Privacy Impact Assessment Update
for the

HSIN R3 User Accounts: Identity Provider within the National Information Exchange Federation (NIEF)

DHS/OPS/PIA-008(c)

February 18, 2014

Contact Point
James Lanoue
DHS Operations
HSIN Program Management Office
(202) 343-4224

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), Office of Operations Coordination and Planning (OPS) maintains the Homeland Security Information Network (HSIN). HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as undertaking incident management activities.[1] This Privacy Impact Assessment (PIA) Update documents how OPS is establishing of new information sharing relationships with the national Information Exchange Federation (NIEF).

Overview

NIEF is a collection of agencies in the U.S. that have come together to share sensitive law enforcement information.[2] A federation is the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization. Federated[3] information access with NIEF allows HSIN to enable, operate, maintain, enhance, and expand the secure, standards-based, inter- and intra-Departmental information sharing through the globally recognized Global Federated Identity and Privilege Management (GFIPM) standard.

HSIN: Front Door to Information Sharing

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. DHS mission partners rely on HSIN as a trusted environment that supports DHS Information Sharing Environment (ISE)[4] 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.

---

[1] For a detailed description of the HSIN program generally and the associated privacy risks, please *see* DHS/OPS/PIA-007 – HSIN 3.0 Shared Spaces on the Sensitive But Unclassified Network PIA (July 25, 2012) and DHS/OPS/PIA-008 – HSIN R3 User Accounts PIA (July 25, 2012), and subsequent updates, available at http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning

[2] https://nief.gfipm.net/

[3] A federation is the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization

[4] For more information about ISE please visit: https://www.ise.gov/category/free-tags/dhs

Federal Drivers, Government-wide Policy & National Strategy Implementation

A series of official guidance and standards documents establish the requirements for interoperable and federated access, causing HSIN users to demand for this interoperable and federated access. These are detailed below.

The July 3, 2003 Office of Management and Budget (OMB) policy Memorandum, "*Streamlining Authentication and Identity Management within the Federal Government*," calls for reducing "...the burden on the public when interacting with government by allowing citizens to use existing credentials to access government services and enabling new services that otherwise could not or would not have been available," when addressing the requirements ofrequired Section 203 of the E-Government Act[5] and discussing how to comply with the Government Paperwork Elimination Act.[6]

In addition, OMB Memorandum M-11-11, issued in February 2011, requires Agencies to "align [with the] Federal Chief Information Officer (CIO) Council's Federal Identity, Credential and Access Management[7] (FICAM) Roadmap and Implementation Guidance."[8] One of the government-wide governance initiatives under the FICAM Roadmap (Initiative 2) is to establish a federated identity framework for the U.S. federal government.

The December 2012 National Strategy for Information Sharing and Safeguarding (NSISS) highlights the importance of gathering and reporting locally-generated information while emphasizing two-way flows of timely and actionable information among government, public, and private entities. Prioritized objectives outlined in the NSISS, requires information sharing systems to "adopt metadata standards to facilitate federated discovery, access, correlation, and monitoring across Federal networks and security domains." Moreover, NSISS calls upon the federal government to "extend and implement the FICAM Roadmap across all security domains."

Other developments strengthened the push to use trusted third-party credentials via a trust framework provider. The National Strategy for Trusted Identities in Cyberspace (NSTIC), issued in April 2011, calls for the federal government "to promote the emergence of an integrated landscape of solutions, building on a number of existing or new public and private initiatives to facilitate the creation of the Identity Ecosystem. [State, local, tribal and territorial governments] will also offer services online as relying

[5] P.L. 104-347

[6] P.L. 105-277

[7] Requires a mechanism to assess the identity management standards against applicable federal requirements, policies, and laws. http://ise.gov/building-blocks-content/federal-identity-credential-and-access-management-ficam

[8] OMB Policy Memorandum M-11-11 (February 3, 2011) http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

parties and, as subjects, will use services provided by others."[9] The October 6, 2011 OMB Memorandum on Requirements for Accepting Externally-Issued Identity Credentials, requires agencies to enable externally-facing applications to accept third-party credentials.[10]

More directly, homeland security information sharing ensures trust between users and content owners. That trust is now supported through improved technology and policies. Federal agencies and all their partners now use trust frameworks and their common, standardized, and enforced user credentials to ensure trust, sharing, and safeguarding. In this way, efficiencies are gained by breaking down silos of information while reinforcing the overall security of all networks in the trust framework.

