Privacy Impact Assessment Update
for the

HSIN Release 3 User Accounts: Identity Proofing Service

DHS/OPS/PIA-008(b)

May 22, 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 designed to facilitate the secure integration and interoperability of information sharing resources among federal, state, local, tribal, private-sector commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as in undertaking incident management activities.[1] The HSIN program prepared this Privacy Impact Assessment (PIA) update to clarify information about HSIN's use of and the data handling practices of the identity proofing service (IDP Service[2]). This PIA Update is being conducted to document the program's updated understanding of the information collected and stored by the IDP Service during, and following, new user registration on the HSIN R3 platform.

Overview

Identity Proofing Service (IDP Service)

When registering for a new account with HSIN, all registrants must process through an IDP Service to verify their identity. Registrants must submit information to verify their identity prior to being granted an account within HSIN. During the HSIN Account Registration experience, a registrant will be requested to input personally identifiable information (PII) into the system.

This verified identity is used to create an account in HSIN. The IDP Service generates 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 Service 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 Service in order to verify his or her identity and gain access to HSIN. After answering the questions, the IDP Service will send HSIN a transaction number, reasons for a session failure (if failure occurred), reasons for session success (if successful), and the date and time of the transaction. The information that is transmitted back to HSIN will be used by the HSIN Program Management Office (PMO) to

[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] At the time this PIA Update was composed, the HSIN Program Management Office (PMO) was engaged with Equifax as its IDP Service. The provider of IDP services to HSIN PMO may change and when it does this PIA will be further updated.

facilitate troubleshooting, system management, and system improvement including usage statistics on how many individuals were unable to have their identity verified by the IDP Service.

Each individual will be asked a minimum of two and a maximum of four knowledge-based questions. The IDP Service pulls data from aggregate providers that use only data that is high-level, basic information, including, but not limited to, name, previous addresses of residences, motor vehicle registration information, and demographics (such as age) data. If there is not enough commercial identity verification information to generate at least two questions, then the individual's identity cannot be verified and he or she will not be able to continue through the HSIN online registration. As stated above, the IDP Service maintains an audit log of each IDP Session. 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. If the registrant is able to answer the questions correctly, verifying his or her identity, a pass indicator is returned to HSIN, and the individual will continue through the HSIN online registration process. If identity verification was not successful, the registrant will have a total of three attempts to try again. However, the registrant may only fail the electronic IDP Service two times in any 24-hour period. On the third attempt, a registrant must wait 24 hours before trying again. If on the third attempt, the registrant fails the questions asked by the IDP Service, he or she will be unable to have his or her identity verified electronically and must call the HSIN Help Desk for further guidance.[3]

IDP Process

The HSIN Account Registration form requests and collects the following information, which DHS stores:

- First Name
- Last Name
- Middle Initial
- Business Phone (and extension)
- Mobile Phone
- US Citizen (Y/N)

[3] For a detailed description of the Manual Identity Verification process, please see DHS/OPS/PIA-008(a) HSIN R3 User Accounts Update: Manual Identity Proofing Process, (January 15, 2013), available at www.dhs.gov/privacy.

- Accepted Terms of Service (Y/N)
- Primary Email
- Two-factor authentication[4] information:
    - Email address (*which may be different from primary email upon user discretion*)
    - Mobile Phone for SMS
    - Phone Number for interactive voice response

Within the HSIN Account Registration form, there is a clearly labeled section for registrants to input information for the identity proofing process. This labeled section includes the following text assuring the registrant what will occur with his or her inputted information: "The information in this section will be sent to a third party identity proofing provider for validation purposes. A series of questions will be compiled by the third party provider requiring your response to verify your identity. This information will not be retained by DHS." DHS sends the third party provider the registrant's first and last name in addition to the following fields listed below:

- Home Street Address
- Home City
- Home State
- Home Postal Code
- Home Phone Number (optional)
- Date of Birth
- Social Security Number (optional)

