# PRIVACY IMPACT ASSESSMENT

| | |
|---|---|
| **SYSTEM OR APPLICATION NAME:** | Eventbrite |
| **DATE:** | 9/25/2025 |
| **SYSTEM OWNER & TITLE:** | Chuck Trucco, Associate Director of Operations Support |
| **CONTACT POINT** | Chuck Trucco |
| **ORGANIZATION:** | Bureau of Field Service |
| **REVIEWING OFFICIAL NAME & TITLE** | Mark Blythe, Director of Field Service |
| **ORGANIZATION:** | Information Resources Management Center<br>Bureau of Information Services |

| | |
|---|---|
| **System or Application Name:** | Eventbrite |
| **Date:** | 9/25/2025 |

## Overview

Eventbrite is a third-party event management and registration platform that enables the Railroad Retirement Board (RRB) to facilitate public event registration. Eventbrite allows the RRB: to create event registration, speaker profiles, organizer profiles, and other webpages related to public events; to promote those pages and events to visitors or browsers on Eventbrite services; and to facilitate event registration and management for registrants and the agency.

The RRB conducted this Privacy Impact Assessment (PIA) because the agency may utilize Eventbrite to collect and retain personally identifiable information (PII), including an event registrant's name, address, email address, phone number, and other information that enable the RRB and/or Eventbrite to identify individuals. Eventbrite's Terms of Service and Privacy Policy govern Eventbrite's collection, use, maintenance, and disclosure of information. Users may wish to review the Eventbrite Privacy Policy before using its services to understand how and when Eventbrite collects, uses, and shares the information submitted for RRB events utilizing Eventbrite's services.

## Section 1.0 -- The System and the Information Collected and Stored within the System

The following is intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The RRB utilizes Eventbrite to collect a registrant's name, address, phone number, email address, and/or current and/or previous associated railroad employer to facilitate training and event registration. Depending on the event, RRB organizers can set up event registration pages to collect additional information from registrants (for example, requests for accommodations) in connection with the Department's event registration process and to facilitate event registration. Event pages may also include speaker biographic information (e.g., name, position, etc.). Components will only provide this information with the consent of the speaker, if the speaker is not an RRB employee. Overall, the RRB will collect only information necessary for the proper performance of agency functions and that has practical utility.

Event registrants and/or users may choose to create an Eventbrite account, although this is not required to register for an event. To create an Eventbrite account, users provide their email address, create a password, and provide additional information as required by Eventbrite. Eventbrite does not provide this account information to the RRB to facilitate event registration in its official capacity.

1.2 From whom is the information collected?

Information is about and collected directly from government employees and members of the public who choose to attend RRB-hosted trainings and events that utilize Eventbrite to manage registration.

## Section 2.0 -- The Purpose of the System and the Information Collected and Stored within the System

The following delineates the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The RRB uses the information to communicate with event attendees about event materials, for event logistics purposes, to request for event feedback, and to otherwise facilitate RRB events. Additionally, information may be necessary to maintain the security of the personnel and locations at which the RRB operates.

2.2 What specific legal authorities, arrangements, agreements authorize the collection of information?

The collection of information through Eventbrite is authorized and governed by existing Railroad Retirement Board privacy documentation and systems of records:

- Benefit Payment Operations Privacy Impact Assessment (BPO PIA), which describes the handling of personally identifiable information (PII) in connection with the administration of RRB benefits and associated customer engagement tools.
- System of Records Notices (SORNs):
    - RRB–21, Railroad Unemployment and Sickness Insurance Benefit System of Records – covering records used in the administration of unemployment and sickness insurance benefits, including communications and notices to beneficiaries.
    - RRB–22, Railroad Retirement, Survivor, and Pensioner Benefit System of Records – covering records used in the administration of retirement and survivor benefits, including related outreach and correspondence activities.

These authorities collectively authorize the collection and use of contact and registration information via Eventbrite to facilitate outreach, communications, and benefit-related events.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The RRB has taken appropriate steps to mitigate any potential threats to privacy that exist in light of the event registration information collected and shared. For the purposes of event registration, the RRB will collect only information necessary for the proper performance of agency functions and that has practical utility, minimizing the risks of collecting unnecessary information. Additionally, RRB employs a robust IT security system to protect its servers and access terminals to minimize the unauthorized access or misuse of registration information maintained by the RRB. Finally, information is entered directly by the registrant to minimize the possibility of the RRB entering inaccurate information.