HSIN's Vision & NIEF Membership

HSIN is rooted in providing a network of trust for its users. HSIN ensures trust by breaking down vertical information sharing silos through: 1) attribute-based access to content; 2) simplified sign-on capabilities; and 3) access to a series of system partners within the federated eco-system. These advancements are realized through HSIN's recent membership acceptance into NIEF. As a federated system under NIEF, HSIN is now a trusted partner with the abilities to have its users leverage multiple information sharing systems through a more simplified access point.

Membership in NIEF is open to all U.S. justice, homeland security, emergency management, and public safety agencies, as well as other agencies and organizations that provide information services to these communities. HSIN's membership in NIEF allows HSIN users access to justice and homeland security-related information from all levels of government through systems operated by current NIEF partners. (*See Figure 1* for an illustration of the HSIN/NIEF relationship.) This allows individuals to use the same user name and password, or other personal identification, to securely sign on to the networks of more than one enterprise in order to conduct transactions (a process known as "single sign-on"). Federation can allow agencies to share applications and information securely without maintaining full user accounts for their partner's clients, which helps to maintain privacy protections.

HSIN uses NIEF as a Trust Framework Provider

NIEF permits systems within its federated eco-system[11] to authenticate users across various organizations with only a limited amount of information transmitted

[9] National Strategy for Trusted Identities in Cyberspace
http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[10] FICAM TFS, version 1.0.0 11/11/13
http://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_Overview_v1.0.0_DRAFT.pdf
[11] Federated eco-system—An information sharing model where partners are trusted and information is shared within and across enterprises and value chains for a variety of purposes. http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf

between them. The federal government (including DHS) established the Trust Framework Solutions (TFS), which facilitate trusted, confident, secure, and privacy-enhancing authentication of individuals using valid credentials from approved organizations. *See Figure 1* below for an illustration that outlines HSIN's relationship to NIEF and the drivers, processes, and standards that support this partnership.

