Privacy Impact Assessment
for the

DHS Single Point of Service Request for Information Management Tool

DHS/ALL/PIA-044

June 17, 2013

Contact Point
Carl Gramlick
Director, DHS National Operations Center
Office of Operations Coordination and Planning
(202) 282-8000

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

Abstract

The Single Point of Service (SPS) refers to a joint effort between the Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), and the Office of Intelligence and Analysis (I&A) to provide a centralized DHS Headquarters location to receive, facilitate, process, and, in some circumstances, respond to operational or intelligence related "Requests for Information" (RFI) that originate from federal, state, local, tribal, and territorial entities. In order to perform this function, OPS and I&A employ the RFI Management Tool, which standardizes the process by which entities request operational or intelligence-related information. DHS is conducting this Privacy Impact Assessment because the RFI Management Tool collects, retains, and disseminates personally identifiable information.

Overview

The Department of Homeland Security is the primary federal source of accurate, actionable, and timely homeland security-related information for its federal, state, local, tribal, and territorial partners. To carry out this mission, among other components, the DHS Office of Operations Coordination and Planning (OPS) provides situational awareness and a common operating picture through its National Operations Center (NOC), which fuses law enforcement, intelligence, emergency response, private sector, and open-source reporting, and shares this information at the unclassified level through the Homeland Security Information Network (HSIN),[1] the [B-LAN] Homeland Secure Data Network (HSDN), and [C-LAN] Joint Worldwide Intelligence Communication System (JWICS). I&A further supports this departmental mission, by collecting, processing, analyzing, and disseminating homeland security-related information to its homeland security partners.

OPS and I&A have developed a coordinated business process, the Single Point of Service, to ensure that all operational and intelligence RFIs are responded to expeditiously and that there is accountability for this transactional activity. The RFI Management Tool serves as a means of recording and tracking requests, cataloging responses, which may in turn be disseminated to multiple Requestors with similar information queries, and ensuring enhanced coordination and effective oversight of this information sharing process.

The RFI Management Tool is one element of the DHS Common Operating Picture (COP). The DHS COP is a geospatial visualization tool designed to facilitate shared situational awareness across the homeland security enterprise that can display and integrate incoming information into a readily understandable format. It is a web-based, incident response and management system that provides all users with a secure, shared picture of unfolding incidents. The RFI Management Tool is the only element of the DHS COP that collects and maintains PII.

---

[1] HSIN is designed to facilitate the secure integration of information-sharing resources among federal, state, local, tribal and territorial, private sector, international and other non-governmental partners involved in identifying and preventing terrorism as well as in undertaking incident management activities. A privacy impact assessment for HSIN 3.0 Shared Spaces on the Sensitive but Unclassified Network, July 25, 2012, available at www.dhs.gov/privacy.

The Request for Information Process

DHS defines an RFI as "A request for operational or intelligence information validated for action by an SPS-RFI Manager and capable of being satisfied through the exploitation of existing databases, analysis, or collection." The SPS serves as DHS Headquarters centralized location to receive, track, and facilitate operational and intelligence RFIs. OPS/NOC is responsible for processing operational RFIs, which, generally speaking, are requests seeking information related to a situational awareness or a common operating picture, in the event of a natural disaster, act of terrorism, or other man-made disaster; or critical terrorism and disaster-related information. I&A is responsible for processing intelligence RFIs consisting of both raw and evaluated information of tactical, operational, or strategic value, including foreign intelligence and counterintelligence; or information requests originating from an Intelligence Community element.

The RFI Management Tool standardizes the processing of RFIs submitted to SPS. All information collected by the RFI Management Tool is necessary for the SPS to effectively receive, track, validate, coordinate, and respond to an RFI. When an RFI is submitted for action, the SPS records the PII of the individual submitting the request (i.e., the "Requestor"), which includes: name, telephone number, email address, and agency he or she represents. The RFI itself may also contain the PII of a person of interest. SPS also records the substance of the request in the tool.