## Section 3.0 -- Uses of the System and the Information

The following delineates the intended uses of the information in the system.

3.1 Describe all uses of the information.

The RRB uses the information to facilitate in-person event logistics and communication, to request event feedback, and to disseminate event materials.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

The RRB will not dictate what applications will be used by Eventbrite to analyze data that users voluntarily submit.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

Eventbrite event registrant/user information is entered directly by the registrant to minimize the possibility of inaccurate information.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The information collected and retained on Eventbrite is not an agency record. To the extent the RRB creates and maintains event or training rosters separately from Eventbrite, these records will be retained in accordance with the RRB-wide records schedule for training records.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Event and training roster records maintained separately from Eventbrite will be stored in RRB internal systems with appropriate retention record schedules applied.

**Section 4.0 -- Internal Sharing and Disclosure of Information within the System**

The following defines the scope of sharing within the RRB.

4.1 With which internal organizations of the RRB is the information shared?

Information will be shared within RRB personnel who have a need to know, including internal organization(s) staff responsible for event logistics. Only internal organization staff managing event registration will have direct access to Eventbrite. By providing information through Eventbrite for a RRB event, Eventbrite will also collect, use, maintain, and disclose user information in accordance with its Terms of Service and Privacy Policy. User may wish to review the Eventbrite Privacy Policy before using its services to understand how and when Eventbrite collects, uses, and shares the information submitted for RRB events utilizing Eventbrite's services.

4.2 For each recipient organization or office, what information is shared and for what purpose?

Registrants' information (registrant's name, address, phone number, email address, and/or current and/or previous associated railroad employer to facilitate training and event registration) may be shared with other internal organizations for event logistics purposes, to request and analyze event feedback, and to otherwise facilitate RRB events.

4.3 How is the information transmitted or disclosed?

RRB Eventbrite event information and registrant information will be transmitted using approved agency IT systems.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The RRB has taken appropriate steps to mitigate any potential threats to privacy that exist in light of the event registration information collected and shared. For the purposes of event registration, the RRB will collect only information necessary for the proper performance of agency functions and that has practical utility, minimizing the risks of collecting unnecessary information. Additionally, RRB employs a robust physical security system to protect its servers and access terminals to minimize the unauthorized access or misuse of registration information maintained by the RRB. Additionally, Eventbrite maintains a Privacy Policy which the agency and individual users may access.

| | |
|---|---|
| **SYSTEM OR APPLICATION NAME:** | Eventbrite |
| **DATE:** | 9/25/2025 |

## Section 5.0 -- External Sharing and Disclosure

The following defines the content, scope, and authority for information sharing external to RRB which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-RRB) is the information shared?

RRB may share registrant information including registrant's name and/or current and/or previous associated railroad employer with railroad employers and/or railroad employee union organizations.

5.2 What information is shared and for what purpose?

Registrant's name and/or current and/or previous associated railroad employer for attendance notification purposes.

5.3 How is the information transmitted or disclosed?

RRB Eventbrite event information and registrant information will be transmitted using approved agency IT systems following established data protection procedures and methodologies.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

No

5.5 What type of training is required for users from agencies outside RRB prior to receiving access to the information?

No training is required.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

No

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The RRB has taken appropriate steps to mitigate any potential threats to privacy that exist in light of the event registration information collected and shared. Registrants will be notified their name and current and/or previous railroad employer information may be shared with their current and/or previous railroad employer and/or their railroad employee union organization. RRB employs a robust physical security system to protect its servers and access terminals to minimize the unauthorized access or misuse of registration information maintained by the RRB. Additionally, Eventbrite maintains a Privacy Policy which the agency and individual users may access.

## Section 6.0 – Notice

The following describes the notice to the individual of the scope of information collected, the opportunity to consent to uses of the information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice [link] published in the Federal Register Notice.) If notice was not provided, explain why not.

The RRB will set up official event registration pages that clearly establish that RRB is hosting the event. For example, the RRB will, where feasible, use the RRB seal on event registration pages.

