager (ISSM), or appointed alternate.

registrant's identity by reviewing at least one form of a government-issued photo ID. The MIV will then electronically submit the manual IdP online form to the HSIN Security Office.

The HSIN ISSM is the ultimate approving authority for processing the registrant into the system. Approximately 24 hours after the manual IdP form is received by the HSIN ISSM, or appointed alternate,[4] the registrant will receive either an acceptance or rejection email. If accepted, the system generates an email to the registrant with a link to complete the HSIN New User Registration Process. This process is the standard, online, electronic process all registrants complete after IdP and prior to gaining access to HSIN. The registrant's completed registration is automatically placed in the validation queue. The appropriate COI Validator will review the queue.

Scenario (2): A HSIN registrant who has a time-sensitive, mission-critical role requiring timely admission to HSIN

This scenario is followed when a HSIN registrant with a time-sensitive, mission-critical role requiring timely admission is requesting immediate HSIN access. In this case, a registrant must meet qualifying criteria as defined by the occurrence and participation in a major national response (Level 2 or Level 3) incident, a planned leadership role in a potential national response, and/or a statutorily- or directive- defined senior leadership role within DHS.

The mission critical registrant contacts the HSIN Help Desk requesting manual IdP processing instructions. The HSIN Help Desk representative will analyze and confirm or deny if the registrant meets the qualifying criteria outlined above to process through to manual IdP. If yes, the HSIN Help Desk representative provides the registrant with a list of local MIVs. The MIV will personally verify and validate the registrant's identity by reviewing at least one form of a government-issued photo ID. The MIV will then submit the manual IdP online form to the HSIN Security Office.

The HSIN ISSM is the ultimate approving authority for processing the registrant into the system. Approximately 24 hours after the manual IdP form is received by the HSIN ISSM, or appointed alternate, the registrant will receive either an acceptance or rejection email. If accepted, the system generates an email to the registrant with a link to complete the HSIN New User Registration Process. This process is the standard, online, electronic process all registrants complete prior to gaining access to HSIN. The registrant's completed registration is automatically placed in the validation queue. The appropriate COI Validator will review the queue.

Scenario (3): International registrant

This scenario is used to vet, validate, and admit a non- U.S. citizen registrant onto HSIN, generally referred to as "international registrants." The HSIN system will recognize, based upon a checked box in the initial, on-line IdP stages, that a registrant is not a U.S. citizen, and instruct

[4] The HSIN ISSM may appoint an alternate HSIN PMO staff representative to act in his capacity for approving, validating and/or rejecting registrants during the manual IdP process.

the registrant to directly contact the HSIN PMO to process through the adopted exception process. The DHS IT Security Program Exception to Citizenship Requirement Request Form will be used to submit exception requests to the HSIN Security Office for international registrant access to HSIN. The minimum information required to submit a HSIN exception request is:

- Name
- Date of Birth
- Place of Birth (City)
- Position
- Country of Citizenship
- Foreign Service National (If yes, attach “Security Certification” issued in accordance with 3 FAM 7220)
- Justification

Requests for one or more registrants may be submitted on a single form but all registrants on one form must have the same citizenship. A single justification may be used for all users on a request as appropriate. The form can only be sent via email and is not submitted through HSIN like the MIV process. The completed form will not be shared with the HSIN Mission Advocate.

HSIN Outreach will receive status notifications from the HSIN ISSM, or appointed alternate, and will update the “Current HSIN Non-U.S. Accounts and Approved (But Not yet Provisioned) Non-U.S. Personnel” spreadsheet for the HSIN Help Desk representatives to reference. Upon HSIN ISSM, or appointed alternate, approval, the registrant may proceed through to the New User Registration Process.

Privacy Impact Analysis

Each of the below sections consider how the system has changed and what impact those changes have on the fair information principles. In some cases there may be no impact and that is indicated.

The System and the Information Collected and Stored within the System

The HSIN Help Desk will collect basic contact information, including full name, email address, telephone number, directly from registrants applying for access to HSIN. This basic personally identifiable information will be transmitted from the HSIN Help Desk to the relevant MIV to facilitate the manual IdP process. Registrants will be required to show one form of government-issued identification to a HSIN certified MIV to confirm identity. The type of government-issued identification and year of expiration will be captured on the form submitted to the HSIN Security Office.