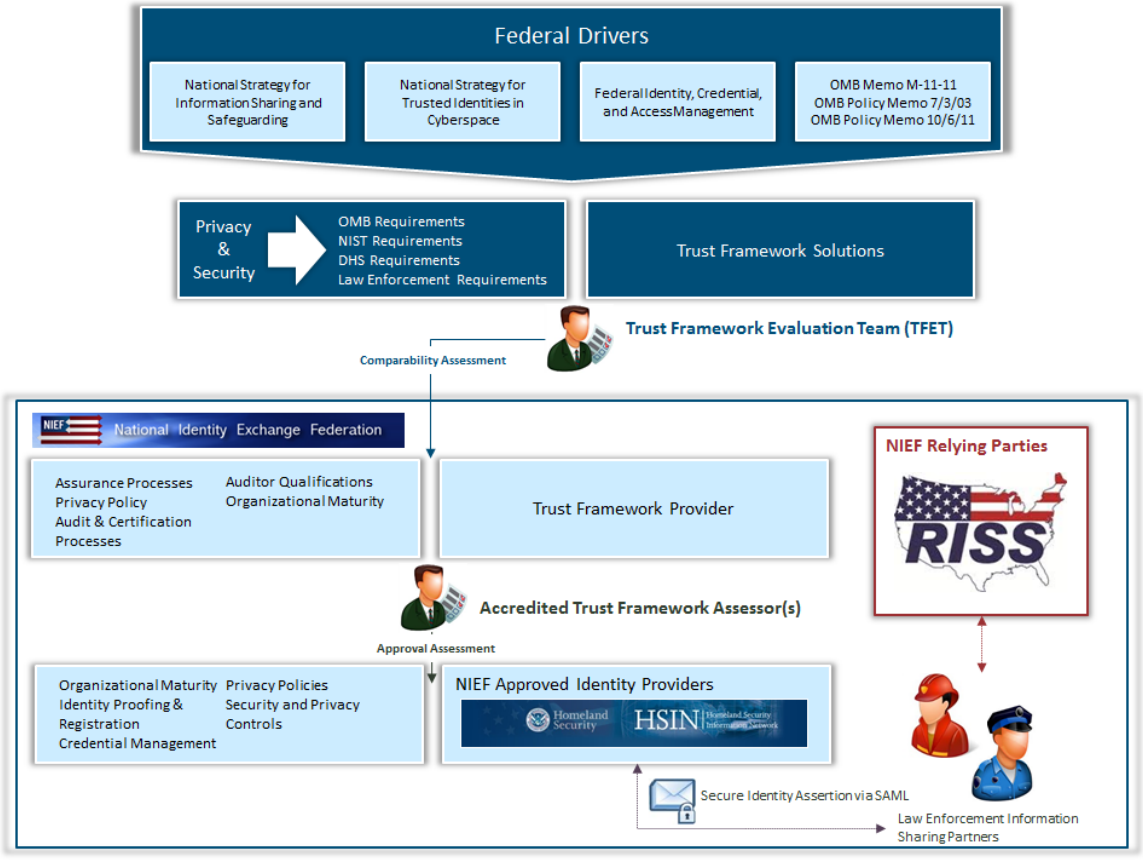

Figure 1: HSIN / NIEF relationship

1. Trust Framework Adoption Process.

The Trust Framework Provider Adoption Process (TFPAP) established by the federal government is used to assess existing, industry-based, Trust Frameworks and approve them as Trust Framework Providers (TFP).[12] TFPs are the governance structure for a specific identity system consisting of:

Technical and Operational Specifications that have been developed:

- To define requirements for the proper operation of the identity system (i.e., so that it works);

[12] A Trust Framework Provider whose framework (as submitted to the FICAM Trust Framework Evaluation Team (TFET)) is fully comparable to the TFP Adoption Process, and who has provided all requested proofs in that regard. The TFP can assess and approve third-party credential providers on behalf of ICAM. http://www.idmanagement.gov/approved-trust-framework-providers

- To define the roles and operational responsibilities of participants; and
- To provide adequate assurance regarding the accuracy, integrity, privacy, and security of its processes and data (i.e., so that it is trustworthy).

Legal Rules that govern the identity system in order:

- To regulate the content of the Technical and Operational Specifications;
- To make the Technical and Operational Specifications legally binding on and enforceable against the participants; and
- To define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

2. Trust Framework

A trust framework is established by a community whose members have similar goals and perspectives. The framework defines the rights and responsibilities of that community's participants; specifies the policies and standards specific to the community; defines the community-specific processes and procedures that provide identity assurance; and governs the overall adherence to community specific policies. All trust frameworks that are approved by the federal government (such as NIEF) must meet a baseline set of auditable security and privacy standards established by OMB,[13] the National Institute of Standards and Technology (NIST),[14] and the General Services Administration (GSA).[15]

3. Identity Provider Credential Process

TFPs define the processes for assessing Identity Provider (IP) credentialing processes against federal requirements for issuance, privacy, and auditing. Simply put, TFPs, such as NIEF, audit and accredit member IPs based on certification criteria they define that meet federal requirements. NIEF is a TFP candidate, currently undergoing accreditation by the FICAM TFS Program's Trust Framework Evaluation Team (TFET). HSIN will only share identity information within the NIEF Trust Framework once NIEF becomes a FICAM-approved Trust Framework Provider.

Credentials issued by an IP that has been approved by a TFP can be trusted by an agency Relying Party (RP). Said another way, federal RPs that are a member of a TFP such as NIEF, do not need to establish point-to-point agreements, requirements, and

[13] OMB Memo M-11-11 http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), OMB Memo M-05-05, 7/3/03 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-05.pdf), OMB Memo 10/6/11 (http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/ombreqforacceptingexternally_issued idcred10-6-2011.pdf)
[14] NIST 800-63-1 Electronic Authentication Guide (http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf)
[15] GSA's FICAM Roadmap (http://www.idmanagement.gov/) and TFS (http://idmanagement.gov/trust-framework-solutions)

standards with individual IPs since NIEF has already done this on behalf of all RPs, and in accordance with federal guidelines. All RPs understand and concur with the certification of IPs that are part of the TFP. Additionally, these credentials must be exchanged using approved standards that define the security and privacy data exchange protocols that are acceptable for federal government use. Given that the TFS Program, including NIEF, leverages existing, industry-based frameworks, it enables a scalable model for extending identity assurance across a broad range of citizen and business needs.[16]

4. HSIN's Capabilities within the Federation

The first phase of HSIN's capabilities within this federation is to operate as a NIEF IP. This capability means HSIN provides user identity assurance to other RPs within NIEF. In other words, HSIN users who are registered, validated, and authenticated into HSIN now have the capability of obtaining access to NIEF RPs without having to re-prove their identity. The first federated partnership for HSIN within NIEF is with the Regional Information Sharing System, hereinafter referred to as RISSNET. However, HSIN now has the ability to share information with a broad range of partners without modifying its strict, FICAM-approved, security and privacy controls for identity assurance and authentication in the longer term because NIEF consists of a community of approved IPs and RPs.

