Privacy Impact Assessment
for the

DHS Single Point of Service Request for Information Tool

DHS/ALL/PIA-044(a)

March, 21, 2017

<u>Contact Point</u>
Ronald Shipman
Chief, Collections Management
(202) 447-4607

<u>Reviewing Official</u>
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 (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 (PIA) because the RFI Management Tool collects, retains, and disseminates personally identifiable information (PII). DHS is updating and reissuing the SPS-RFI PIA, originally published in June 2013, in order to better identify the potential privacy risks and mitigations associated with the use of both an unclassified and an accredited classified instance of the application. The 2013 PIA only dealt with an unclassified instance of the application.

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 (OPS) and the Office of Intelligence and Analysis (I&A) have developed a coordinated business process, the Single Point of Service (SPS), to ensure that all operational and intelligence Requests for Information (RFI) receive expeditious responses 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 the information sharing process. DHS is updating and replacing the SPS-RFI-PIA, originally published in June 2013, in order to better identify the potential privacy risks and mitigations associated with the use of both an unclassified and an accredited classified instance of the application. The 2013 PIA only dealt with an unclassified instance of the application.

The RFI Management Tool is one element of the DHS Common Operating Picture (COP)[1]

[1] The DHS COP is a geospatial visualization tool that can integrate incoming information related to specific incidents or geographic areas, and display it in a readily understandable format that is designed to facilitate shared situational awareness across the homeland security enterprise. It is a web-based incident response and management

hosted within the Geospatial Information Infrastructure (GII)[2] accreditation boundary on the [A-LAN] Sensitive but Unclassified network and within the Mission Application Virtualization Platform (MAVP) on the [C-LAN] Joint Worldwide Intelligence Communication System (JWICS). The RFI Management Tool is an application that serves as a method by which stakeholders can request access to information held by DHS or other participating organizations for an authorized purpose. The RFI process is executed by OPS and I&A under the DHS SPS Desk. The SPS Desk serves as the single ingest point for all operational and intelligence related RFIs.

The RFI Management Tool collects and maintains all information regarding the status and processing of a RFI, including information on individuals submitting the request (the Requestor), as well as the specific information requested in a RFI, which may or may not include PII. The RFI application may also contain information that is responsive to the request, such as a person's name, date of birth, citizenship, immigration information, law enforcement, and other identifying information. It also records any internal coordination, such as with the Office of the General Counsel (OGC) or other oversight offices (e.g. the DHS Privacy Office (PRIV) and Office of Civil Rights and Civil Liberties (CRCL)), as well as Action Agency information, (i.e., the agency and individual responding and contact information). Depending on the nature and scope of the RFI, information provided in response to a query may also be maintained in the Tool, making it available (provided a user has the appropriate role and permissions) for subsequent queries when the same information is responsive. Depending upon the nature and type of RFI, the information may be routed to relevant DHS components, and in certain cases, other state, local, tribal, and federal agencies.

At the application's user level, all access and authentication is role-based to ensure users can only access or change information pertinent to their official duties. Audit trails are created throughout the process and are reviewed by the development team on a regular basis. Upon logging in to the system, the user acknowledges consent to monitoring or is denied access to the tool.

The Request for Information Process

The SPS serves as DHS Headquarters' centralized location for receiving, tracking, and facilitating the processing of operational and intelligence RFIs. The OPS National Operations Center (NOC) is responsible for processing operational RFIs, which are requests seeking information related to a natural disaster or a disaster-related issue; a man-made emergency or

system that provides all users with a secure, shared picture of unfolding incidents.

[2] Geospatial Information is data derived from, among other things, remote sensing, mapping, and surveying techniques; and mapping, geodetic data, and related products.

disaster; or an act of terrorism or terrorism-related information.[3] 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 organization/agency.

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 a RFI. When a RFI is submitted for action, the SPS records the PII of 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 a 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 individual 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 actual response may also be stored in the RFI Management Tool.
- Information pertaining to the review/approval of a RFI from OGC, PRIV, CRCL, Intelligence Organization (IO), and the Office of Public Affairs (OPA).
- Action Agency information, including the responding person, his or her organization, his or her 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

[3] According to 28 C.F.R. § 0.85, terrorism-related information is information associated with "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

sensitive sources, methods, or other operational information. Tearlines release classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification.

