Privacy Impact Assessment Update
for the

DHS Request for Information Management Tool:

CBP Module

DHS/ALL/PIA-044(b)

October 30, 2019

Contact Point
Ronald J. Ocker
Office of Intelligence
U.S. Customs and Border Protection
(202) 325-1251

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

Abstract

The Department of Homeland Security (DHS) Intelligence and Analysis (I&A) Request for Information (RFI) Management Tool serves as a centralized DHS Headquarters location for receiving, facilitating, processing, and responding to operational or intelligence-related RFIs originating outside the Department. Because the DHS RFI Management Tool[1] is specific to DHS Headquarters' business processes and requests, U.S. Customs and Border Protection (CBP) is modifying the DHS RFI Management Tool by creating a single web application RFI Tool for CBP's use. DHS is publishing this Privacy Impact Assessment (PIA) update to provide notice of the CBP RFI Tool and describe the associated privacy risks and mitigations for the personally identifiable information (PII) the tool collects, retains, and disseminates.

Overview

U.S. Customs and Border Protection (CBP) combats terrorism and transnational crime by providing timely, actionable, and relevant intelligence information to drive operations, planning, and decision-making in the border security strategic environment. CBP prioritizes building and strengthening strategic partnerships in the Intelligence and Law Enforcement Communities, and regularly responds to domestic and foreign Requests for Information (RFI).

CBP defines a RFI as a validated expression of need or gap within an organization or among organizations for information, which can be satisfied through the exploitation of existing CBP databases or collection not otherwise available to the requestor. A CBP RFI is limited in scope and answers a single, specific operational or intelligence question. RFIs may pertain to a variety of subjects, including information contained in CBP intelligence products, and results of CBP inspection and enforcement operations. For the purposes of this PIA, an RFI is limited to a request for information handled by the CBP Office of Intelligence (OI). Other CBP offices, including the Privacy and Diversity Office, also process requests for information that may be similar in content to RFIs handled by OI; however, such requests are managed through a different process and are not maintained in the CBP RFI Tool. This PIA does not include bulk information-sharing requests[2] or requests for correspondence operated under the DHS Executive Secretariat.[3] CBP may respond to a RFI with existing intelligence products, results from searches of information

[1] *See* DHS/ALL/PIA-044(a) DHS-wide RFI Management Tool, *available at* www.dhs.gov/privacy.
[2] *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.
[3] The DHS Executive Secretariat governs the Department-wide process for responding to correspondence and preparing the Secretary's briefing book, congressional authorization reports, hearing testimony, and questions for the record related to congressional authorizing committees. Correspondence related to the Executive Secretariat's roles are stored in the Enterprise Correspondence Tracking system: *see* https://www.dhs.gov/publication/enterprise-correspondence-tracking-ect-system.

from CBP databases, or new data collected in response to the RFI consistent with intelligence priorities. In addition to responding to RFIs from external law enforcement or intelligence partners, CBP employees may initiate RFIs when they need information they cannot access as part of their daily duties.

The CBP OI processes operational and intelligence-related RFIs within CBP. In order to carry out its mission, CBP has leveraged the infrastructure of the DHS RFI Management Tool and created a separate database and user interface for CBP. The CBP RFI Tool serves as a means for OI to centrally record and track requests, catalog responses, and ensure enhanced coordination and effective oversight of this information sharing process.

CBP is obligated by the Privacy Act of 1974 to ensure that information is properly collected, maintained, secured, and disseminated in order to maintain the integrity of the data, as well as mitigate the risk of adverse consequences due to a breach or misuse of the data. CBP Directive number 2120-010 "Privacy, Policy, Compliance, and Implementation" holds the CBP Privacy Officer responsible for overseeing the process to permit the ad hoc sharing of information containing PII consistent with the law and DHS/CBP Policies. The CBP Privacy Officer is working on delegating the approval of requests to share PII with U.S. partners in response to a category of information or class of other agency requests to OI for requests that come through the RFI process. This delegation will provide guidance on how to appropriately share information on a case-by-case basis with law enforcement and intelligence partners and speed up the approval process in lieu of obtaining CBP Privacy approval for each individual RFI.