[4] DHS Sensitive Systems Policy Directive 4300A defines Two Factor Authentication - authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g., a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms. Three-factor authentication uses all three forms. The process of establishing confidence in the identity of users or information systems. http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf

The IDP Service requests and collects the PII listed above (e.g., home street address, home city, home state, home postal code, home phone number (if provided), date of birth, and Social Security number (if provided)), in order to verify a registrant's identity. In addition to this information, the first and last name of the registrant is sent to the IDP Service from DHS. These data elements are collected by the IDP Service in order to "match" the information from the registrant with the information already owned by the IDP Service. This IDP Service is used to identify data consistencies and ultimately, verify the identity of the registrant. Registrants provide this PII by using a DHS Account Registration form. That form, itself, sits on a DHS site. However all PII that is collected for the identity proofing section of the form is sent directly to the IDP Service along with the registrant's first and last name. DHS does not store or retain the information collected in the identity proofing section of the DHS Account Registration form. Once registrants provide their PII, the IDP Service generates knowledge-based quiz questions for identity verification. If the registrant passes the IDP knowledge-based questions he or she will be granted access and requested to proceed forward to the rest of the DHS registration process. The remaining process requests the user to input information such as his or her preference on two-factor authentication delivery (i.e., SMS, email, phone number) illustrated in Figure 1, employment information (i.e., job title, job role, and organization), business street address, topics of interest, supervisor information (i.e., name, organization, email address, phone, and job title), and affiliation (e.g., mission area – federal, state, local). Refer to Figure 2 below for a sample view of the HSIN Account Profile sample screen. The user's name, email, and phone number (if provided) may already be captured in the designated fields of the CONTACT tab, illustrated below in Figure 3, from the nomination process. The nomination process involves a registered HSIN user submitting a qualified registrant's name, email address, and phone number (if provided) on the HSIN Nomination Form via HSIN Release 3.

Figure 1: HSIN Two-Factor Authentication Delivery Sample Screen

Figure 2: HSIN Account Profile Sample Screen

Figure 3: HSIN Account Profile Sample Screen – CONTACT TAB

Registrants use a website hosted on a .gov server to answer the IDP quiz questions; however, the information provided is passed directly through this .gov server to the IDP Service. At no time during this process does DHS store this information. When taking the quiz, registrants enter their information into a .gov website that has clearly been labeled as passing their information on directly to a non-.gov, IDP Service server. The screen displaying the IDP questions is a blank, non-branded screen with a different font than the DHS website. Refer to Figure 4. This .gov website and server are acting as a pass-through proxy for the IDP Service's service, and directly sending the registrants' information to the non-.gov, IDP Service server. DHS does not store, or have access to, this passed-through information. Furthermore, DHS does not have access to the commercial identity verification information used to generate the knowledge-based questions.