- ***Exercise*** – A 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.
- ***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.
- ***Bulk Data Request*** – A request for a large number of DHS records coming from an external Agency.

RFI Validation Process

Prior to submitting a RFI to DHS SPS 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. Additional queries ask for information of the intended recipients of the information and whether the request contains USPER information. These questions help OPS and I&A ensure that the request is handled in a manner consistent with federal legal requirements, including the Privacy Act of 1974[4], Executive Order 12333,[5] and the I&A Intelligence Oversight Procedures.[6]

[4] *See* the Privacy Act of 1974, 5 U.S.C. § 552a.

[5] *See* Executive Order No. 12333 – United States Intelligence Activities, 46 Fed. Reg. 59941 (Dec. 8, 1981), *available at* http://www.archives.gov/federal-register/codification/executive-order/12333.html.

[6] *See* Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (Jan. 19, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf.

The DHS SPS desk verifies and reviews the RFIs based on the roles designated within the RFI application. Federal agencies and DHS components route requests through their respective headquarters elements for validation prior to submission. Similarly, state and local partners route their requests through fusion centers for validation. DHS defines validation as "[a] multi-level review conducted by RFI Managers[7] 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" and job related requirement for the information."

In a typical RFI transaction, a Requestor from a DHS component, or a federal, state, local, or tribal partner that has been provided with role-based access, will submit a completed DHS Form 10058 "Request for Information" 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, which will automatically assign an RFI Tracking number. After verifying the request contains the required information, the SPS desk, acting as the Validation Office, determines whether the RFI request is valid. If it is determined that the request is not valid, the RFI SPS desk team members will cancel the RFI.

The DHS SPS desk's Validation Office examines 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" and job-related requirement for the information. RFIs not meeting the validation criteria are returned to the Requestor for additional clarification.

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 DHS HQ, the next step is to ask the agency most capable of responding to the request ("Action Agency(ies))" for assistance. Depending on the nature and scope of the RFI, the Action Agency may be a federal agency, DHS component, or state and local fusion center.[8] Also depending upon

[7] RFI Managers include the SPS Desk and I&A/OPS

[8] *See* https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

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 to the RFI Requestor. In either case, the RFI Management Tool is annotated with the status of the request. The original RFI, as well as an annotation of the response if it was in writing or in the form of a document/file, is kept as an attachment in the RFI Management Tool. The Tool also includes information about the Action Agency, including who responded, his or her organization, and contact information.

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 requiring"). SPS RFI managers and validation personnel are responsible for monitoring all open requests and RFI responses, as well as performing the required follow-up actions to ensure the RFI is answered in a timely manner. All of these actions are recorded in the RFI Management Tool. In some cases, review or approval of the RFI requires input from OGC, PRIV, CRCL, IO, and/or OPA. The results of this review or approval are documented in the RFI Management Tool.

The RFI Management Tool includes robust metrics and reporting capabilities 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 HQ.

Bulk Requests

When the SPS receives a RFI requesting a bulk data[9] transfer, the SPS submits the request to the Data Access Review Council (DARC). The members of the DARC consist of personnel from I&A and DHS oversight offices, including the Office of Policy, OGC, PRIV, CRCL, and IO. Additionally, the DARC coordinates requests with appropriate Mission Advocates,[10] as well as Senior Review Officials, Subject Matter Experts, and the Data Access Review Team. The DARC is the coordinated oversight and compliance mechanism for the review of departmental initiatives and activities involving the internal or external transfer of PII through bulk data transfers in support of the Department's national and homeland security missions. As such, the DARC ensures that

[9] *Bulk Data:* The collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided to the data recipient for the recipient to identify information of intelligence value within it.

[10] Mission Advocates are Components or offices within or elements of Components whose operational, intelligence, or other authorized activities are implicated by a matter subject to DARC review. They are designated on an ad hoc basis for each matter before the Council.

bulk data sharing activities comply with applicable law and adequately protect the privacy, civil rights, and civil liberties of the individuals whose information is shared. In addition, I&A's role as a member of the DARC is to ensure that members are aware of the Department's strategic intelligence, information sharing, and safeguarding perspective and to provide input into the sharing of data with that perspective in mind.