The CBP RFI Process

The CBP RFI process starts when there is a need for pertinent CBP data to carry out the requestor's official duties. Requestors can be DHS employees who may need information they cannot access as part of their daily duties, or other federal, state, local, tribal and territorial entities that have a law enforcement or intelligence mission need for CBP information. The majority of requests are submitted to the CBP RFI Mailbox or directly to a CBP analyst by email. If DHS receives a request for CBP information through its RFI process, they it forwards the request to CBP by email following internal coordination with the Office of the General Counsel (OGC) and other oversight offices such as the DHS Privacy Office (PRIV), the Office for Civil Rights and Civil Liberties, and the Office of Intelligence and Analysis (I&A) Intelligence Oversight. OGC and PRIV, and when appropriate the other Oversight offices, 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]

Once CBP receives a request, an Approved User of the CBP RFI Tool initiates a new record that generates a unique task number based on the CBP organization that received the initial request. This task number allows users to easily track and route a request back to the appropriate CBP organization where the request originated. PII collected into the Tool during this process includes the requestor's name, telephone number, email, and the organization that requestor represents. The request also includes a detailed justification that describes the need for the records, the intended use of the information, and the classification level of the request. Typically, RFIs are subject-based and include PII on the subject(s) of interest or any third parties. This can include name, date of birth, citizenship, immigration status, law enforcement information, and other identifying information that requestor may optionally add to the request.

After the user has created a new record in the CBP RFI Tool, the Approved User sends the record to a RFI Manager within his/her CBP organization who will place the RFI in an "under review status" to be validated. The validation process ensures that: 1) the request pertains to information that is within CBP's authorities to share; 2) the RFI complies with the laws, regulations, and policies governing information sharing and the dissemination of classified or otherwise controlled information; 3) CBP can answer the RFI with information in existing databases, reporting, analysis, and/or collection; 4) the requestor is authorized to receive the information; and 5) the individual and/or organization submitting the RFI possesses a valid "need to know." In instances in which the RFI Manager is unsure if the request meets any of the above criteria, the RFI Manager will confer with CBP's Office of the Chief Counsel and the Privacy and Diversity Office. The RFI Tool documents the results of the internal coordination.

After the RFI Manager validates the RFI, he or she assigns the request to a "CBP Action Office" (i.e., the custodian of the requested information). The assigned CBP Action Office first examines existing data that resides in the RFI Tool to determine if there is any previous reporting on the subject. In order to use existing data from a previous request, the user must conduct an assessment to ensure that data is still accurate. If there is no existing data within the Tool to satisfy the request, the Action Office will run queries in CBP systems to which it has access. If no responsive information is available, the Action Office may defer the RFI to another CBP Office for action, or determine if a new collection is required.

Before disseminating the response back to the Requestor, the Action Office must send the response to a CBP RFI Manager who reviews the response to ensure that the data is accurate and

[4] 5 U.S.C. § 552a.
[5] Executive Order 12333, United States Intelligence Activities (Dec. 4, 1981), 46 FR 59941.
[6] Office of Intelligence and Analysis, U.S. Department of Homeland Security, Instruction: IA-1000 (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 response is relevant to the request. If the information does not match the nature of the requested information, or if it is discernably incomplete, the CBP RFI Manager will return the request to the CBP Action Office to provide the correct or complete information.

Once approved, the RFI Manager will disseminate the response directly to the Requestor. The RFI Tool will record the annotation of the release (if it was in writing or in the form of a document/file). Depending on the nature and scope of the RFI, the RFI Manager may upload the responsive record as an attachment into the Tool.

Reason for PIA Update

CBP developed the CBP RFI Tool in order to record and track CBP Office OI requests, catalogue responses, and ensure enhanced coordination and effective oversight of the CBP information sharing process. Because the business processes for RFIs within DHS Headquarters and CBP are similar, CBP modified the existing DHS RFI Management Tool for use at CBP. The CBP RFI Tool resides on a separate web application and does not have a direct connection to the DHS RFI Management Tool. DHS is publishing this PIA update to discuss CBP's RFI process and the PII the CBP RFI Tool collects, retains, and disseminates.