RISSNET is a sensitive but unclassified (SBU) system serving thousands of local, state, federal, and tribal criminal justice agencies in their effort to identify, detect, deter, prevent, and solve criminal and terrorist-related investigations.[17] HSIN's trusted relationship with RISSNET, and simple pass-through of minimal information, has expanded information sharing capabilities and provides access to information verticals that have previously not been available. HSIN is among a federation of systems that interoperate with each other, under the strict guidelines and membership criteria between all parties under NIEF, the policies and standards outlined in the FICAM documents, and in alignment with the federal mandates cited above.

Federated Identity Management Roles[18]

In this federated information sharing model identity credentials issued to a user by a particular service or entity are recognized by a broad range of other systems. A trust-enabled federation typically contains the following roles:

[16] http://www.idmanagement.gov/trust-framework-solutions
[17] http://www.riss.net/
[18] A federated identity is an identity system that allows the sharing of identity credentials, and for identity information to be asserted, by one or more identity providers, with multiple relying parties and trusted partners. *See* American Bar Association Identity Management Legal Task Force Confidential Discussion DRAFT, Solving the Legal Challenges of Online Identity Management PART 1 Identity Management Fundamentals and Terminology, December 30, 2011.

- **Relying Party (RP), or Service Provider (SP):** A web application that provides a service to the user, but which has outsourced user authentication. This service thus "relies" on a third party to provide identity information.
- **Identity Provider (IP)**: An approved organizational entity with which the user has established his/her identity in accordance with OMB Memo 04-04 (E-Authentication Guidance for Federal Agencies)[19] and NIST 800-63-1 (Electronic Authentication Guideline).[20] The IP provides identity verification services to the RP.
- **Discovery Service**: A means of finding an IP that is acceptable to both the user and the RP; this could be as simple as a drop-down menu on the SP's website.

HSIN as an Identity Provider within NIEF

HSIN operates as an IP within NIEF with RISSNET as the first RP allowing HSIN users to access RISSNET data. (The full list of potential RPs with which HSIN may transact can be found in the *Appendix*.) The benefits of HSIN operating as an IP within NIEF means that HSIN users do not need to go through the time-consuming process of re-authenticating their identity in order to gain access into a RP, such as RISSNET. Instead, a user may use active credentials from HSIN to gain access into NIEF RP data (e.g., RISSNET). Only the information required for the user to operate within RISSNET is exchanged from HSIN to RISSNET during this transaction. Additional benefits of joining NIEF as an IP include access to an abundance of justice-related information resources at all levels of government that are already available from current NIEF partners. The benefits from operating as an RP within NIEF affects more than 95,000 users representing various justice-related organizations who can access information resources (subject to the specific RPs access control policy) without requiring the RP to manage any additional user accounts. The following narrative outlines more details about this information exchange.

The NIEF trust framework provides a fabric in which RPs of information resources make those resources available to other active users of NIEF IPs. Each RP controls which of the NIEF IP users gain access to each of their resources by inspecting trusted attributes about a user. Those user attributes are encapsulated in a Security Assertion Markup Language (SAML) data structure that is sent to the RP by the IP when the user attempts to gain access to a particular resource. This exchange of attribute information within a SAML assertion requires protection of personally identifiable information (PII) in transit using FIPS 140-2 compliant encryption. The assertion is digitally signed to further prove the validity and trustworthiness of the information being

[19] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
[20] http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

exchanged per GFIPM and FICAM guidelines. All assertions transmitted to NIEF use the FICAM/GFIPM approved SAML profile. That SAML profile package includes the following:

SAML Assertion Profile Package			
Data Requested	**Contents**	**Collected (by RISSNET)**	**Stored (by RISSNET)**
1. Where the user came from (which IP)?	HSIN, for example	✓	✓
2. How did the user login?	Using their username/password, token, for example? The actual access credentials are never provided to the RP, only the actual method of login.	✓	✓
3. What is the level of assurance of this system? – e.g., HSIN is LOA 3[21]	Level of Assurance (LOA) 1: Little or no confidence in the asserted identity's validity. Level of Assurance (LOA) 2: Some confidence in the asserted identity's validity. Level of Assurance (LOA) 3: High confidence in the asserted identity's validity. Level of Assurance (LOA) 4: Very high confidence in the asserted identity's validity.	✓	✓
4. 8 GFIPM attributes	**Identity Provider Id** o The unique identifier within the federation that identifies the identity provider of the user within the federation (e.g., this is HSIN's ID number.)	✓	✓
	Federation Id o The persistent, federation-unique identifier for the user, comprising a federation part, an optional trusted identity broker (TIB) part, an identity provider (IDP) part, and a local ID.	✓	✓