The RRB and its components will, where feasible, provide a privacy notice on any Eventbrite event page requesting information. The notice will explain that Eventbrite is not a RRB website, that it is controlled and operated by a third party, and that the RRB's Website Privacy Policy does not apply to the third party. The notice will also describe how the RRB will maintain, use, or share PII, and explain that individuals may be providing information to third parties by using Eventbrite.

6.2 Do individuals have an opportunity right to decline to provide information?

To the extent that participating in a RRB event is voluntary, individuals have the opportunity to decline to provide information to the RRB through Eventbrite, however, failure to provide information may delay or prohibit event registration.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Implicit in RRB notifying registrants of the particular uses of their information, individuals have the opportunity to consent to the uses of their information provided to the RRB through Eventbrite. Individuals do not otherwise have the opportunity to consent to the particular uses of the information. The minimal information collected is required to facilitate event and training registration and communication.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

## Section 7.0 -- Individual Access and Redress

The following questions concern the ability of individuals to ensure the accuracy of information collected about them.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Event registrants and/or users may choose to create an Eventbrite account, although this is not required to register for an event. To create an Eventbrite account, users provide their email address, create a password, and provide additional information as required by Eventbrite. Individuals who create an Eventbrite account are able to access past and current event registration information. Eventbrite does not provide this account information to the RRB to facilitate event registration in its official capacity. Individuals who do not create an Eventbrite account are provided email confirmation of the information provided to register for a RRB event on Eventbrite. Individuals are not provided a means through which to redress their information once provided through Eventbrite to register for a RRB event.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Procedures for seeking access to or amendment of information is provided through email for all registrants and, additionally, through an individual's Eventbrite account if the individual chose to create an Eventbrite account.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives to the individual?

| SYSTEM OR APPLICATION NAME: | Eventbrite |
|---|---|
| DATE: | 9/25/2025 |

N/A

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Eventbrite event registrant/user information is entered directly by the registrant for each event registration instance to minimize the possibility of inaccurate information.

**Section 8.0 -- Technical Access and Security**

The following describes technical safeguards and security measures.

8.1 Which user will have access to the system?

Internal organization staff managing event registration will have direct access to Eventbrite.

8.2 Will contractors to the RRB have access to the system? If so, please submit a copy of the contract describing their role with this PIA?

No

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes

8.4 What procedures are in place to determine which users may access the system and are they documented?

Bureau/office Executive Committee members, or their designee(s), approve user access to the system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Eventbrite roles are independent of RRB system roles and rules. Eventbrite roles, and the functionality those roles permit users is managed by the Eventbrite account holder. Individual RRB employees will only be assigned the Eventbrite system roles, and the functionality those roles permit, for their responsible duties.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

| SYSTEM OR APPLICATION NAME: | Eventbrite |
|---|---|
| DATE: | 9/25/2025 |

Administrative Safeguards:

- Administrative access limited strictly to RRB system administrators.
- Event organizers, communications, and talent teams have restricted user roles.

Physical Safeguards:

- Eventbrite's own perimeter defenses, firewall systems, and data center best practices.

Technical Safeguards:

- User Identification required for access.
- Use of password protections.
- Encryption of sensitive data.
- Multi-factor Authentication (MFA) employed.

Auditing and Monitoring:

- Eventbrite offers 24×7 monitoring of security systems and alerting infrastructure.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Users undergo required annual privacy training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification and Accreditation last completed?

Eventbrite is third-party application that uses generally accepted commercial business practices for IT security, to ensure that systems are operated and maintained in a secure manner, and that management, operational and technical controls are employed to protect the security of systems and data. Eventbrite complies with PCI-DSS 4.0.1 Level 1 as both a Merchant and a Service Provider. As such, Eventbrite is regularly audited by a Qualified Security Assessor (Coalfire, Inc.), passes internal and external application and network penetration testing performed by independent security firms, and is scanned monthly by an Approved Scanning Vendor (ASV).