RFIs typically ask for additional PII on persons of interest, such as name, date of birth, citizenship, immigration information, law enforcement information, and other identifying information. After an RFI is validated, the request is sent to the "Action Agency" (i.e., the custodian of the requested information). The Action Agency then releases only the requested information to either the RFI requestor or the SPS which, in turn, disseminates the response to the Requestor. The original RFI is kept as an attachment in the RFI Management Tool. The following types of information are maintained by the RFI Management Tool:

- Requestor information (such as name, organization to which the person is assigned, and contact information),
- The original request and all associated documentation, which may include PII.
- Depending on the nature and scope of the RFI, the response may also be stored in the RFI Management Tool.
- Information pertaining to the review/approval of an RFI from the Offices of General Counsel, Privacy, Civil Rights/Civil Liberties, Intelligence Oversight, and Public Affairs.
- Action Agency information including the responding person, his or her organization, contact information, and whether the response was sent directly back to the requesting agency or through SPS.

RFIs are categorized into the following types:

- ***Amplifying Information*** – A request for additional information that was originally contained in a raw or finished report.

- ***Tearline*** – Tearlines are portions of an intelligence report or product that provide the substance of a more highly classified or controlled report without identifying sensitive sources, methods, or other operational information. Tearlines release classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification.[2]

- ***Exercise*** – An RFI in support of a DHS exercise.

- ***Identity Request*** – A request to have a U.S. Person ("USPER") identified, whose identity was minimized in a raw or finished intelligence report.

- ***Intelligence Support*** – A request for an assessment or analytical support from a member of the Intelligence Community.

- ***Name Trace*** – A request to search one or more databases for information on a named individual with a nexus to terrorism.[3]

- ***Other*** – A request that falls outside the scope of the RFI process and is logged for tracking purposes only. Depending on the request's nature and scope, it will either be transferred to an organization capable of providing a response or closed.

- ***Statistics*** – A request for demographic or law enforcement information (such as arrests or seizures) on unnamed individuals during a specified time period.

- ***Translation*** – A request to have written or electronic media translated from one language to another.

- ***Watch Support*** – A request for immediate or short-suspense requirements for an Operational assessment or Operational support.

---

[2] Office of the Director of National Intelligence "Intelligence Community Directive 209: Tearline Production and Dissemination" (September 6, 2012).

[3] All "name trace" RFIs have a nexus to terrorism, and therefore receive both an RFI and NOC tracking number and, in some instances, are forwarded to the National Operations Center Operations Counterterrorism Desk (NCOD). For a detailed description of the NCOD process, please see the DHS/OPS/PIA-009 National Operations Center Operations Counterterrorism Desk Database PIA, available at www.dhs.gov/privacy. Within the SPS Management Tool, a copy of name trace RFIs as received, are kept in accordance with NARA/OPS records schedule N1-563-08-023. However, as stated in the DHS/OPS/PIA-009, the results of name trace RFIs are not stored in the SPS Management Tool. The NCOD only informs the Validation Office that a name trace RFI has been answered and that the RFI can be closed.

RFI Validation Process

Prior to submitting an RFI to DHS for assistance, the Requestor must exhaust local sources of information. This step is verified by a specific entry in the tool, in which the resources already examined are identified. (In some cases, based on the subject of the query, it will be apparent that no local resources were available.)[4] The tool also requires Requestors to provide a "detailed description of the precise information requested" to ensure that the request is answered as accurately as possible. A separate query asks whether the request contains U.S. person information and another seeks information on the intended recipients of the information. These questions help OPS and I&A ensure that the request is handled consistent with federal legal requirements, including the Privacy Act and Executive Order 12333.

Generally speaking, federal agencies and DHS components route their requests through their respective headquarters elements, which validate the requests prior to submission. Similarly, state and local partners route their requests through fusion centers, which validate them. DHS defines validation as "[a] multi-level review conducted by RFI Managers to ensure: 1) the RFI falls within the Department's authorities; 2) the RFI complies with the laws, regulations, and policies governing information sharing and the dissemination of classified or otherwise controlled information; 3) the RFI is capable of being satisfied through the exploitation of existing databases, reporting, analysis, and/or collection; 4) the requested information can be legally gathered by a state, local, territorial, tribal ("SLTT"), or other federal entity; and 5) the individual and/or organization submitting the RFI possesses a valid "need to know."