Section 1.0 Authorities and Other Requirements

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:

OPS Authorities:

- 6 U.S.C. § 321d.[11]

I&A's Authorities:

- The National Security Act of 1947, as amended (I&A), 50 U.S.C. § 401 et seq.[12]
- The Homeland Security Act of 2002,[13] as amended, by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and the Implementing Recommendations of the 9/11 Commission Act of 2007.[14]
- Executive Order No. 12333, as amended (I&A).[15]
- Executive Order 13388.[16]

In exercising its responsibilities under the Homeland Security Act, I&A is specifically

[11] *See* 6 U.S.C. § 321d, *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2010-title6/pdf/USCODE-2010-title6-chap1-subchapV-sec321d.pdf.
[12] *See* The National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (codified as amended at 50 U.S.C. ch. 15 (2012)), *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/pdf/USCODE-2011-title50-chap15-sec401.pdf.
[13] *See* 6 U.S.C. §§ 121-122 (2012), *available at* https://www.dhs.gov/homeland-security-act-2002.
[14] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266.
[15] *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 8, 1981), *available at* Exec. Order No. 12333 – United States Intelligence Activities, 46 Fed. Reg. 59941 (Dec. 8, 1981), available at http://www.archives.gov/federal-register/codification/executive-order/12333.html.
[16] *See* Exec. Order No. 13,388, 70 Fed. Reg. 62,023 (Oct. 25, 2005), *available at* https://www.gpo.gov/fdsys/pkg/FR-2005-10-27/pdf/05-21571.pdf.

authorized by statute to access and receive (collect) intelligence, law enforcement, and other information from federal, state, and local agencies and private sector entities.[17] That information includes any relevant reports, assessments, analyses, and unevaluated intelligence that may be collected, possessed, or prepared by any agency of the Federal Government for purposes of further analysis, integration, and other uses by the Department. This also includes authorization to disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland or national security, and to agencies of state and local governments and private sector entities with such responsibilities.

In carrying out these activities, I&A must consult with the Director of National Intelligence (DNI), other appropriate intelligence, law enforcement, or other elements of the Federal Government, state and local governments, and the private sector; to ensure the appropriate exchange of information is occurring.[18] Further, I&A must ensure that any materials it receives are protected from unauthorized disclosure and that any intelligence information is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947.[19]

Finally, the Homeland Security Act assigns I&A the responsibility of coordinating support to organizations that provide information to the Department or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information.[20] Those organizations include the elements and personnel of the Department, other agencies of the Federal Government, state and local governments, and the private sector.

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

The collection of PII maintained in the RFI Management Tool is described by the following SORNs:

[17] *See* 6 U.S.C. § 121(d)(1) (2012), *available at* https://www.gpo.gov/fdsys/granule/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapII-partA-sec121.
[18] *See* 6 U.S.C. § 121(d)(9) (2012), *available at* https://www.gpo.gov/fdsys/granule/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapII-partA-sec121.
[19] *See* 6 U.S.C. § 121(d)(11); National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (codified as amended at 50 U.S.C. §§ 401-442(b) (2012)), *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/pdf/USCODE-2011-title50-chap15-sec401.pdf.
https://www.gpo.gov/fdsys/granule/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapII-partA-sec121
[20] *See* 6 U.S.C. § 121(d)(15) (2012), *available at* https://www.gpo.gov/fdsys/granule/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapII-partA-sec121.

- DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN.[21]

- The DHS/I&A-001 I&A Enterprise Records System (ERS) SORN.[22]

To the extent that the RFI Management Tool contains data from other DHS components or other agencies that is responsive to a 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 resides within the GII accreditation boundary on the A-LAN and on MAVP on C-LAN as a major application. Both GII and MAVP currently have an ATO and are in full compliance with DHS 4300A, 4300B, and 4300C.[23]

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

I&A RFI records are covered by records schedule N1-563-07-16-5, which requires records to be destroyed or deleted after three years or when no longer needed for review and analysis. Additionally, records schedule N1-563-11-010-2 covers incident tracking indices, logs, summaries, source documents, and files for all events, incidents, and/or case files or which the NOC monitors or provides support. These records are considered permanent and are transferred to the National Archives after five years.

