

Privacy Impact Assessment

1. Contact Information

<p>A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services</p>

2. System Information

- (a) Name of system: Event Brite
- (b) Bureau: EUR
- (c) System acronym: Event Brite
- (d) iMatrix Asset ID Number: 245317
- (e) Reason for performing PIA:
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable):

3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
 X Yes No
- (b) What is the security Assessment and Authorization (A&A) status of the system?
Currently in the Assessment Phase. Just received P/DCIO Qualify Approval Memo.
- (c) Describe the purpose of the system:
Event Brite allows users to create, share, find and attend public events. Offices are able to post a public event on the Event Brite website and on their own webpage such as an Embassy website. Individuals interested in participating in an event may RSVP online to reserve a spot. This platform will only be used for Embassy hosted events outside of the Embassy.
- (d) Describe the PII that the system collects, uses, maintains, or disseminates:

The PII collected is required to send out notices of Embassy events and to document the status of RSVPs by participants. The PII includes full names, emails and company affiliations.

NOTE: While other fields are available in the user profile, they are not collected by the Department. However individuals are able to use the platform for non-Embassy hosted events and, as such, may populate additional fields at their own discretion. These fields include: telephone, website, gender, date of birth, age along with credit card information. In the event credit card information is entered it is encrypted with strong industry-standard cryptographic protocols such as AES and SSL while in transit through our systems. Embassy hosted events are free and do not require payment, so credit card information will not be collected.

- (e) What are the specific legal authorities and/or agreements that allow the information to be collected?

22 U.S.C. 2651a, Organization of the Department of State.

- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes If yes, provide:

- SORN Name and Number: Protocol Records, State-33
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): February 26, 2016

No If a SORN is not required, explain how the information is retrieved without a personal identifier.

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes No

If yes, please notify the Privacy Division at Privacy@state.gov.

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)):
 - Type of information retained in the system:
 - Length of time the information is retained in the system:
- As the system is currently unscheduled, all records will be maintained indefinitely (no records will be destroyed/deleted). Program offices are engaged with relevant officials in A/GIS/IPS to create and finalize a record schedule for submission to the National Archives and Records Administration for appraisal and ultimate approval.

4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
 U.S. Government employees/Contractor employees
 Other

- (b) Does the system contains Social Security Numbers (SSNs), if so, is the collection necessary?

Yes ____ No X

- If yes, under what authorization?

- (c) How is the information collected?

Individuals consent and provide their contact information to Embassy personnel for inclusion in the contact management database (CMD). Based on individuals' interests, Embassies send invitations to hosted event via Event Brite. Individuals can create an account on the Event Brite website and voluntarily populate any field in the User Profile .

- (d) Where is the information housed?

- Department-owned equipment
 FEDRAMP-certified cloud
 Other Federal agency equipment or cloud
 Other

- If you did not select "Department-owned equipment," please specify.

Amazon EC2 is part of the FedRAMP approved GovCloud and US East/West US Public Cloud.

- (e) What process is used to determine if the information is accurate?

The website has certain requirements to create an account. This information must be verified by confirmation emails with the individuals. It is up to the individual to verify information is accurate. Embassy staff will review all RSVP's and contact any invitee if further verification is needed.

- (f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

It is up to the individual to maintain the accuracy of his or her own account profile.

- (g) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use information from commercial sources nor publicly available information.

- (h) Is notice provided to the individual prior to the collection of his or her information?
 There is a website privacy link available during the registration process.
 The individual participant voluntarily provides all of the necessary information to the website.
- (i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes No

- If yes, how do individuals grant consent? Individuals voluntarily register through the website. During the registration there is a step that involves agreeing to the terms of service, Privacy policy and cookie policy. Each policy is hyperlinked to the policy page for review.

- If no, why are individuals not allowed to provide consent?

- (j) How did privacy concerns influence the determination of what information would be collected by the system?
 The PII in this system is entered voluntarily by the individual. The information required for RSVPs are full names and company/school. This amount of PII limits the potential harm to individuals.