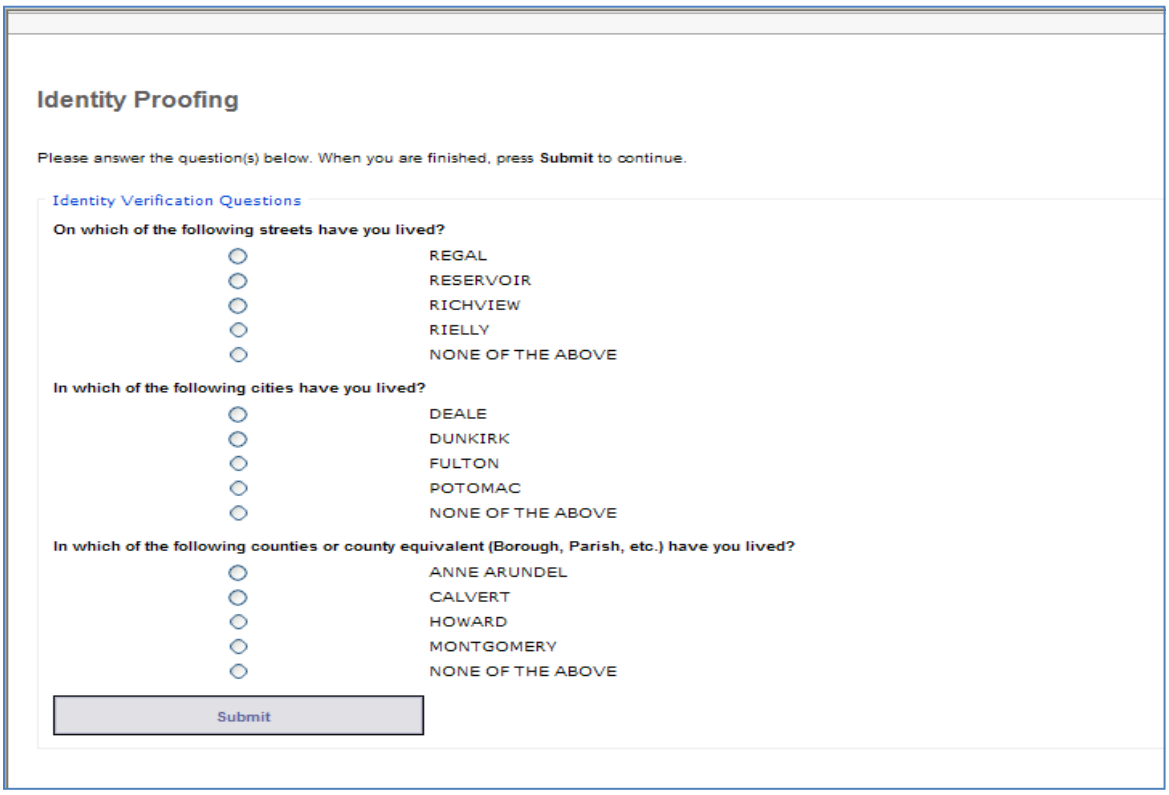

Figure 4: HSIN Account Profile Sample Screen – CONTACT TAB

The following outlines the IDP process of the HSIN registration experience:

1. The user accesses HSIN registration via the auth.dhs.gov URL. The HSIN registration form is located on DHS servers.

2. The user enters IDP information on the HSIN registration form. The fields that are used for IDP purposes include a registrant's: home street address, home city, home state, home postal code, home phone number (if provided), date of birth, and Social Security number (if provided). In addition to this information, the first and last name of the registrant is sent to the IDP Service from DHS.

3. Once the user completes entry, HSIN registration sends a request for transaction ID to the IDP server (Anakam.IDP server). The Anakam.IDP application is located on DHS servers. The contents of this request are: home street address, home city, home state, home postal code, home phone number (if provided), date of birth, and Social Security

number (if provided). In addition to this information, the first and last name of the registrant is sent to the IDP Service from DHS.

4. The Anakam.IDP server acts only as a proxy and forwards this information to the IDP Service cloud. The IDP Service Cloud is located outside of DHS Data Center 2 (DC2). Communication between the Anakam.IDP server (DHS) and IDP Service Cloud is protected by SSL.

5. The IDP Service cloud generates a transaction ID (which it stores) and attempts to find unique commercial records on the individual based upon the content sent in the request. This individual data is stored.

6. The IDP Service cloud returns the unique transaction ID and whether a unique match was found (in the form of result codes) in order to generate IDP questions. No questions/answers/user information is returned from the IDP Service Cloud at this point.

7. The Anakam.IDP server returns two unique transaction ID and result codes to the HSIN registration application.

8. The HSIN registration application evaluates the result codes and, if IDP questions can be generated, HSIN registration redirects the user to the Anakam.IDP server (auth.dhs.gov/idp). As part of the redirect, the HSIN registration application only sends the transaction ID (no questions/answers/user information is sent).

9. The Anakam.IDP server uses the transaction ID and requests the questions/answers (Q/A) from the IDP Service Cloud.

10. The IDP Service Cloud returns the Q/A to Anakam.IDP.

11. Anakam.IDP presents to the user the Q/A. Anakam.IDP does not know the correct answers. It is simply the proxy.

12. Once the user has answered the questions, Anakam.IDP submits the answers back to the IDP Service Cloud with the transaction ID.