Additionally, Eventbrite agrees in their Amendment to Terms of Service that Apply to Federal Agencies Using Eventbrite Services to discuss additional security controls as deemed necessary by the RRB for specific system applications which require additional security controls to conform to FISMA requirements.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

| SYSTEM OR APPLICATION NAME: | Eventbrite |
|---|---|
| DATE: | 9/25/2025 |

1. Collection of Personal Data by a Third Party
Eventbrite collects personally identifiable information (PII) such as names, email addresses, physical addresses, and occasionally additional custom fields depending on the event organizer's configuration.
Risk: Users may not realize that their data is being collected by a third party and may assume only the host agency is handling their data.
Mitigation: Agencies must provide clear notice explaining that Eventbrite is a third-party platform and that its own privacy policy does not apply to Eventbrite.

2. Oversharing or Unnecessary Data Collection
Some events might require more information than necessary, or attendees may inadvertently provide more PII than needed.
Risk: Over-collection increases exposure and potential for misuse or breach.
Mitigation: Agencies are encouraged to collect only what is strictly necessary for event logistics and communication.

3. User Misunderstanding of Control and Ownership
Attendees may believe Eventbrite is the official agency site and not understand how their data is handled, stored, or shared.
Risk: Misperception could lead to unintended consent or mishandling concerns.
Mitigation: Notices should clearly state Eventbrite's independent operation and direct users to its privacy policy.

4. Inherent Platform Security & Vendor Risk
Even reputable platforms like Eventbrite are subject to data breaches, hacking, or other attacks.
Risk: Any data transmitted via Eventbrite could be intercepted or exposed.
Mitigation: Agencies must review Eventbrite's security posture regularly. Strategies include vendor risk assessments and monitoring breaches or security updates.

5. Access Control by Agencies Using Eventbrite
Proper internal controls are essential. Many agencies restrict access by internal roles, enforce login authentication, and require privacy/security training for event managers.
Risk: Unauthorized internal access may lead to data being misused or exposed.
Mitigation: Implement strict need-to-know access, enforce secure authentication, auditing, and training.

6. Federal Records and Retention Issues
Because Eventbrite is a third-party system, data there may not be considered an official agency record. For agencies like DOJ and NARA, this may complicate record-keeping or retention obligations.
Risk: Non-compliance with federal records schedules or lack of transparency in retention.
Mitigation: Agencies should export relevant data into their enterprise systems and apply compliant retention schedules.

## Section 9.0 -- Technology

The following critically analyze the selection process for any technologies utilized by the system, including system hardware, and other technology.

| | |
|---|---|
| **System or Application Name:** | Eventbrite |
| **Date:** | 9/25/2025 |

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Analysis of other federal agency PIA documentation was conducted.

9.3 What design choices were made to enhance privacy?

Internal process development.

**Conclusion**

Eventbrite offers an event management and registration technology solution to effectively logistics of agency hosted education events for the railroad community.

**Certification of Responsible Officials**

| | |
|---|---|
| Preparer Signature & Title | CHARLES TRUCCO Digitally signed by CHARLES TRUCCO Date: 2025.09.30 08:12:07 -05'00', Associate Director of Operations Support |
| System Owner Signature | CHARLES TRUCCO Digitally signed by CHARLES TRUCCO Date: 2025.09.30 08:12:33 -05'00', Associate Director of Operations Support |
| Approved Signature & Title | MARK BLYTHE Digitally signed by MARK BLYTHE Date: 2025.10.15 11:27:14 -05'00', Director of Field Service |
| PTA Control Number (if a PTA was submitted prior to PIA) | PTA- |
| PIA Control Number | PIA- 20250925-001 |

# Description of G-514, Privacy Impact Analysis elements:

The contact point completes items on the G-514 beginning with the Overview through Section 9 and the preparer's signature in the Certification box. The system owner completes the second signature box. The last signature box and the PTA/PIA control numbers are completed by IRMC.

**Overview**

Begin with a three sentence highlight, as follows:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

A clear and concise overview of the system gives the reader the appropriate context in which to view the remainder of the PIA. In total, the overview should cover all of the following, clearly and concisely:

- The system name, the unique number if there is one, and the name of the bureau or office that owns the system;
- The objective or purpose of the new or revised system, sub-system, application, or technology, and how it relates to the agency, bureau or office mission;
- A general description of the information in the system;
- A description of a typical transaction conducted in the system;
- Any information sharing done by the system, sub-system, or application;
- A general description of the modules and subsystems, where relevant, and their functions. (You may continue in an Appendix if the overview would exceed one page.)
- The authority under which the system or program operates.