5. Use of information

- (a) The intended use(s) for the information is/are:
 The name and company/school will be used to verify the invitee's RSVP to an event.
- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
 Yes, the information given to Event Brite is minimal to the effect of securing a place at an event. It only collects the information required.
- (c) Does the system analyze the information stored in it? Yes No

If yes:

- (1) What types of methods are used to analyze the information?
 Past events are analyzed to determine events attended by the individuals.
- (2) Does the analysis result in new information?
 Yes, it will provide the individual with events similar to ones they have attended in the past.
- (3) Will the new information be placed in the individual's record? Yes No

- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
Yes ____ No X

6. Sharing of Information

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Information will be shared with the event organizer, Public Affairs Officer, RSO and Executive Office. The event organizer (normally Protocol) will only use the necessary information for the check-in process.
- (b) What information will be shared?
The only information to be shared will be full name, email address and company/school.
- (c) What is the purpose for sharing the information?
The RSO may need to review the invite lists for security screening. Executive Office may need to review in order to identify who will be attending, i.e., any VIPs.
- (d) The information to be shared is transmitted or disclosed by what methods?
The list may be transmitted via OpenNet or hardcopy.
- (e) What safeguards are in place for each internal or external sharing arrangement?
OpenNet has a DS technical security standards in place. Paper version will stay in the possession of Embassy staff. The information within the website will be protected using 256-bit Secure Socket Layer (SSL) encryption.
- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
The information within Event Brite's website is within the control of registered users. While there is more information available in user profiles, only name, email and company/school affiliation will be used for Embassy-hosted events. When information containing PII is shared within our offices it will be on a need to know basis. Information sharing will be limited to Protocol, Public Affairs, RSO and Executive Office.

7. Redress and Notification

- (a) What procedures allow individuals to gain access to their information?
Users can access their own account information from the website or from an app that is available on many mobile devices.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information? Yes No

If yes, explain the procedures.

The account information and account settings is fully editable by the user; provided they have successfully authenticated their own credentials.

If no, explain why not.

- (c) By what means are individuals notified of the procedures to correct their information? Event Brite notifies registered users about the ability to correct user profiles.

8. Security Controls

- (a) How is the information in the system secured?

The system uses an Advanced Encrypted Standard (AES) 256 bit encryption.

The system is also International Organization for Standardization (ISO) certified using the Information Security Management System 27001. The system has been verified and audited by the Statement on Auditing Standards (SAS) No. 70, Service Organizations.

This certifies this service has been through an in-depth examination of their control objectives, control activities and controls over information technology.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

Access to the organizer portion, the Embassy’s organizer account credentials, will be limited to the Protocol office and the Public Affairs Officer.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Access to the organizer account by the Protocol Officer and Public Affairs Officer will provide a check and balance on misuse.

- (d) Explain the privacy training provided to authorized users of the system.

In-House training will be provided to all users of the system. The users will be thoroughly trained in the protection of PII. Currently, Department of State personnel are trained annually in cyber security and the protection of PII.

- (e) Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users? Yes No

If yes, please explain.

The system requires a 2 factor authentication (Username and Password). Password requirements of: minimum 4 characters of capital and lowercase letters, numbers, but special characters are not required.

The connection uses a 256 bit Secure Socket Layer (SSL) encryption. There is also 24 hour monitoring in place by a dedicated security team. This security team has tools in place that monitor the network, detect and identify possible intrusions.

- (f) How were the security measures above influenced by the type of information collected? Based upon the Event Brite's security and privacy policy we feel safe collecting only names and company/school for RSVPs. Also, the information provided is completely voluntary, in which there is an agreement that must be clicked during registration process.

9. Data Access

- (a) Who has access to data in the system?
Only Protocol and Public Affairs will have access to Embassy-hosted events and RSVP statuses of participants. Within Event Brite's organization all employees are subject to reference, education, and other personnel checks. Certain employees are also subject to detailed background checks.
- (b) Access to data in the system is determined by:
Access to the data within EventBrite is determined solely by need. Those who do not require access to this data will not be given permission to access the system.
- (c) Are procedures, controls or responsibilities regarding access to data in the system documented? Yes No
- (d) Will all users have access to all data in the system or will user access be restricted?
Please explain.
No, users will not have access to all of the data in the system. As it is a public website, some profile information may be public and may be able to be seen by others. This information which can be seen is entirely voluntary by the user; they can choose what information is public or private. PII and credit card information is never shared.
- (f) What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?

The Public Affairs Officer and Protocol Officer will have full control of the data and the system. At this time there is no concern of unauthorized browsing as they will have full need-to-know of anyone RSVP'ing to an Embassy hosted event.