Privacy Impact Analysis

Authorities and Other Requirements

The CBP RFI Tool derives its authority primarily from Title II of the Homeland Security Act of 2002 (Pub. L. 107-296), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458, 118 Stat. 3638); the Tariff Act of 1930, as amended; the Immigration and Nationality Act ("INA"), 8 U.S.C. § 1101, et seq.; the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53); the Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104-132, 110 Stat. 1214); SAFE Port Act of 2006 (Pub. L. 109-347); Aviation and Transportation Security Act of 2001 (Pub. L. 107-71); and 6 U.S.C. § 202.

DHS/CBP-024 Intelligence Records System (CIRS)[7] covers the collection of PII maintained in the CBP RFI Tool and the RFI process. To the extent that the CBP RFI Tool contains data from other DHS components or other agencies that is responsive to a RFI, the source system System of Records Notice (SORN) governs that information. Information not owned by CBP will only be releasable pursuant to the owning agency's information sharing agreement with CBP, or if no such information sharing agreement exists, only after obtaining the express consent of the owning agency.

[7] 82 F.R. 44198 (September 21, 2017).

Characterization of the Information

The CBP RFI Tool maintains all information related to RFIs processed by CBP OI, including its status and information related to the processing of the request. The information in the CBP RFI Tool is similar to what is collected and maintained in the DHS RFI Management Tool. The CBP RFI Tool collects information about who the request originated from, including name, telephone number, email address, and the organization the requestor represents. If a request is subject-based, the PII of the subject(s) of interest may be stored in the Tool. This can include name, date of birth, citizenship, immigration status, law enforcement information, and other identifying information the request may include. When the Action Office receives the request for action, the RFI Tool includes information about the Action Office, including who responded to the request, to which CBP organization the employee acting on the request belongs, and his/her contact information. Once the Request and responsive records are validated, the Tool will document when the request was disseminated, an annotation of how the record was disseminated to the requestor, and depending on the nature and scope of the request, the responsive record may be stored as an attachment in the Tool.

In some instances, other agency data may be included in CBP's response. Other agency data is only releasable by CBP when the owning agency's information sharing agreement permits the onward sharing of that data, or if no such information sharing agreement exists, only after obtaining the express consent of the owning agency.

Privacy Risk: There is a risk that CBP will share information in response to a RFI that is outdated or inaccurate, or that it will share information from an aggregated system that is not the original source of the record.

Mitigation: This risk is partially mitigated. When responding to a request, users receive training to pull information from the source system. In addition, all responses to a RFI must go through a RFI Manager who reviews the data to ensure its integrity before the release of the record.

Privacy Risk: The CBP RFI Tool could present a risk of the over collection of PII or the excessive aggregation of disparate PII from various CBP systems.

Mitigation: This risk is partially mitigated through the validation process. Before researching and examining existing holdings to satisfy a request, RFIs must be validated to ensure: 1) the request pertains to information that is within CBP's authorities to share; 2) the RFI complies with the laws, regulations, and policies governing information sharing and the dissemination of classified or otherwise controlled information; 3) CBP can answer the RFI with information in existing databases, reporting, analysis, and/or collection; 4) the requestor is authorized to receive the information; and 5) the individual and/or organization submitting the RFI possesses a valid "need to know." If the RFI does not meet the validation criteria, CBP sends the request back to the Requestor to ask for clarification. If the Action Office determines that a RFI is still invalid, the

Action 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.

Privacy Risk: There is a risk that CBP will share information in response to a RFI that is not consistent with the purpose of the original collection.

Mitigation: This risk is partially mitigated. CBP ensures that its release of information in response to RFIs is consistent with the routine uses of the source SORN; prior to publication of a SORN, CBP reviews all routine uses to ensure that they are consistent with the original purpose of the collection. The CBP Office of the Chief Counsel and the Privacy and Diversity Office assist in overseeing the CBP RFI process to ensure that CBP only releases information consistent with applicable laws and departmental policies.