13. The IDP Service Cloud evaluates the answers and returns a result response. The result response includes pass/fail and any generic result codes. Result codes are listed in Appendix B of the IDP integration guide.

14. Anakam.IDP redirects the user back to the HSIN registration application (auth.dhs.gov) with the result response obtained from the IDP Service Cloud.

15. HSIN registration evaluates the pass/fail header in the response that originated from the IDP Service Cloud and presents the results to the user.

16. HSIN registrant's who successfully pass the IDP questions, may now continue with the HSIN registration process by completing the HSIN registration forms, to include a resubmission of PII except for name, email and phone number (if provided) which would have been captured during the nomination process (see Figure 3 and description above).

The information submitted through the following fields simply pass through the HSIN registration and Anakam.IDP DHS servers, on their way to the IDP service provider's cloud server – the information is not stored on the DHS servers: address (street, city, zip), date of birth, social security number, or home phone number.

IDP Audit Log Retention and Uses

The IDP Service maintains an audit log of all identity verification transactions. The log includes information submitted by the user (name, address, date of birth, and if provided, the individual's SSN and home phone number), the questions asked of the user, whether the user answered the questions correctly, the scores generated during the proofing process, and the business rules that were triggered during the transaction. The purposes of maintaining the audit logs are (1) to conduct system management, and (2) to generate usage statistics/troubleshooting for customers of the IDP Service.

Audit logs of IDP transactions are first stored in the IDP Service's live database for three months. They have updated timestamps and remain fully accessible by the IDP Service's operating system during that time. After three months, the audit logs are archived for an additional seven years. They are maintained in a frozen state, inaccessible by the IDP Service's operating system, and must be pulled from the archive's backup system. DHS does not have access to the IDP Service live database or the archives. For a full table of the contents stored in the audit logs, refer to Table 1 below.

Data Element(s)	Purpose of Collection	Purpose of Storage	How data is used for purpose identified	Retention Period (how long does Anakam, Inc. keep this information)
Name	To verify identity.	To conduct system management and to generate usage statistics / troubleshooting for customers of the IDP Service.	This data is used to generate knowledge based questions from commercial identity verification information collected by third-party companies from financial institutions, public records, and other service providers.	Audit logs of IDP transactions are first stored in the IDP Service's live database for three months. They have updated timestamps and remain fully accessible by the IDP Service's operating system during that time. After three months, the audit logs are archived for an additional seven years. They are maintained in a frozen state, inaccessible by the IDP Service's operating system, and must be pulled from the archive's backup system.
Address of Residence				
DOB				
SSN (if optionally provided)				
The questions asked of the HSIN registrant				
Whether the registrant got the answers correct				
The scores generated during the proofing process				
Business rules which were triggered during the transaction				

Table 1: Data Elements Stored in IDP Service Audit Log

System Management

During system management, the IDP Service analyzes the performance of the functions of its system through logistic regression model tuning. The IDP Service's functions rely on models that leverage different types of data from its various sources when verifying an individual's identity. These models require refinement, or tuning, from time to time, to ensure that the automated system is properly weighting and using different aspects of the identity data. During such tuning, all PII data derived from audit logs is anonymized and aggregated prior to use. Anonymization is defined as the act of permanently and completely removing personal

identifiers from data. Anonymized data is data that can no longer be associated with an individual in any manner. Once this data is stripped of personally identifying elements, those elements can never be re-associated with the data or the underlying individual. This means that during system management, the PII held in audit logs cannot be attributed to any, single person.

Customer service usage statistics

When developing and providing usage statistics and conducting troubleshooting the IDP Service acts at the request of the HSIN PMO to provide aggregate statistics on system performance to the customer for research, performance measures, and reporting on the quality of the services the customer is receiving from the IDP Service. Generation of usage statistics and troubleshooting will always require initiation from the customer; the IDP Service will not otherwise access the audit logs. HSIN PMO intends to request usage statistics from the IDP Service on no more or less than a quarterly basis. Neither the HSIN PMO nor DHS can receive an individual's PII when receiving usage statistics or troubleshooting results – any data provided in reports will be in the aggregate and anonymous.