[21] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

SAML Assertion Profile Package			
Data Requested	**Contents**	**Collected (by RISSNET)**	**Stored (by RISSNET)**
	Given Name* ○ A first name of a HSIN user.	✓	✓
	Surname* ○ A last name of a HSIN user.	✓	✓
	Email Address Text* ○ The electronic mailing address by which the user may be contacted.	✓	✓
	Telephone Number* ○ The telephone number for a telecommunication device by which the user may be contacted.	✓	✓
	Local Id* ○ The unique local identifier associated with the user for internal purposes within the user's identity provider (e.g., a numeric code that HSIN associates with its user.) ○ Not saved by RISSNET.	✓	
	Employer Name* ○ The name of the organization that is the user's primary employer. ○ Not saved by RISSNET. **** Indicates data elements that are PII***	✓	

Table 1: SAML Assertion Profile Package

A full illustration of the system transaction flow and narrative to describe each step is illustrated below in *Figure 2*.

For purposes of this illustration below, the terms IP "Identity Provider" and "IdP" are synonymous. The term "AuthNRequest" mean "authentication request." The following narrative explains each step in the process:

- **Step 1**: End user visits the RP (i.e., RISSNET) website (*See Figure 3*).

- **Step 2**: End user chooses an IP (e.g., HSIN) from list (*See Figure 4*). End User is redirected to IP (e.g., HSIN, *See Figure 5*) to authenticate. *This is a technical back-end function.*
- **Step 3**: End user logs in using HSIN credentials on HSIN website (*See Figure 5*) and authenticates. End user is redirected to the RP (e.g., RISSNET) with a valid authentication assertion. The full SAML assertion profile package is described in Table 1 above.
- **Step 4**: RP verifies the SAML assertion profile package from HSIN by validating the system signature. RP then provides the end user with appropriate access (in this case, permission to access the desired RP resource).

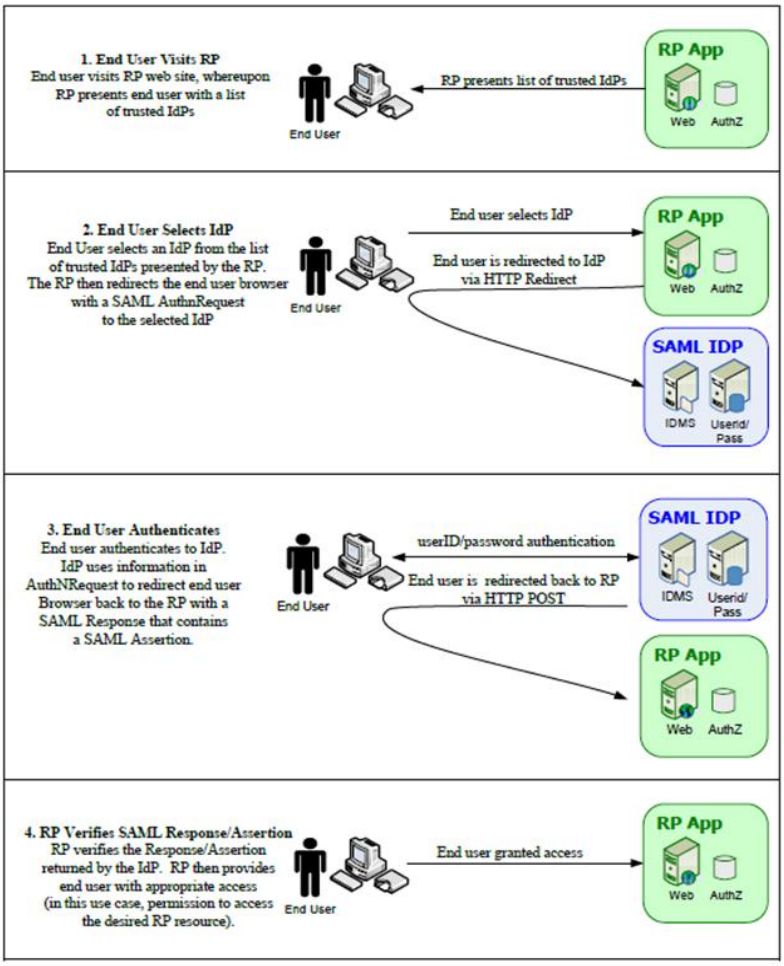

Figure 2: Conceptual Diagram[21]