[21] *See* DHS/OPS-003 – Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, 75 Fed. Reg. 69689, (November 15, 2010) *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-11-15/html/2010-28566.htm.

[22] *See* 73 Fed. Reg. 28128 (May 15, 2008), *available at* https://www.gpo.gov/fdsys/pkg/FR-2008-05-15/html/E8-10888.htm.

[23] The Department of Homeland Security (DHS) 4300 series of information security policies are the official documents that create and publish Departmental standards and guidelines in accordance with DHS Management Directive 140-01 Information Technology System Security.

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.

I&A information collections are exempt from the PRA requirements pursuant to 44 U.S.C. § 3518(c)(1)(D). OPS' use of the RFI Management Tool is exempt from the PRA pursuant to 44 U.S.C. §§ 3518(a) and (c)(1)(B)(ii).

Section 2.0 Characterization of the Information

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

The RFI Management Tool maintains all information related to a RFI, including its status and processing. It collects information on the Requestor, including name, telephone number, email address, and the agency he or she represents. The system also maintains a record of the specific information requested in a RFI, which may or may not include PII. The information contained within a RFI may consist of identifying information about third parties, such as full name, citizenship, immigration status, as well as any possible law enforcement or national security nexus. In response to a request, the RFI Management Tool is limited to providing only an individual's name, date of birth, citizenship, immigration status, law enforcement information, and other identifying information that may be contained within the RFI itself.

The Tool also maintains information about the request and its compliance with DHS requirements for RFIs. It 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). The tool retains information provided in response to the query, making it available (provided a user has the appropriate role and permission) for subsequent queries when the same information is applicable.

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 as well as the Action Agency.

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

No. The RFI Management Tool does not contain information from commercial sources of publicly available data.

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 or the most accurate information from their records. Data are entered directly by users, which should reduce errors in transcription. A dedicated RFI Manager (assigned to the I&A RFI Team) will also review the data to ensure its integrity. The RFI Manager will examine the provided information and the submitted RFI to ensure that the data provided pertains to the customer's request. If the provided information does not match the nature of the requested information, or if it is discernably incomplete, the RFI Manager will return the request to the action agency with identified concerns highlighted and request the correct or complete information.

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-identfifying 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: This risk is partially mitigated. The RFI Management Tool reflects data submitted by other agencies and entities, which are presumed to provide accurate data from their records. 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 a 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

3.1 Describe how and why the project uses the information.

The RFI Management Tool uses the contact information, which may include PII, from the Requestor and the Action Agency to manage RFI submissions and responses.

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 a 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. Other components do have assigned roles and responsibilities with the system. On A-LAN, the U.S. Coast Guard has access to the RFI application. On C-LAN, only DHS and other U.S. Government users that have existing access to JWICS/C-LAN, which can be confirmed via Public Key Infrastructure (PKI),[24] are able to authenticate into the Tool. Users must be assigned a role by the RFI SPS Desk based on "need to know" to request and manage RFIs submitted by, as well as those submitted to, their organization. Authentication and role-based user access requirements ensure that users can only access or change information that is appropriate for their official duties and their organizations. The effectiveness of authentication and security protections are verified through the analysis of system operations and usage.

Dependent upon their user roles and level of access, external partners are able to submit a request to the SPS directly through the RFI Management Tool in order to obtain results. These reports are used by the requesting agencies in the furtherance of their particular missions. All RFIs are validated by the SPS Desk 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.

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, resulting 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

[24] A Public Key Infrastructure (PKI) is a set of roles, policies, and procedures needed to manage public-key encryption and to create, manage, distribute, use, store, and revoke digital certificates.

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. On the A-LAN, all users must receive a HSIN[25] account and be assigned a role by the SPS Desk. On the C-LAN, users must have an active IC PKI certificate and be assigned a role by the SPS Desk based on a demonstrated "need to know" or job-related requirement. 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 the analysis of system operation and usage. Unauthorized use of the RFI Management Tool will result in the suspension of a user's access and may include the loss of a security clearance and the termination of employment. Further, the SPS is located in a Sensitive Compartmented Information Facility (SCIF), an access controlled location, limited to those with valid access.