Uses of the Information

CBP uses the information stored in the Tool in order to coordinate the RFI process and maintain all associated records. The CBP RFI Tool collects contact information from both the Requestor and the CBP Action Office in order to manage and track RFI submissions and responses.

The CBP RFI Tool also aggregates statistical data on the RFI process to generate performance management reports. These performance reports help CBP to prioritize needs, identify process improvements, evaluate potential courses of action, and assess the impact of operating decisions. In addition, there is an auditing capability in the CBP RFI Tool that will track all actions by users. CBP management or other offices with oversight responsibility may use this information 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 CBP RFI Tool.

Users have different roles within the Tool consistent with their responsibilities and applicable to their official duties. Within the CBP RFI Tool, there are three basic types of users for each operational level of the RFI Tool architecture:

- Approved User: This user has the ability to draft, edit, and submit only those RFIs that the User has created.
- RFI Manager: Responsible for the vetting, validating, coordinating, and tracking of all RFIs originating from his/her CBP Unit. A RFI Manager has the ability to draft, edit, and submit RFIs that anyone in the Unit has created, as well as deferring a RFI to a lateral Unit or his/her Unit's Administrator.
- Administrator: The Administrator has same capabilities as a RFI Manager plus the ability to grant accesses (create/approve a user profile) to people within the RFI system.

There is at least one Administrator at each Unit. Outside of CBP, no other DHS Component or Agency has assigned roles and responsibilities within the CBP RFI Tool.

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

Mitigation: To mitigate this risk, access to the RFI CBP RFI Tool is strictly controlled. RFI Managers assign users roles based on their "need to know". Authentication and role-based user access requirements ensure that users can only access or change information that is appropriate for their official duties. Administrators will monitor unauthorized use of the CBP RFI Tool through audit logs which could result in the suspension of a user's access.

Privacy Risk: There is a risk that there will be exposure to a record in the Tool that a user is not provisioned to see in the source system.

Mitigation: This risk partially mitigated. Although access controls allow for limitation of who sees the requests and associated responses within a user's Unit, the CBP RFI Tool does not have the capability to provide access controls at the individual record level. However, the impact of the risk is relatively low because majority of users to the RFI Tool are trusted users of various CBP source system data for a request that would fall under their Unit's purview.

Notice

This PIA provides notice to the public of CBP's use and sharing of information through the RFI Tool. CBP also provides notice of the original collection of information in the individual PIAs and SORNs for those systems. Whenever possible, CBP provides notice to the individual via Privacy Act Statements or other privacy notices at the original points of collection or via published SORNs for the underlying systems, which include routine uses describing how CBP may share information with law enforcement entities.

The CBP RFI 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 law enforcement or intelligence efforts, which could 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 potentially 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.

Privacy Risk: There is a privacy risk that individuals may be unaware of the CBP RFI Tool's collection of their information, or the use of their information by CBP.

Mitigation: This risk cannot be fully mitigated. CBP provides notice through the publishing of this PIA, as well as the publication of the corresponding PIAs and SORNs, which cover the source collection of information. While CBP cannot reasonably provide direct and timely notice to the individual for each instance of sharing outside the agency, it ensures that all sharing is consistent with the Privacy Act of 1974.

Data Retention by the Project

CBP will retain RFI records (including corresponding research, responses, and supporting documentation) for 10 years, consistent with DHS Office of Intelligence and Analysis DHS N1-563-07-016 records schedule.

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 CBP RFI Tool is based on operational needs. CBP is responsible for purging all RFIs according to the records retention schedule. Retention of these records allows CBP to respond to homeland security partners expeditiously and provides accountability for the transactional activity.

Privacy Risk: There is a risk that retaining records in the RFI Tool for ten years will result in records that have since been modified or updated in the source system.

Mitigation: This risk is partially mitigated. RFI users may search the tool to find records that may have been satisfied through a similar request. If a responsive record is pulled from a separate request, the user is trained to check the source system to verify that responsive record is still accurate. In addition, all responses to a RFI must go through a RFI Manager who reviews the data to ensure its integrity before the release of the record. If a record in the tool is found to be inaccurate, the record will be deleted immediately.