Reason for the PIA Update

HSIN is establishing a series of information sharing relationships, by means of

[21] http://www.idmanagement.gov/sites/default/files/documents/SAML20_Web_SSO_Profile.pdf

federated access, with new system partners. This PIA Update is necessary because of the trusted partnership that is inherited through NIEF that allows HSIN to be an IP for other partner systems in this federation. As an IP within NIEF, a registered HSIN user[22] may use his/her credentials to log-on to other federated systems that are current, active NIEF partners. This capability allows a HSIN user's identity to be automatically validated with other partner systems within NIEF.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

Operationally, in order for RISSNET to accept the HSIN user into its system, HSIN, as the IP, automatically sends the following SAML assertion profile package to RISSNET. Table 1 above (the SAML Assertion Profile Package) provides detail on the data requested, the contents, and collection and storage by RISSNET. The following general data elements are collected by the RP:

- Where the user came from (which IP)?
  - HSIN, for example
- How did the user login?
  - Username/password, token, etc.
  - Note: The actual access credentials are never provided to the RP, only the actual method of login.
- The level of assurance of this system (LOA 1, 2, 3, or 4)
  - HSIN is LOA 3, for example
- 8 GFIPM attributes:
  - Identity Provider ID
  - Federation ID
  - Given Name
  - Surname
  - Email Address Text
  - Telephone Number

[22] A HSIN user who has been validated and authenticated by the HSIN system. The DHS/OPS/PIA-008(b) - HSIN Release 3 User Accounts: Identity Proofing Service PIA describes this process (http://www.dhs.gov/publication/dhsopspia-008b-hsin-release-3-user-accounts-identity-proofing-service).

- Local ID (not saved by RISSNET)
- Employer Name (not saved by RISSNET)

Uses of the Information

This SAML assertion profile package contains 8 attributes exchanged between the IP (e.g., HSIN) and the RP (e.g., RISSNET). From these 8 attributes, only 6 are stored by RISSNET in its active directory (AD) system audit log. NIEF policy requires that the use of these attributes be limited to: 1) making authorization decisions; 2) dynamically provisioning accounts; and 3) performing audit logging. Any additional use of PII about a user is prohibited unless the following conditions are met: 1) the user's identity provider (e.g., HSIN) must agree to it; and 2) the use must be disclosed to the user. The minimal PII shared between HSIN and RISSNET allows HSIN users to access RISSNET without performing identity proofing processes since these users are recognized by HSIN as an authenticated and validated, active user.

Retention

The 8 attributes stated above are sent from HSIN to RISSNET via SAML assertion. Once RISSNET receives the information from HSIN, they create a user audit entry within their AD system storing 6 of the 8 attributes sent in the SAML assertion. RISSNET saves the following 6 attributes in the audit log: 1) Identity Provider ID, 2) Federation ID, 3) Given Name, 4) Surname, 5) Email Address Text, and 6) Telephone Number. The information sent from HSIN to RISSNET is covered by the DHS/ALL - 004 General Information Technology Access Account Records System (GITAARS) System of Records Notice (SORN).[22] This information is stored within the AD for 6.5 years after date of last activity, account termination or alteration, or when no longer needed for investigative or security purposes, whichever is later.

The information will continue to be stored, consistent with the relevant retention schedule and data security safeguards, even if the partner system ceases to provide this service or be a federated partner. Access to these attributes (or linking to a real identity) is not possible once the user is removed from HSIN since HSIN is the identity provider. The information stored in RISSNET's AD is only accessible by RISSNET's Security Administrative personnel. The information sent from HSIN to RISSNET will be covered under a forthcoming DHS-wide "E-Authentication" SORN when the SORN is published in the Federal Register. The SORN will be reflective of the retention schedule(s) identified in NIST SP-800-63-2.[23] This PIA will be updated when the new DHS-wide SORN is published in the Federal Register.

[22] DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792
[23] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

As a partner within NIEF, NIEF's RPs (e.g., RISSNET) are required by policy to limit their use of PII to making authorization decisions, dynamically provisioning accounts, and performing audit logging. Any additional use of PII about a user is prohibited unless the following conditions are met: 1) the user's identity provider (e.g., HSIN) must agree to it; and 2) the use must be disclosed to the user.