In a typical RFI transaction, a Requestor will submit a completed DHS Form 10058 "Request for Information" Form to the SPS via email or directly into the RFI Management Tool. Upon receipt, the RFI Manager will enter the request into the RFI Management Tool in which it will automatically be assigned an RFI tracking number. After verifying the request contains the required information, the SPS desk forwards the RFI to appropriate OPS or I&A Validation Office personnel for review.

The Validation Offices examine every RFI to ensure: 1) the RFI falls within the Department's authorities; 2) the RFI does not violate existing policies governing information sharing or the dissemination of controlled information; 3) the requested information/support can be legally gathered by a federal, state, local, territorial or tribal entity; 4) the Requestor has exercised due diligence by exhausting all local sources of information associated with satisfying the request; and 5) the Requestor possesses a valid "need to know." RFIs not meeting the validation criteria are returned to the Requestor for additional clarification. After clarification, if the Validation Office determines that an RFI is still invalid, the Validation Office records only the RFI tracking number for program management purposes and deletes the content of the RFI to avoid maintaining any inappropriate PII.

[4] A query that would involve access to immigration records, for example, could only be answered by research into federal data sources.

Once a request has been validated OPS and/or I&A personnel check existing data in the RFI Management Tool to determine if there is any previous reporting on the subject and whether the request can be answered from existing resources. If the request cannot be answered at HQ DHS, the next step is to ask the agency most capable of responding to the request ("Action Agency(ies))" for assistance in responding. The Action Agency may be a federal agency, DHS component, or state and local fusion center, depending on the nature and scope of the RFI. Also depending on the nature and scope of the RFI, the Action Agency will either disseminate the response directly to the RFI Requestor or submit the response to the RFI Management Tool from which it is disseminated by SPS personnel. In either case, the RFI Management Tool is annotated with the status of the request. The original RFI is kept as an attachment in the RFI Management Tool.

It is important to note, as a matter of policy, RFIs are not considered to be "tasking" another agency; rather, they are considered "requests" to an agency for possible action (i.e., "asking not tasking"). SPS RFI managers and validation personnel are responsible for monitoring all open requests and performing the required follow-up actions to ensure the RFI is answered in a timely manner. All these actions are recorded in the RFI Management Tool.

In some cases, review or approval of the RFI requires input from the Offices of General Counsel, Privacy, Civil Rights/Civil Liberties, Intelligence Oversight, and/or Public Affairs. The results of this review or approval are documented in the RFI Management Tool. The Tool also includes information about the Action Agency, including who responded, his or her organization, and contact information.

The RFI Management Tool includes a robust metrics and reporting capability to measure the effectiveness of SPS processes and response rates from all federal, state, and local customers. Internal reports are produced summarizing data on the organizations submitting requests, the types of requests being submitted, the Action Agencies responding to the requests, and organizational responsiveness. These reports do not typically contain PII and are not disseminated outside of DHS Headquarters.

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The following authorities support the collection of information in the RFI Management Tool:

- 6 U.S.C. § 321d (OPS).
- The National Security Act of 1947, as amended (I&A), 50 U.S.C. § 401 et seq.
- The Homeland Security Act of 2002, as amended, Title II (I&A), 6 U.S.C.A. § 121.
- Executive Order No. 12333, as amended (I&A).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The collection of personally identifiable information maintained in the RFI Management Tool is described by the following SORNs:

- DHS/IA-001 Enterprise Records System (ERS), May 15, 2008, 73 FR 28128.
- DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN, November 15, 2010, 75 FR 69689.

To the extent that the RFI Management Tool contains data from other DHS components or other agencies that is responsive to an RFI, that data is covered by the SORNs for those source systems.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The RFI Management Tool uses HSIN 3.0 for access authentication.[5] The HSIN Program Management Office (PMO) has developed a HSIN 3.0 System Security Plan (SSP) in full compliance with DHS Sensitive Systems Policy Directive 4300A, and received a final authorization to operate (ATO) on July 20, 2012.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The RFI records retained in the Management Tool are covered under NARA/OPS records schedule N1-563-11-10-2 and have either a five (5) year retention period or, in the case of an RFI pertaining to a phase 2 or 3 event,[6] is a permanent record. I&A RFI records are covered by schedule N1-563-07-16-5, and are maintained for 10 years after the end of the year in which the RFI was submitted.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Both OPS and I&A information collections are excepted from the PRA requirements due to their respective law enforcement investigatory and intelligence activities.