The IDP Service ensures, under contract, that none of the information provided by registering HSIN users is shared, sold, or distributed beyond the scope of system maintenance or customer usage statistics, as described above. Neither the HSIN PMO, nor DHS, have the ability to request or collect any of the information maintained by the IDP Service in its audit logs or otherwise.

Reason for the PIA Update

Since completion of the July 2012 HSIN R3 User Accounts PIA, the HSIN PMO has received additional, clarifying information from the IDP Service regarding the full contents of its identity verification session audit logs and how long such logs are maintained.

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.

Authorities and Other Requirements

Authorities have not changed from the original HSIN PIA.

Characterization of Information

Prior to registering for a new account with HSIN, all registrants must process through an IDP Service to verify their identity. Registrants must submit information to verify their identity prior to being granted an account within HSIN.

HSIN PMO now clarifies that, in order to generate its knowledge-based questions, the IDP Service requests and collects basic PII from the individual including: home street address, home city, home state, home postal code, home phone number (if provided), date of birth, and Social Security number (if provided). In addition to this information, the first and last name of the registrant is sent to the IDP Service from DHS. These data elements are collected by the IDP Service in order to "match" the information from the registrant with the information already owned by the IDP Service. This IDP Service is used to identify data consistencies and ultimately, verify the identity of the registrant. Registrants provide this PII by using a DHS Account Registration form. That form, itself, sits on a DHS site. However all PII that is collected for the identity proofing section of the form is sent directly to the IDP Service, along with the registrant's first and last name. DHS does not store or retain the information collected in the identity proofing section of the DHS Account Registration form. Individuals provide this information from a .gov domain and it is passed directly to the IDP Service. The SSN, address of residence, date of birth, and home phone number will not be stored by HSIN or the HSIN PMO at any time, for any purpose during identity verification.[5]

HSIN PMO also clarifies that the IDP Service maintains an audit log of all identity verification transactions. Audit logs are maintained by the IDP Service to conduct system management and to generate customer usage statistics. The log includes information submitted by the user (name, address, date of birth, and if provided, the individual's SSN and home phone number), the questions asked of the user, whether the users got the answers correct, the scores generated during the proofing process, and the business rules that were triggered during the transaction.

Uses of the Information

Information	DHS Use	IDP Use
Name, address of residence, date of birth, Social Security number	Although individuals use a DHS form to provide this information, it is passed directly to the IDP Service. DHS does	To generate knowledge-based questions for a quiz from commercial identity verification information.

[5] HSIN will require individuals to verify their identity through the IDP Service and providing a SSN enhances the ability of the IDP Service to generate knowledge-based questions.

Information	DHS Use	IDP Use
(optional), phone number	not retain this information.	
Commercial identity verification information	DHS does not have access to, nor does it retain, this information.	To generate knowledge-based questions.
Knowledge based questions, responses to questions	DHS displays the knowledge-based questions generated by the IDP Service on a .gov domain and passes the responses to these questions directly to the IDP Service. DHS does not store the questions or responses to the questions.	To conduct system management and to generate usage statistics / troubleshooting for customers of the IDP Service.
Audit log (name, address, date of birth, and if provided, the individual's SSN and home phone number), the questions asked of the user, whether the users got the answers correct, the scores generated during the proofing process, and the business rules that were triggered during the transaction.	None – DHS does not have access to this information.	To conduct system management and to generate usage statistics / troubleshooting for customers of the IDP Service.
HSIN registration information (post identity verification)	By retaining the user's profile, other members can benefit from his or her contributions, understand the user's qualifications and expertise for context, and judge the accuracy of the information contributed. Additionally, the retention of users' profiles permits the community to contact them in reference to that particular subject matter and their declared expertise through job changes and reassignments.	None – the IDP Service does not have access to this information from the HSIN registration form post identity verification.