All RISSNET personnel (including the security administrators) involved in the handling of PII sensitive documents for this information exchange receive training that outlines all requirements and standards that align with RISSNET's Security Policy 07-001 and Terms of Use.[24]

Internal Sharing and Disclosure

There are no changes to the internal sharing and disclosure procedures described in the HSIN User Accounts PIA.[25] Any component within DHS may use HSIN to enhance its information-sharing capabilities. HSIN Community of Interest (COI) Sponsors are able to request the configuration of new COIs, which operate under their specific Charter and the HSIN Terms of Service. COIs may specify membership criteria and other controls pertaining to who gains access to what information within the COI. These controls are designed to ensure security and integrity of HSIN and to limit damages to HSIN, providing users with transparency on their rights, duties, and privileges.

External Sharing and Disclosure

To ensure a seamless user experience when attempting to access system information under the federated relationship HSIN must transfer and share the SAML assertion profile package (*See Table 1*) of information externally to RISSNET, to ensure a seamless user experience when attempting to access system information under the federated relationship.

All systems within NIEF, including RISSNET and HSIN, take responsibility for the privacy and security of PII throughout its lifecycle consistent with the international standards that have been developed by NIEF. RISSNET members protect PII according to safeguards that align to applicable laws, regulations, and agency-specific policies, including 28 C.F.R., RISSNET's Security Policy 07-001, and RISSNET's Privacy Policy. No further disclosures are made.

The sharing and disclosure of user information by HSIN for identity proofing is currently covered under the DHS/ALL – 004 General Information Technology Access Account Records SORN.[26] DHS is in the process of writing a new DHS-wide SORN for

[24] RISSNET's Security Policy (https://extranet.riss.net/public/761d86ca-1b3c-45c3-9b5b-cbbafe58fb8b) and RISSNET Terms of Use (https://logon.riss.net/Terms.aspx)
[25] HSIN R3 User Accounts, July 25, 2012
[26] DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS)

E-Authentication. Authentication information collected by HSIN and sent to RISSNET (or other federated systems) will receive coverage under this new SORN when it is published in the Federal Register. Sharing of authentication information with RISSNET is permitted by routine uses (i) and (k) of the DHS/ALL – 004 General Information Technology Access Account Records SORN.[27] This PIA will be updated when the new "E-Authentication" SORN is published.

Notice

HSIN users receive notice prior to each login that their activity on HSIN is logged and monitored in accordance with DHS authorities and policies to ensure appropriate use of DHS systems. HSIN users have access to HSIN's Privacy Policy at all times and when using their credentials to logon to RISSNET and are able to access RISSNET's Privacy Policy from the logon screen.

A differentiation of screens are used so that HSIN users know to logon with their username/password to access RISSNET. *Figures 3, 4*, and *5* below capture the images that a HSIN user or federated partner views when logging into RISSNET.

- **Step (1)**: A HSIN user goes to RISSNET's website at www.RISSNET.net
- **Step (2)**: A HSIN user clicks on "Logon—RISSNET Logon" and views *Figure 3* below.
- **Step (3)**: A HSIN user clicks on "Access RISSNET through another identity provider (federation partners) (*Figure 3* below).
- **Step (4)**: A HSIN user selects "HSIN Logon" and a pop-up screen appears with HSIN's logon screen page (*Figure 4* below) and a message permitting the user to opt-in stating: "By logging on with your HSIN credentials, the following PII is shared with other federated systems in order for you to gain access: 1) Given name, 2) Surname, 3) Telephone number, 4) Email address, 5) Local ID, and 6) Employer name. You may opt-out of this service but you will limit and/or revoke your system access into this federated system. By clicking "agree" you accept this action."

November 27, 2012, 77 FR 70792
[27] DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS)
November 27, 2012, 77 FR 70792