---

[5] A PIA for HSIN 3 was published on July 25, 2012.
[6] An event meeting any of the four criteria outlined in Homeland Security Presidential Directive-5.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The RFI Management Tool maintains all information regarding the status and processing of an RFI. It collects information on the individual submitting the request (the Requestor), which includes: name, telephone number, email address, and agency he or she represents. The specific information requested in an RFI, which may or may not include PII, is also recorded. This may consist of identifying information about third parties, such as full name, citizenship, immigration status, and any law enforcement or national security nexus. The RFI Management Tool may also contain information that is responsive to the request, such as a person's name, date of birth, citizenship, immigration information, law enforcement information, and other identifying information.

The tool maintains information about the request and its compliance with DHS requirements for RFIs. It also records any internal coordination, such as with the Office of the General Counsel or other oversight offices, as well as Action Agency information, i.e., the agency and individual responding and contact information. Information that responds to the query is also maintained in the tool, making it available (provided a user has the appropriate role and permission) for subsequent queries when the same information is responsive.

2.2 What are the sources of the information and how is the information collected for the project?

Information in the RFI Management Tool may be acquired from the Requestor, and/or the agency responding to the request. The RFI Management Tool relies on the system(s) containing the original information to provide accurate data. Information is entered into the RFI Management Tool by DHS-SPS RFI Managers.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The RFI Management Tool will contain commercial or publicly available data only to the extent that the data are already contained in records maintained by Action Agencies, subject to their respective authorities, policies, and procedures, are responsive to the RFI, and are submitted through the Tool for response to the Requestor. For example, ICE may serve as the action agency for an RFI pertaining to an illegal immigrant. ICE agents and officers may use public and commercial data to identify residences, criminal relationships, or law enforcement activity related to the individual. This public/commercial information could then be passed to the Requestor. A copy could also be maintained in the RFI Tool if ICE responds by using the Tool.

2.4 Discuss how accuracy of the data is ensured.

Information Requestors are presumed to submit information that is as accurate as possible. Action Agencies likewise are presumed to be sharing accurate information. Data are entered directly by users, which should reduce errors in transcription. A dedicated Performance Management Manager (assigned to the I&A Support Branch) will also review the data to insure its integrity.

The RFI Management Tool reflects data submitted by other agencies and entities, which are presumed to provide accurate data. SPS personnel first examine existing holdings to determine if a query can be answered with the information that is already maintained within the Tool. Part of the decision-making process in this regard is an assessment of whether the existing information is accurate for purposes of the query. If not, or if no information exists that responds to the query, SPS personnel seek out Action Agencies for assistance.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Information stored in the RFI Management Tool is not collected directly from the subject individuals (beyond Requestor-identifying data, which is presumed to be accurate); therefore there is a risk that the data in the RFI Management Tool could be incomplete or inaccurate.

Mitigation: The RFI Management Tool reflects data submitted by other agencies and entities, which are presumed to provide accurate data. Nevertheless, SPS personnel search DHS databases to confirm, to the extent possible, the accuracy of the information submitted. Similarly, responses from Action Agencies are presumed to reflect correct data, but review of the submissions and general oversight of the responses conducted by SPS personnel helps to mitigate this potential risk.

Privacy Risk: The RFI Management Tool could present a risk of the over-collection of PII or the excessive aggregation of disparate PII from separate agency systems.

Mitigation: The respective OPS and I&A Validation Office(s) examine every RFI to ensure: 1) the RFI falls within the Department's authorities; 2) the RFI does not violate existing policies governing information sharing or the dissemination of controlled information; 3) the requested information/support can be legally gathered by a federal, state, local, territorial or tribal entity; 4) the Requestor has exercised due diligence by exhausting all local sources of information associated with satisfying the request; and 5) the Requestor possesses a valid "need to know." RFIs not meeting the validation criteria are returned to the Requestor for additional clarification. After clarification, if the Validation Office determines that an RFI is still invalid, the Validation Office records only the RFI tracking number for program management purposes and deletes the content of the RFI to avoid maintaining any inappropriate personal information.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The RFI Management Tool uses the contact information from the Requestor and the Action Agency to manage RFI submissions and responses. It uses the substance of the information request, which may include PII, to scope the RFI response appropriately and as a repository of information to respond to subsequent requests on the same issue. The SPS may collate RFI responses on the same topic, but it does not alter them.