At the application level, all user access and authentication is role-based to ensure users can only access or change information that is appropriate to their official duties. Audit trails are created throughout the process and are reviewed on a consistent basis by the system administrator.

Section 4.0 Notice

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 identifying how and why the information is necessary, and that the provision of information is voluntary, is provided during HSIN log-on. Individuals who are the subject of requests, however, do not have specific notice of such collection because RFIs may

[25] *See* DHS/OPS/PIA-001 Homeland Security Information Network Database, *available at* https://www.dhs.gov/publication/dhsopspia-001-homeland-security-information-network-database.

contain sensitive but unclassified information, as well as classified information related to intelligence, counterterrorism, homeland security, and law enforcement programs, activities, and investigations. Additionally, the provision of direct notice to an individual at the time of a RFI search could undermine related law enforcement missions, operations, or activities.

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. 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. Allowing individuals to consent to collection and use would (1) notify the individual that he/she is the focus of DHS efforts, which would permit the individual to impede Government efforts to protect homeland security; (2) reveal sensitive methods or confidential sources used to acquire the relevant information; or (3) implicate an ongoing law enforcement investigation and permit the individual to impede the investigation. 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.

DHS developed the I&A RFI Management Tool, which supports the review, approval, or denial of a request, as a central repository for the results of the request and the tracking of the completion status of the request.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals may be unaware of the RFI Management Tool's collection of their information, or the use of their information by I&A and OPS.

Mitigation: This risk cannot be fully mitigated. DHS provides indirect notice through the publishing of this PIA, as well as the publication of the corresponding SORNs, DHS/I&A-001 Enterprise Records System (ERS), and DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion, which cover the collection of information.

With respect to information that is collected or shared with the homeland security community for law enforcement or intelligence purposes, notice is provided generally under the ERS SORN. The ERS SORN provides general notice to the public on the categories of individuals on whom information is collected, the types of information maintained, the purposes for the collection, and the routine uses of that information when disclosed outside of DHS. Although the SORN notes that this system of records has been exempted from notification, access, and correction to the extent permitted under subsection (k) of the Privacy Act, it does provide information on how the public can gain access to, and request correction of, any non-exempt records.

Section 5.0 Data Retention by the project

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

I&A RFI records, which are temporary in terms of retention, are cut off at the end of the calendar year when a request is completed, are covered by records schedule N1-563-07-016-5. The records are destroyed or deleted three years after cut off or when no longer needed for review and analysis. Additionally, records schedule N1-563-11-010-2 covers incident tracking indices, logs, summaries, source documents, and files for all events, incidents, and/or case files the NOC monitors or supports. These records are permanent and are cut off at the end of the calendar year in which the case (request) is closed. These records are transferred to the National Archives five years after cut off.

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 an inherent risk in the retention of PII for any length of time, the data retention period for the RFI Database is based on operational needs. Within the DHS-SPS, I&A is responsible for purging all RFIs validated by I&A and OPS purges all RFIs validated by the NOC.

Section 6.0 Information Sharing

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 RFI 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.

Both the ERS SORN, which provides coverage for the collection and maintenance of records by I&A, as well as DHS/OPS-003 SORN, which outlines the collection and maintenance of records by OPS, contain routine uses that allow for the external sharing of information. Additionally, those routine uses are compatible with the OPS and I&A missions as established under U.S. laws and Executive Orders. 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. To the extent that the RFI Management Tool contains and shares data from other DHS components or other agencies that is responsive to a RFI, that sharing is covered by the routine uses associated with SORNs for those source systems. 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?

Yes, Requestors can query the RFI Management Tool to see if a 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. The SPS Desk notifies Requestors of re-dissemination limitations verbally or in writing via classification and markings. These notifications are made, and tracked within the application.

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 Impact 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 Oversight Offices control access to their requests and can limit who sees the requests and associated responses. In cases in which 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 the 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/I&A-001 Enterprise Records System (ERS), and DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion.