Information Sharing

CBP uses the RFI tool to facilitate and maintain a record of all RFIs processed by CBP OI. The Tool allows CBP to ensure that it shares information in response to RFIs in compliance with existing privacy documentation. The business process built into the tool ensures multiple levels of review prior to disclosing information outside of the agency. All releasable RFIs go through the validation process described above and are shared in accordance with the routine uses listed in the applicable SORNs. RFIs resulting in foreign disclosures go through CBP OI's Foreign Disclosure Office (FDO). The FDO ensures that OI CBP RFIs from other governments are appropriately reviewed, there is a valid need to know, and the RFIs abide by applicable laws and agency

objectives prior to disclosures of information to a foreign government or multilateral governmental organization. The FDO ensures that there is a clear benefit to the United States, a proper need to know is established, that there is no unreasonable risk to U.S. operations, sources, and methods, and finally that DHS and Office of the Director of National Intelligence policies and guidelines are followed. When information belongs to another agency, the OI FDO works with other agencies FDOs to obtain approval to share the information.

Privacy Risk: There is a potential risk of RFIs and their responses being improperly disclosed, misused, lost, or further disseminated without permission by the receiving agencies.

Mitigation: Access controls allow CBP to limit who sees the requests and the associated responses. CBP personnel who provide responses receive training 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. In cases in which a record is being requested that is maintained in CBP systems but owned by another agency, users are trained to get the permission of the originator before releasing that record. The delegated authority by the CBP Privacy Officer to OI to release records that contain PII will include Standard Operating Procedures and a checklist to ensure OI is properly releasing records and placing limitation on onward sharing.

Redress

Most of the information within CBP RFI Tool is duplicative of the underlying source datasets. To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of CBP systems, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place. The source system PIAs and SORNs notify the public regarding procedures for access and correction of applicable records.

Individuals seeking access to information maintained by CBP may file a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229
Fax Number: (202) 325-1476

If an individual believes that CBP records contain incorrect or inaccurate information, the individual may direct inquiries to:

U.S. Customs and Border Protection
CBP Info Center
Office of Public Affairs
1300 Pennsylvania Avenue NW
Washington, D.C. 20229

Privacy Risk: There is a privacy risk that individuals will not be able to request correction of the records maintained in or shared using the CBP RFI Tool when a correction is made to the original record.

Mitigation: This risk is mitigated. Users receive training to pull all responsive records from the source system for this reason. If a record is already stored within the CBP RFI Tool and used to fulfill a similar request, the user must check the source system to make sure that record is still accurate. If a record in the tool is found to be inaccurate, the record will be deleted immediately.

Auditing and Accountability

The RFI application resides on both the unclassified and classified networks where CBP users access the RFI Tool. The RFI Manager assigns user roles based on "need to know," and authentication and role-based user access requirements ensure that users can only access or change information consistent with their official duties. CBP verifies the effectiveness of authentication and security protections through the analysis of system operations and usage. Privacy protections include strict access controls, including passwords and auditing that tracks access to electronic information. Access to the CBP RFI Tool at the unclassified level is only granted if the user possesses a valid CBP RFI Tool account and government email address, and only upon verification by the RFI Manager within their unit. For classified use of the Tool, the user must have the appropriate security clearance to access the Tool and the Top Secret Network it resides on. All CBP RFI Tool Users receive instruction on how to complete, submit, and respond to a RFI. All CBP RFI Managers receive training on the management of RFIs. CBP employees may be subject to discipline and administrative action for unauthorized use or disclosure of this information.

Additionally, CBP 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. In addition, all CBP employees are required to take annual computer security training, which includes privacy training on appropriate

use of sensitive data, and proper security measures. When the CBP Privacy Officer signs the delegated authority to OI to release records containing PII, all RFI users will be required to review that delegated authority, and read the attached standard operating procedures.

Responsible Officials

Steven Griffin
Director
Collections Division, Office of Intelligence
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

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