The RFI Management Tool also aggregates statistical data on the RFI process to generate performance management reports. These performance reports assist OPS and I&A to prioritize needs, identify process improvements, evaluate potential courses of action, and assess the impact of operating decisions. Moreover, the RFI Management Tool records significant actions taken to process an RFI. This information may be used by OPS/I&A management or other offices with oversight responsibility for employee conduct or system security to review the actions of account holders and to investigate any allegations or indications of system-related misuse or misconduct by users of the RFI Management Tool.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. I&A and OPS have access to the system as RFI Managers. DHS Requestors have the ability to submit an RFI and execute the required queries to effectively manage their submissions, provided they have been assigned a role appropriate for this purpose. OPS/I&A personnel assign these roles. Action Agencies within DHS will have the ability to query and review all RFIs they have accepted for action as well as RFIs they have submitted to DHS-SPS for action.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that RFIs will be tasked to OPS or I&A outside the scope of their authorities, and thus result in distribution of PII in the RFIs that DHS should not maintain.

Mitigation: This privacy risk is mitigated through validation of all RFIs by the Validation Offices. The RFIs are reviewed to ensure: 1) the request falls within the respective OPS or I&A authorities; 2) the request does not violate existing policies governing information sharing or the dissemination of controlled information; 3) the requested information can be legally gathered by a federal, state, local, territorial or tribal entity; 4) the Requestor has exercised due diligence by exhausting all local sources of information associated with satisfying the request; and 5) the Requestor possesses a valid "need to know." RFIs that are not validated are returned to the submitter for additional clarification and/or purged from the system.

Privacy Risk: There is a privacy risk of misuse or unauthorized access to the information.

Mitigation: To mitigate this risk, access to the RFI Management Tool is strictly controlled. Roles are assigned by I&A and OPS. All users must receive a HSIN password. Authentication and role-based user access requirements ensure that users can only access or change information that is appropriate for their official duties. The effectiveness of authentication and security protections are verified through analyses of system operation and usage. Unauthorized use of the RFI Management Tool will result in the suspension of a user's access. Further, the SPS is located in a Sensitive Compartmented Information Facility (SCIF) with access limited to those who have been preapproved.

Audit trails are created throughout the process and are reviewed if a problem or concern arises regarding the use or misuse of the information. At log-in to the system, the user acknowledges consent to monitoring or is required to log off.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Requestors who use the RFI Management Tool input their own PII directly into the Tool. A Privacy Act Statement is provided during HSIN log-on. Individuals who are the subjects of requests, however, do not have specific notice of such collection, because direct notice to these individual at the time of a RFI search could undermine the law enforcement mission that animates RFIs.

This PIA, nevertheless, serves as public notice of the existence, contents, and uses of the RFI Management Tool. In addition, notice of the original collection of information and its maintenance in an underlying government system is described in the individual PIAs and SORNs for those systems or in other privacy-related documentation. Individuals may be provided notice via Privacy Act Statements or other privacy notices at the original points of collection, or via

published SORNs for the underlying systems, which typically include a routine use describing how information may be shared with law enforcement entities.

As part of this PIA process, DHS reviewed the applicable SORNs to ensure that the operational uses were appropriate given the notice provided and purpose of the system(s). Information that comes from SLTT partners through a fusion center must comply with the privacy policies for that fusion center or with other, applicable state privacy requirements.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The RFI Management Tool does not collect information directly from individuals who are the subjects of inquiries. Information is collected directly from Requestors who are presumed to provide it voluntarily. As such, there are no opportunities for the individuals to consent to uses or for individuals to decline to provide information or opt out of the project.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: The RFI Management Tool does not collect information directly from the subjects of requests, so those individuals do not have notice that their information may be used by the SPS.

Mitigation: General notice about the RFI Management Tool is provided through this PIA and by publication of the corresponding SORNs, DHS/IA-001 - Enterprise Records System (ERS), 73 FR 28128 (May 15, 2008), and DHS/OPS-003 - Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, 75 FR 69689 (November 15, 2010), which cover the collection of information.