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 a 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, the Office of the General Counsel-Intelligence Law Division or other appropriate offices. 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

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.

Under the ISE Privacy and Civil Liberties Protection Policy,[26] the Department has also established a process to permit individuals to file a privacy complaint. Individuals who have privacy complaints concerning analytic division intelligence activities may submit complaints to the DHS Privacy Office at privacy@dhs.gov. Individuals may also submit complaints alleging abuses of civil rights and civil liberties or possible violations of privacy protections by I&A

[26] *See* Guidelines to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the Information Sharing Environment, *available at* https://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf.

employees, contractors, or grantees to the Office of the Inspector General at the OIG Hotline website.[27] Additionally, individuals may file complaints alleging violations of civil rights and civil liberties by going to the CRCL website, completing the fillable form, and emailing it to CRCLCompliance@hq.dhs.gov.

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, individuals may request access to their records under the FOIA process, and on a selective basis may provide the requested records. Individuals may also file a privacy complaint as previously described. Any requests from the public for information stored in the RFI Management tool will be reviewed on a case by case basis in light of the reasons that the RFI Management tool is exempted from certain provisions of the Privacy Act.

Sometimes erroneous information is published in an intelligence product. When incorrect information is discovered, a revised product is published to correct the information or to note the questionable fact or content. Additionally, as previously noted, under the I&A Intelligence Oversight Procedures, products containing USPER information are reviewed on an annual basis to determine whether continued retention of the information is necessary to the conduct of an authorized I&A intelligence activity.

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/I&A-001 Enterprise Records System (ERS), and DHS/OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that individuals will not be afforded the ability to access and correct their information, resulting in a limited ability for individuals to ensure the

[27] DHS Office of Inspector General; Hotline website, *available at* https://www.oig.dhs.gov/index.php?option=com_content&view=article&id=51%3Ahotline-info&catid=1&Itemid=23.

accuracy of data.

Mitigation: This risk is partially mitigated. I&A performs annual reviews of information related to USPERs that is held within the RFI Tool in accordance with I&A's Intelligence Oversight Procedures. The ISE Privacy and Civil Liberties Policy requires that analysts endeavor to use and share information on USPERs that is reasonably considered accurate and appropriate for their documented purposes and to protect data integrity.[28] This policy also requires analysts to notify others in the ISE when information that is determined to be inaccurate is disseminated or received by I&A.

To the extent that records are no exempt under these authorities, DHS will provide access to them. Individuals, regardless of immigration status, may also request access to their records under FOIA. Additionally, U.S. persons may request access under the Privacy Act. Individuals may also file a privacy complaint with the DHS Privacy Office, and a civil rights and civil liberties complaint with CRCL, or the OIG.

Section 8.0 Auditing and Accountability

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 A-LAN (Unclassified) and C-LAN (Top Secret) is incumbent upon 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. All RFI Management Tool Users receive instruction on how to complete, submit, and respond to a RFI. All RFI Managers are trained on the management of RFIs and are required to denote PII/USPER information contained in a RFI as part of the validation process. DHS employees may be subject to discipline and administrative action for unauthorized use or

[28] *See* Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment, *available at* https://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf.

disclosure of this information, including but not limited to loss of clearance and/or termination of employment.

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

All DHS employees, contractors, and other personnel receive initial privacy training within 30 days of onboarding. Additionally, I&A employees, contractors, and other personnel receive privacy and security awareness training within 30 days of onboarding. 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. Users who fail to take intelligence oversight training within one year will have their TS/SCI account suspended, and their account will not be reinstated until they complete the required training. DHS Components are responsible for ensuring that their users have received privacy, security, intelligence oversight, or other training as appropriate to perform their professional duties in support of their missions.

All RFI Management Tool Users receive instruction on how to complete, submit, and respond to a RFI. All RFI Managers are trained on the management of RFIs and are required to denote PII/USPER information contained in a RFI as part of the validation process.

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 a 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?

The DARC reviews and approves all disseminations based on a RFI outside of the Department.

Responsible Officials

Ronald Shipman
Chief, Collections Management
Department of Homeland Security

Approval Signature

____

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