Information	DHS Use	IDP Use
HSIN Nomination Form – name, email, phone number (if provided) (executed by a registered HSIN account holder – nominating a qualified individual into the system)	Pre-populates the "CONTACT" tab information in the HSIN Account Profile page, see Figure 3 above.	None – the IDP Service does not have access to this information from the HSIN Nomination Form.

Table 2: Uses of Information

Audit logs of IDP transactions are first stored in the IDP Service's live database for three months. They have updated timestamps and remain fully accessible by the IDP Service's operating system. After three months, the audit logs are archived for an additional seven years. They are maintained in a frozen state, inaccessible by the IDP Service's operating system, and must be pulled from the archive's backup system.

During system management, the IDP Service analyzes the performance of the functions of its system through logistic regression model tuning. This tuning is simply a performance analysis activity that allows the IDP Service to more closely align to and re-adjust applications, functionalities, or designs in order to better serve its customer base. The IDP Service's functions rely on models that leverage different types of data from its various sources when verifying an individual's identity. These models require refinement, or tuning, from time to time, to ensure that the automated system is properly weighting and using different aspects of the identity data. During such tuning, all PII data derived from audit logs is anonymized and aggregated prior to use. Anonymization is defined as the act of permanently and completely removing personal identifiers from data. Anonymized data is data that can no longer be associated with an individual in any manner. Once this data is stripped of personally identifying elements, those elements can never be re-associated with the data or the underlying individual. In other words, during system management, the PII held in audit logs cannot be attributed to any, single person – it is made anonymous.

When developing and providing usage statistics and conducting troubleshooting, the IDP Service acts at the request of its customer, in this case the HSIN PMO, to provide aggregate statistics on system performance to the customer for research, performance measures, and reporting on the quality of the services the customer is receiving from the IDP Service. Generation of usage statistics and troubleshooting will always require initiation from the customer - the IDP Service will not otherwise access the audit logs. HSIN PMO intends to request usage statistics from the IDP Service on no more or less than a quarterly basis. Neither the HSIN PMO nor DHS can receive an individual's PII when receiving usage statistics or

troubleshooting results – any data provided in reports will be in the aggregate and anonymous.

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.

Data Retention by the project

In order to generate its knowledge-based questions, the IDP Service requests and collects basic PII from the individual including: home street address, home city, home state, home postal code, home phone number (if provided), date of birth, and Social Security number (if provided). In addition to this information, the first and last name of the registrant is sent to the IDP Service from DHS. These data elements are collected by the IDP Service in order to "match" the information from the registrant with the information already owned by the IDP Service. This IDP Service is used to identify data consistencies and ultimately, verify the identity of the registrant. Registrants provide this PII by using a DHS Account Registration form. That form, itself, sits on a DHS site. However all PII that is collected for the identity proofing section of the form is sent directly to the IDP Service along with the registrant's first and last name. DHS does not store or retain the information collected in the identity proofing section of the DHS Account Registration form. Individuals provide this information from a .gov domain and it is passed directly to the IDP Service. The SSN, address of residence, date of birth, and home phone number will not be stored by HSIN or the HSIN PMO at any time, for any purpose during identity verification.[6] HSIN registrants move to the IDP Service's site to take the actual IDP Service quiz. The IDP Service maintains an audit log of all identity verification transactions. The log includes information submitted by the user (name, address, date of birth, and if provided, the individual's SSN and the home phone number), the questions asked of the user, whether the users got the answers correct, the scores generated during the proofing process, and the business rules which were triggered during the transaction. The sole purposes of maintaining the audit logs are to conduct system management and to generate usage statistics/troubleshooting for customers of the IDP Service.