**Section1.0 The System and the Information Collected and Stored within the System.**

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

1.1.1 Identify and list all of the types of information in identifiable form that are collected and stored in the system that either directly identify an individual (such as name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique identifying number, code, or characteristic) or when combined, indirectly identify an individual (such as a combination of gender, race, birth date, geographic indicator, license number, vehicle identifier including license plate, and other descriptors).

1.1.2 In some cases, a general summary of the information may be put in the first section and an appendix with the full list may be added to the back of the PIA.

1.1.3 Do RRB system data fields exist for this information and/or do fields need to be created?

1.2 From whom is the information collected?

1.2.1 List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual, as in the case of an investigator taking a statement from a suspect, or is it collected other sources, such as commercial data aggregators?

1.2.2 Describe why information from sources other than the individual are required. For example, if a program is systematically incorporating databases of information in identifiable form that are purchased or obtained a commercial aggregator of information or if information needs to

be collected third parties in an ongoing investigation, state the fact that this is where the information is coming from and then in 2.1 indicate why the program is using this source of data.

**Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.**

2.1 Why is the information being collected?

2.1.1 In responding to this question, you should include:

2.1.1.1 A statement of why this particular information in identifiable form that is collected and stored in the system is necessary to the organizations or to the RRB's mission. Merely stating the general purpose of the system without explaining why particular types of information in identifiable form should be collected and stored is not an adequate response to this question.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

2.2.1 In responding to this question, include:

- the status of any information collection clearances with OMB, including the OMB numbers of any approved collections (see Directive Circular IRM-9, *Public Reporting Requirements of the Paperwork Reduction Act*),
- citation of any other authorities that permit or require collection of the information (law, regulation, directives, etc.); specify authority for collection of SSN.

2.3 *Privacy Impact Analysis*: Given the amount and type of data collected, as well as the purpose discuss what privacy risks were identified and how they were mitigated. For example, if during the design process, a decision was made to collect less data, include a discussion of this decision.

**Section 3.0 Uses of the System and the Information**

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

3.1.1 Identify and list each intended use (internal and external to the agency) of the information collected or maintained.

3.1.2 If a SORN is being or has been published for the system, the routine uses for the SORN should be listed in this section. (List the applicable SORNs and/or Federal Register Notices.) In addition, list the uses internal to the RRB since the routine uses listed in the SORN are limited to disclosures made outside of the agency.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (e.g., data mining)?

3.2.1 Many systems sift through large amounts of information in response to a user inquiry or programmed. This is loosely known as data mining. When these systems sift through information they make determinations and, sometimes, conclusions based upon the information they analyze. If the system being analyzed in the PIA conducts such preliminary and conclusory functions, please provide greater detail on what type of determination the system makes

3.2.2 If the system creates or makes available new or previously unavailable information about an individual, what will be done with the newly derived information? Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to government employees who make determinations about the individual? If so, explain under what circumstances that information will be used and by whom.

3.3 How will the information collected from individuals or derived by the system, including the system itself be checked for accuracy? In responding to this question address the following where applicable:

3.3.1 Explain whether information in the system is checked against any other source of information (within or outside your organization) before the information is used to make determinations about an individual. If not, explain whether your organization has any other rules or procedures in place to reduce the instances in which inaccurate data is stored in the system.

3.3.2 If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

3.5. *Privacy Impact Analysis*: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses and describe why the information is being retained for the indicated period. For example, is appropriate use of information covered in training for all users of system? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

## Section 4.0 Sharing and Disclosure of Information within the System

The following questions are intended to describe the scope of sharing both within the Railroad Retirement Board and with other recipients.

4.1 With which internal organizations of the agency is the information shared?

4.1.1 Identify and list the names of any organizations, offices, and any other organizations within the RRB with which the information is shared.

4.2 For each recipient organization or office, what information is shared and for what purpose?

4.2.1 If you have specific authority to share the information, please provide a citation to such authority.

4.2.2 Identify the specific information that is shared with the specific information that is shared with the specific organization office, or organization within the RRB and the purpose served by such sharing.

4.3 How is the information transmitted or disclosed?

4.3.1 Is the information shared in bulk, on a case by case basis, or does the sharing partner have direct access to the information?