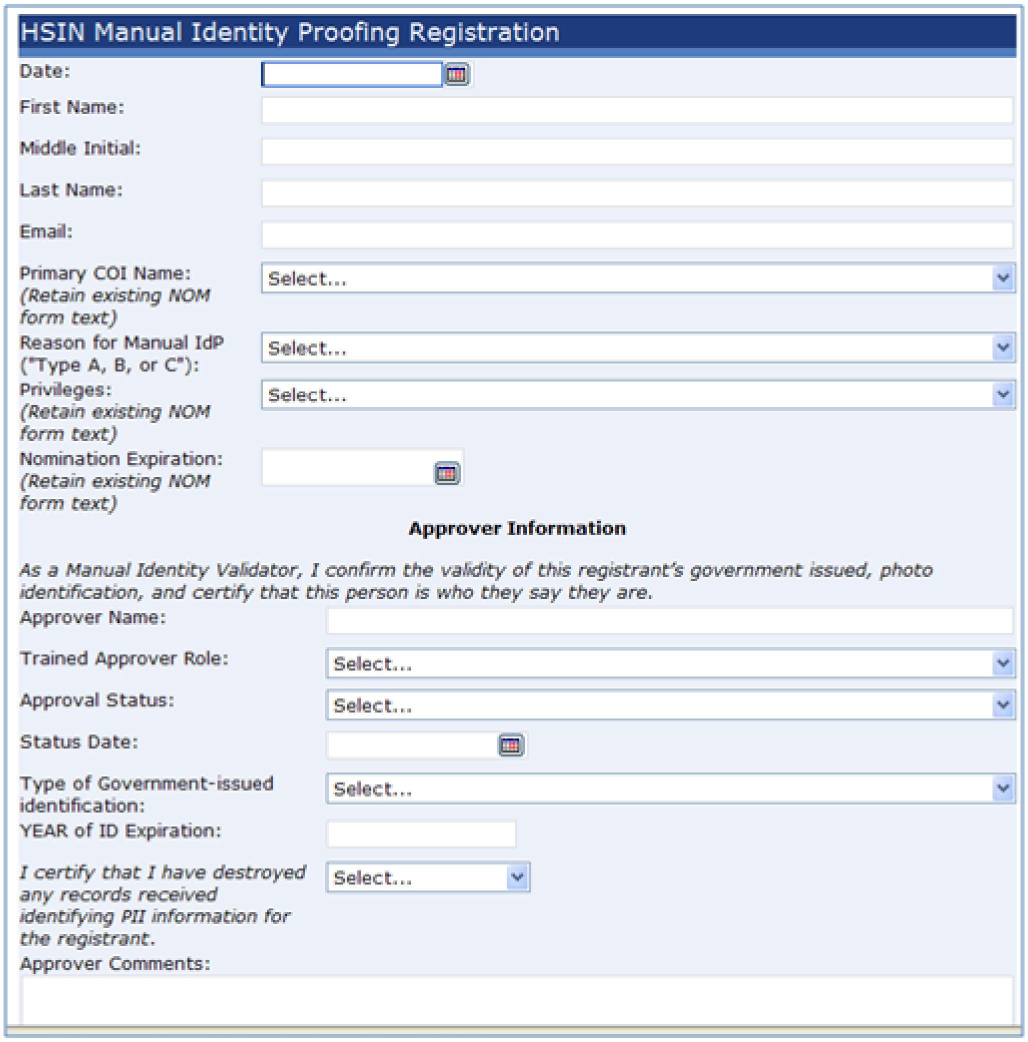
The reasons for a registrant to process through to manual IdP are as follows:

- Scenario (1) A HSIN registrant has failed the online, electronic IdP process three times;
- Scenario (2) A HSIN registrant has a time-sensitive, mission-critical role requiring timely admission to HSIN; and/or
- Scenario (3) A HSIN registrant is an international registrant.

The HSIN manual IdP process will collect the following information in an online form:

- First Name
- Middle Initial
- Last Name
- Email
- Primary COI Name
- Reason for Manual IdP
- Nomination Expiration (+60 days from emailed link)
- Type of government-issued identification
- Year of expiration for government-issued identification
- Certification that any materials collected containing PII have been properly destroyed

The following image illustrates the HSIN manual IdP form required for registrants, MIVs, and the HSIN ISSM, or appointed alternate, to complete.



HSIN Manual Identity Proofing Registration

Date:	
First Name:	
Middle Initial:	
Last Name:	
Email:	
Primary COI Name: *(Retain existing NOM form text)*	Select...
Reason for Manual IdP ("Type A, B, or C"):	Select...
Privileges: *(Retain existing NOM form text)*	Select...
Nomination Expiration: *(Retain existing NOM form text)*	

Approver Information

As a Manual Identity Validator, I confirm the validity of this registrant's government issued, photo identification, and certify that this person is who they say they are.

Approver Name:	
Trained Approver Role:	Select...
Approval Status:	Select...
Status Date:	
Type of Government-issued identification:	Select...
YEAR of ID Expiration:	
I certify that I have destroyed any records received identifying PII information for the registrant.	Select...

Approver Comments:

Figure 1: HSIN Manual IdP Form

HSIN PMO will provide training to qualified individuals who will take on the MIV role. The training materials will include a definition of a qualified, manual IdP candidate, how to validate the registrant's identity, appropriate forms of government-issued identification, steps on how to submit materials to the HSIN Security Office, and the mandatory obligation to destroy all PII submitted.

Uses of the Information

HSIN user account information is only used to provide authorized individuals with access to DHS information technology resources. HSIN is designed to allow all relevant, vetted stakeholders access to the information regardless of jurisdictional, geographic, or agency boundaries, so long as the information is appropriate to be shared.