Figure 3: Sample Screenshot of RISSNET's Federated Login Screens

Figure 4: Sample Screenshot of RISSNET's Federated Login Screens PART II

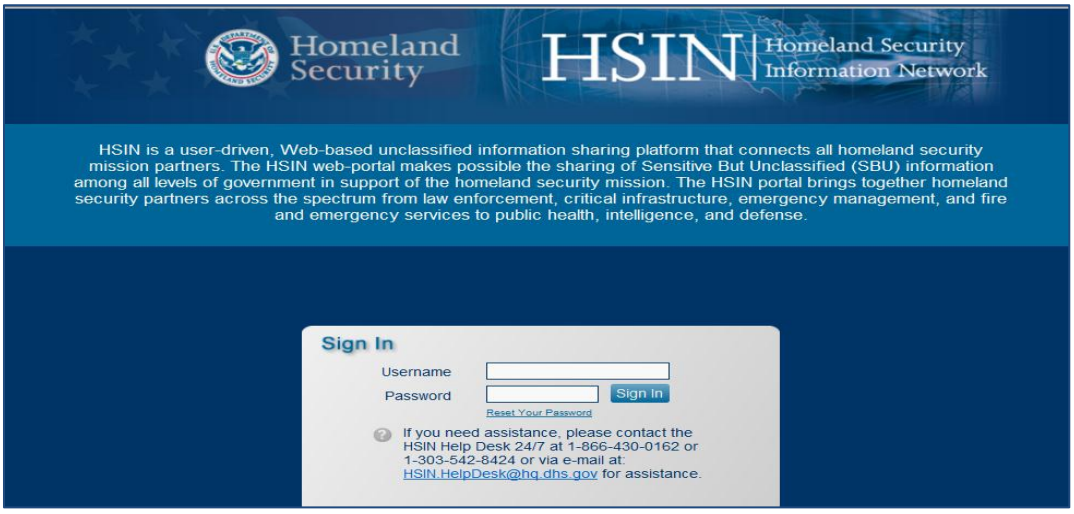

Figure 5: HSIN Logon Screen

- **Step (5):** The HSIN user logs on to the HSIN screen with his/her HSIN credentials and after HSIN accepts them, is redirected back to the RISSNET system with granted access—*See Figure 5*.

Individual Access, Redress, and Correction

There are no changes to access, redress, and correction procedures described in the HSIN User Accounts PIA[28] and the DHS/ALL – 004 General Information Technology Access Account Records SORN.[29]

Technical Access and Security

The 8 user attributes discussed above are sent from HSIN to RISSNET via SAML assertion. Once RISSNET receives the information from HSIN, it creates a user entry within their AD system storing 6 attributes sent in the SAML assertion profile package. Specifically, RISSNET saves the following in its audit log: 1) Identity Provider ID; 2) Federation ID; 3) Given Name; 4) Surname; 5) Email Address Text; and 6) Telephone Number.

This information is stored within this AD for 6.5 years after date of last activity, and will continue to be protected even if the partner system ceases to provide this service or be a federated partner. Access to these attributes (or linking to a real identity) is not possible once the user is removed from HSIN since HSIN is the identity provider. The information stored in RISSNET's AD is only accessible by RISSNET's Security Administrative personnel. NIEF's RPs (e.g., RISSNET) are required by policy to limit their use of PII to making authorization decisions, dynamically provisioning accounts,

[28] HSIN R3 User Accounts, July 25, 2012
[29] DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792

and performing audit logging. Any additional use of PII about a user is prohibited unless the following conditions are met: 1) the user's identity provider (e.g., HSIN) must agree to it; and 2) the additional use must be disclosed to the user. All RISSNET personnel (including the security administrators) involved in the handling of PII sensitive documents for this information exchange obtain training that outlines all requirements and standards that align with RISSNET's Security Policy 07-001.

Technology

This new federated eco-system does not employ any new technology that would raise additional privacy risks. This environment operates behind the system's policies and procedures and in conjunction with the legal instruments surrounding the NIEF environment that bind parties to the obligations related to the appropriate deployment of technology.

Responsible Official

James Lanoue
HSIN Program Director
OCIO/OPS
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix

Since NIEF consists of a community of approved RPs, HSIN has the ability to share information with a broad range of partners without modifying its strict, FICAM-approved security and privacy controls for identity assurance and authentication. This appendix lists the relationships with which HSIN will operate as a NIEF IP. As NIEF grows its RP membership, this list may modify and evolve.

- Criminal Information Sharing Alliance (CISA)
- Pennsylvania Justice Network (JNET)
- Regional Information Sharing Systems (RISSNET)
- U.S. Department of Homeland Security (DHS)
- Los Angeles County
- Federal Bureau of Investigation (FBI)
- Institute for Intergovernmental Research (IIR)
- Tennessee Bureau of Investigation/Tennessee Methamphetamine and Pharmaceutical Task Force
- Verisk Crime Analytics
- Tennessee Integrated Criminal Justice Program
- Texas Department of Public Safety (TX DPS)