Audit logs of IDP sessions are first stored in the IDP Service's live database for three months. This means they have updated timestamps and remain fully accessible by the IDP Service's operating system. After three months, the audit logs are archived for an additional

[6] HSIN will require individuals to verify their identity through the IDP Service and providing a SSN enhances the ability of the IDP Service to generate knowledge-based questions.

seven years. They are maintained in a frozen state, inaccessible by the IDP Service's operating system, and must be pulled from the archive's backup system.

Source	Information Stored	Information Not Stored
DHS	• Salutation • First Name • Middle Initial • Last Name • Suffix • Business Phone • Mobile Phone • Email • TFA Delivery Value 1 (required phone, email, or SMS) • TFA Delivery Value 2 (optional phone, email, or SMS) • TFA Delivery Value 3 (optional phone, email, or SMS) • Password • Security Question & Answer (x4)	• Home Address (street, city, state, postal) * • Date of Birth • SSN * • Country of Citizenship* • Fax* • Pager* • Other Phone* • Business Address* • Deployed Address*
IDP Service	• IDP Sessions o Name, address, date of birth, and if provided, the individual's SSN and the home phone number; o the questions asked of the user; o whether the users got the answers correct; o the scores generated during the proofing process; and o the business rules which were triggered during the transaction.	• Answers to the IDP Service questions

Table 3: Storage of Information

Information Sharing

The IDP Service ensures, under contract, that none of the information provided by registering HSIN users is shared, sold, or distributed beyond the scope of system maintenance or customer usage statistics, as described above. Neither the HSIN PMO, nor DHS, have the ability to request or collect any of the information maintained by the IDP Service in its audit logs or otherwise. Per the software license agreement with the IDP Service, both parties agree not to disclose confidential information given to them by the other party to any third party, absent a court order or other such requirement by law. Confidential information includes names and other such information that a reasonable person would consider to be confidential. IDP Service will not be able to share, sell, or distribute confidential information to any third party.

HSIN PMO intends to request usage statistics from the IDP Service on no more or less than a quarterly basis. Neither the HSIN PMO nor DHS, has the ability to receive any individual's PII when receiving usage statistics or troubleshooting results – any data provided will be in the aggregate.

Redress

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 System of Records Notice (77 FR 70792, November 27, 2012).

Auditing and Accountability

Audit logs of IDP transactions are first stored in the IDP Service's live database for three months. They have updated timestamps and remain fully accessible by the IDP Service's operating system. After three months, the audit logs are archived for an additional seven years. They are maintained in a frozen state, inaccessible by the IDP Service's operating system, and must be pulled from the archive's backup system.

During system management, the IDP Service analyzes the performance of the functions of its system through logistic regression model tuning. This tuning is simply a performance analysis activity that allows the IDP Service to more closely align to and re-adjust applications, functionalities or designs in order to better serve its customer base. The IDP Service's functions rely on models that leverage different types of data from its various sources when verifying an individual's identity. These models require refinement, or tuning, from time to time, to ensure that the automated system is properly weighting and using different aspects of the identity data. During such tuning, all PII data derived from audit logs is anonymized and aggregated prior to use. Anonymization is defined as the act of permanently and completely removing personal identifiers from data. Anonymized data is data that can no longer be associated with an individual in any manner. Once this data is stripped of personally identifying elements, those elements can never be re-associated with the data or the underlying individual. In other words, during system management, the PII held in audit logs cannot be attributed to any, single person – it is made anonymous. Logistical regression model updates occur infrequently. The last logistical model update occurred five years ago. The IDP Service has no update planned at this time.

When developing and providing usage statistics and conducting troubleshooting the IDP Service acts at the request of its customer, in this case the HSIN PMO, to provide aggregate statistics on system performance to the customer for research, performance measures, and

reporting on the quality of the services the customer is receiving from the IDP Service. Generation of usage statistics and troubleshooting will always require initiation from the customer - the IDP Service will not otherwise access the audit logs. HSIN PMO intends to request usage statistics from the IDP Service on no more or less than a quarterly basis. Neither the HSIN PMO nor DHS can receive an individual's PII when receiving usage statistics or troubleshooting results – any data provided in reports will be in the aggregate and anonymous.

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