Section 5.0 Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The records are retained under NARA/OPS records schedule N1-563-11-10-2 and are retained for five (5) years or, if an RFI becomes part of a phase 2 or 3 event, permanently.

Intelligence records fall under schedule N1-563-07-16-5. I&A retains RFIs and their associated responses for 10 years after the end of the year in which the RFI was submitted. These records are retained for use in conducting I&A's authorized intelligence and information sharing activities.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk of retaining information longer than is necessary for any specific RFI.

Mitigation: Although there is always risk inherent in retaining PII for any length of time, the data retention period for the RFI Database is based on operational needs and is consistent with the concept of retaining PII only for as long as necessary to support the agency's mission. Within the DHS-SPS, I&A will be responsible for purging all RFIs validated by I&A and OPS will purge all RFIs validated by the NOC.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local governments, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes, the main mission of the RFI Management Tool is to serve as the primary point of contact for other agency partners to submit RFIs to DHS, contribute information that responds to them, and receive responses to their RFIs. Provided they have been given a user role, external partners are able to submit a request to SPS directly through the Management Tool to obtain the results. These reports are used by the requesting agencies in the furtherance of their particular missions. All RFIs are validated to ensure that they are made in furtherance of a lawful government function and are based on a reasonable belief of a potential or actual threat to homeland security or from terrorism.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Each of the two SORNs that cover the information in the RFI Management Tool contains routine uses that allow for external sharing. These SORNs are available at http://www.dhs.gov/system-records-notices-sorns. The routine uses are compatible with the OPS and I&A missions because DHS is required by law and executive order to share intelligence and information with a nexus to homeland security. Specifically, the Homeland Security Act of 2002 established DHS, in part, to improve the sharing of information among federal, state, and local government agencies and the private sector. In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 required the President to establish the Information Sharing Environment (ISE) to facilitate the sharing of terrorism information among all appropriate federal, state, local, tribal, and private sector entities, through the use of policy guidelines and technologies. Executive Order 13388, *Strengthening the Sharing of Terrorism Information to Protect Americans* (August 27, 2004), also directed agencies to give the "highest priority" to the prevention of terrorism and the "interchange of terrorism information [both] among agencies"

and "between agencies and appropriate authorities of States and local governments." Without the sharing outlined in these routine uses, OPS and I&A would be unable to comply with these laws and the Executive Order.

6.3 Does the project place limitations on re-dissemination?

Requestors can query the RFI Management Tool to see if an RFI on a particular subject or event has already been submitted. However, in order to view the response, the Requestor must first submit a request (containing the appropriate justification/intended recipients) to SPS for validation and approval from the Action Agency to further disseminate the response.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

An electronic record of the date, nature, and purpose of each disclosure from the RFI Management Tool, and the name and address of the individual or agency to which information is disclosed, is kept in the RFI Management Tool. The RFI Management Tool can be audited.

6.5 Privacy Risk Analysis: Related to Information Sharing

Privacy Risk: There is a potential risk of RFIs and their responses being improperly disclosed, misused, lost, or further disseminated by the receiving agencies with which DHS shares information.

Mitigation: Requestors – and the Validation Offices – control access to their requests and can limit who sees the requests and associated responses. In cases where there may be disagreement between the Requestors and the Validation Offices regarding further dissemination, the parties will consult to reach agreement. Additionally, agency personnel who provide responses have been trained on proper use of law enforcement sensitive information and understand that they may only provide the information to those who have a need to know. RFI responses are shared with Requestors and/or others with access to the RFI Management Tool, provided the Requestor has agreed to such access. Finally, all sharing is consistent with the routine uses enumerated in DHS SORNs: DHS/IA-001 - Enterprise Records System (ERS), May 15, 2008, 73 FR 28128, and DHS/OPS-003 - Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, November 15, 2010, 75 FR 69689.

Privacy Risk: There is a privacy risk that the SPS may inappropriately share PII externally in response to a RFI.