During the manual IdP process, in order to verify the registrant's identity, PII will be collected to authenticate the registrant for access into HSIN, a COI, or any HSIN collaboration space within the HSIN system. HSIN PMO will train a core set of registered users to perform duties defined for the MIV role.

Retention

The HSIN PMO is assessing the technical capabilities of the HSIN Help Desk ticketing system to determine how they will delete the PII contained in a Help Desk record of a MIV request. HSIN PMO will continue to coordinate with the Privacy Office on a technically feasible retention period, not to exceed one year from a) when the request was filled or b) the original request if an individual fails to use the HSIN MIV. HSIN PMO will provide a memorandum to the Privacy Office detailing the records retention and deletion process once determined.

The HSIN MIV only reviews and submits information through the online manual IdP Form. HSIN MIVs and other HSIN PMO representatives participating in the manual IdP process will obtain rigorous training that outlines all requirements and processes ensuring a seamless, secure, and efficient user experience. Additionally, a detailed manual IdP standard operating procedure (SOP) will be accessible and fully up-to-date for all HSIN PMO, Help Desk representatives, and MIVs.

The retention of HSIN user account records has not changed from the original PIA.

Internal Sharing and Disclosure

There are no changes to the internal sharing and disclosure procedures described in the HSIN User Accounts PIA.

External Sharing and Disclosure

Basic personally identifiable information such as contact information will be transmitted from the HSIN Help Desk to the relevant MIV to facilitate the manual IdP process. This sharing is conducted pursuant to routine use F in the published system of records notice, DHS/ALL - 004 General Information Technology Access Account Records, 77 Fed. Reg. 70792 (Nov. 27, 2012).

Upon completion of the manual IdP process, the MIV does not receive any information from HSIN regarding the completion of the New User Registration Process. Information collected by the MIVs via the HSIN manual IdP form will not be shared externally.

Notice

Registrants will receive a Privacy Act Statement on the user access request form at the time of enrollment. Additionally, users receive notice that their activity on HSIN R3 will be logged and monitored in accordance with DHS authorities and policies to ensure appropriate use of DHS systems. The user notice is provided prior to each login.

Furthermore, for the manual IdP process, a registrant will receive a memo from the HSIN PMO reminding them of HSIN's Privacy Act Statement.

Individual Access, Redress, and Correction

There are no changes to access, redress, and correction procedures described in the HSIN User Accounts PIA. These procedures are also described in the DHS/ALL - 004 General Information Technology Access Account Records, 77 Fed. Reg. 70792 (Nov. 27, 2012).

Technical Access and Security

HSIN PMO will provide training to qualified individuals who will take on the MIV role. The training materials will include a definition of a qualified, manual IdP candidate, how to validate the registrant's identity, appropriate forms of government-issued identification, steps on how to submit materials to the HSIN Security Office, and the mandatory obligation to destroy all PII submitted.

Each manual IdP role has a vital purpose with specific technical access requirements. The following outlined role criterion are baseline requirements for the MIV and the HSIN ISSM:

MIV

The MIV operates as the primary point of contact during the manual IdP process. All MIVs will receive required training from the HSIN PMO in order to transact the necessary duties of identity verification and confirmation for qualified registrants. The MIV must have a Department of Homeland Security supported mission and be an active HSIN user. The MIV is intended to coordinate in-person meeting sessions with HSIN registrants to review required documentation and confirm registrant identity.

HSIN ISSM

The HSIN ISSM is the primary authority who offers access authorization to a registrant applying via manual IdP. The HSIN ISSM may appoint an alternate HSIN PMO Security staff member to execute duties in his absence. Manual IdP forms will be received by the HSIN ISSM, or appointed alternate, by email scan. Once the pertinent information has been captured into the system, the HSIN ISSM, or appointed alternate, must immediately discard any and all materials containing PII. The HSIN ISSM, or appointed alternate, has the right to confirm or deny a registrant's HSIN membership.

The MIV will ensure full and effective validation through identity confirmation. The MIV and HSIN ISSM, or appointed alternate, will be accountable for the destruction of all PII materials submitted through this process. The HSIN PMO will hold periodic compliance audits to ensure all processes are adhered.

Technology

The manual IdP process does not employ any new technology that would raise additional privacy risks. The manual IdP process is used in the three scenarios described above when a HSIN user does not use the automated IdP technology provided. The manual IdP process authenticates potential HSIN users without employing the automated IdP technology, and therefore is a less technological way to authenticate a user's identity. The forms submitted as part of the manual IdP process are electronically submitted from the MIV to the HSIN ISSM. All parties that participate in the manual IdP process will attest to the HSIN PMO that they have successfully destroyed all materials containing PII information.

Responsible Official

Donna Roy

HSIN Program Director

OCIO/OPS

Department of Homeland Security

Approval Signature

Original Signed Copy on File with DHS Privacy Office

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security