4.3.2 Describe how the information is transmitted to each organization or office and any other organization within the agency. For example, is the information transmitted electronically, by paper, or by some other means?

4.4 *Privacy Impact Analysis*: Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, if another Agency organization, office, or organization has access to the system that your office controls, discuss how access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing of information.

## Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to the RRB which includes Federal, state and local government, and the private sector.

5.1 With which external (non-RRB) recipients is the information shared?

5.1.1 Identify and list the name or names of the foreign, federal, state, or local government agencies, private sector organizations, or individuals with the information is shared.

5.2 What information is shared and for what purpose?

5.2.1 Identify the specific information that is shared with each specific recipient and the purpose served by such sharing. For example, the Federal Bureau of Investigation (FBI) may share its information on an individual with Customs and Border Protection. If you provided a list of

routine uses in response to Question 3.1, please reference that fact. You do not need to list them again here.

5.2.2 Where you have a specific to share the information, please provide a citation to or copy of the authority.

5.3 How is the information transmitted or disclosed?

5.3.1 Is the information shared in bulk, on a case by case basis, or does the organization have direct access to the information?

5.3.2 Describe how the information is transmitted to entities to the agency and whether it is transmitted electronically, by paper, or some other means.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared? If possible, include a reference to and quotation from any MOU, contract, or other agreement that defines the parameters of the sharing agreement.

5.5 What type of training is required for users from agencies outside the agency prior to receiving access to the information?

5.6 Are there any provisions in place for auditing the recipients' use of the information?

5.7 *Privacy Impact Analysis*: Given the external sharing, what privacy risks were identified and how were they mitigated? For example, if an MOU, contract, or agreement is in place, what safeguards (including training, access controls, and security measures) have been implemented by the external agency to ensure that information is used appropriately?

## Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to the collection of information?

6.1.1 If yes, identify the form, a citation or a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice [link] published in the Federal Register. If no form of notice was provided, explain why not.

6.1.2 Was the person aware that his or her information was being collected?

6.2 Do individuals have the opportunity and/or right to decline to provide information?

6.2.1 Can the person, from whom or about whom information is collected, decline to provide the information and if so, is there any penalty or denial of service that is the consequence of declining to provide the information?

6.3 Do individuals have an opportunity to consent to particular uses of the information? If such an opportunity exists, what is the procedure by which an individual would provide such consent?

6.4 *Privacy Impact Analysis*: Conspicuous and transparent notice allows individuals to understand how their information will be used and disclosed. Describe how notice for the system was with these principles in mind or if notice is not provided, what was the basis for this decision.

## Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him or her:

7.1 What are the procedures that allow individuals the opportunity to seek access to or redress of their own information?

7.1.1 Cite any procedures or regulations (other than the Agency's FOIA/Privacy Act regulations) that your organization has in place that allow an individual to seek access to or amendment of his or her information. For example, if your organization has a customer service or

outreach unit, that information, along with phone and contact information, should be listed in this section in addition to the agency's procedures.

7.1.2 If the system is exempt the access or amendment provisions of the Privacy Act, explain the basis for the exemption or cite the regulation implementing the exemption.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

7.3.1 Are there other agency procedures that can be utilized by the individual with respect to this information?

7.4 *Privacy Impact Analysis*: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

## Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

8.1.1 Identify and list the types of users. For example: managers, system administrators, contractors, and developers may have access to the system.

8.2 Will contractors to the RRB have access to the system?

8.2.1 If so, please submit a copy of the contract describing their role with this PIA.

8.3 Does the system use "roles" to assign privileges to users of the system?

8.3.1 Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be able to make certain amendments or changes to the information.

8.4 What procedures are in place to determine which users may access the system and are they documented?

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

8.8 Is the data secured in accordance with FISMA requirements?[1] If yes, when was Certification and Accreditation (C&A) last completed?

8.9 *Privacy Impact Analysis*: Given the access and security controls, what privacy risks were identified and how they were mitigated. For example, were decisions made to encrypt certain data sets and not others?

## Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

[1] Contact the Chief Security Officer in IRMC for guidelines.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

9.3 What design choices were made to enhance privacy?

## Conclusion

The concluding section should inform the reader, in a summary fashion, how you constructed your system, program, or technology based on privacy risks and mitigation strategies.