Mitigation: This risk is mitigated through the validation process for RFIs, which ensures that the request falls within the Department's authorities, does not violate existing policies governing information sharing or the dissemination of controlled information, is for information that can be legally gathered by a federal, state, local, territorial or tribal entity, and the Requestor possesses a valid "need to know." In the event that SPS personnel are uncertain whether an RFI is valid, they may request additional information from the Requestor or review from the OPS or I&A Privacy Offices, the DHS Privacy Office, the DHS Office for Civil Rights and Civil

Liberties, the DHS Intelligence Oversight Officer, and/or the Office of General Counsel-Intelligence Law Division. For RFIs that pertain to USPER information, the SPS tags the RFI as pertaining to USPER, thus facilitating compliance with Intelligence Oversight requirements.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to any record containing information that is part of a DHS system of records, or seeking to contest the accuracy of its content, may submit a Freedom of Information Act (FOIA) or Privacy Act (PA) request to DHS. Requests will be processed under both FOIA and PA to provide the Requestor with all information that is releasable. Given the nature of some of the information in the RFI Database (sensitive law enforcement or intelligence information), FOIA and PA exemptions may apply and individual may not be permitted to gain access to or request amendment of his or her record.

Notwithstanding the applicable exemptions, DHS reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of DHS in accordance with procedures and points of contact published in the applicable SORN. Instructions for filing a FOIA or PA request are available at http://www.dhs.gov/foia.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Although records in the RFI Management Tool are exempt from access and amendment pursuant to exemptions published for each of the underlying systems, when amending these otherwise exempt records would not interfere with or adversely affect the purpose for collecting the records (e.g., intelligence or homeland security purposes), DHS may waive the exemptions on a case-by-case basis. Individuals can submit access requests, as described above, in order to ascertain whether the RFI Management Tool contains records about them.

7.3 How does the project notify individuals about the procedures for correcting their information?

Notification is provided by this PIA as well as in the DHS/IA-001 - Enterprise Records System (ERS) May 15, 2008, 73 FR 28128, and DHS/OPS-003 - Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion November 15, 2010, 75 FR 69689

SORNs. Notice for access, amendment, and correction, to the extent it is available, is also provided by the underlying source system SORNs.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: The privacy risk is that an individual may not be afforded adequate opportunity to correct information.

Mitigation: To mitigate this risk, individuals are afforded the opportunity to request access or amendment of their records by either submitting a FOIA or a PA request as outlined above. DHS will consider each request for access to records on a case-by-case basis to determine whether or not information may be released.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Privacy protections include strict access controls, including passwords and auditing that tracks access to electronic information. Access to the RFI Management Tool at the unclassified level is only granted if the user possesses a valid HSIN account and government email address and only upon verification by the Validation Offices. Access to the tool on B-LAN (Secret) and C-LAN (Top Secret) is incumbent on users having the appropriate security clearances to access the tool. Once access to the tool is granted, role-based user access requirements ensure users can only access or change information that is appropriate for their official duties. The effectiveness of authentication and security protections is verified through periodic analyses of system operation and usage. DHS employees may be subject to discipline and administrative action for unauthorized use or disclosure of this information.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All RFI Management Tool Users receive instruction on how to complete, submit, and respond to an RFI. All RFI Managers are trained on the management of RFIs and are required to denote PII/USPER information contained in an RFI as part of the validation process. All DHS employees, contractors, and other personnel receive initial privacy training within 30 days of onboarding. Additionally, all DHS employees and contractors are required to follow DHS Management Directive (MD) Number: 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, January 6, 2005. This guidance controls the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information. All employees and contractors are required to follow Rules of Behavior contained in the DHS Sensitive Systems Handbook. Also, all DHS employees are required to take annual computer security training, which includes privacy training on appropriate use of sensitive data

and proper security measures. I&A personnel are also required to attend annual classroom training on intelligence oversight procedures and how these are to be implemented in I&A.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to the RFI Management Tool will be granted to individuals based on the fact they are either submitting or responding to an RFI. Procedures for granting individual access to the tool are covered in section 8.1. Privacy protections include strict access controls, including passwords and auditing that tracks access to electronic information. Authentication and role-based user access requirements ensure that users can access or change only information that is appropriate for their official duties. The effectiveness of authentication and security protections is verified through audits of system operation and usage. DHS employees and contractors with access may be subject to discipline and administrative action for unauthorized use or disclosure of this information.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

N/A.

Responsible Officials

Carl Gramlick
Director, National Operations Center
Office of Operations Coordination and Planning
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