Third Party Application Privacy Impact Assessment

Department of State Privacy Coordinator Bureau of Administration Global Information Services Office of Information Programs and Services	
Name of Third Party Application: Cvent Inc **ITAB Number:** **Month and Year PIA was completed:** February 2016	

1) Purpose of the Department of State's use of a third-party website or application. (Henceforth, third-party website or applications will be referred to as third party applications.)

(a) Give a general description of the third party application.

The Cvent Inc. application stores personal or contact information about individuals or personnel applying, invited to/attending, or supporting Department of State hosted or co-sponsored functions, events and conferences.

(b) What is the specific purpose for using the third-party application and how does this purpose assist in accomplishing the Department's mission?

The application is used to track and coordinate information about individuals applying or invited to, attending, or supporting Department of State events. It assists the Department by advancing core representational, public diplomacy and organizational objectives inherent in hosted event opportunities.

(c) Is the use of the third-party application consistent with all applicable laws, regulations, and policies? Yes, contingent on forthcoming limited approval for cloud services by the Department's Authorizing Official.

(d) What federal authorities permit the collection of information for the intended purpose of this application?

22 U.S.C. 2621, 22 U.S.C. 2625, 22 U.S.C. 4301 et seq.

2) Personally Identifiable Information (PII*)* available through the use of the third-party application.

(a) What PII will be made available to the Department?

Personally identifiable information may include contact information, address and occupation of invitees, biographical information (e.g., names, nationalities/citizenship, gender, copies of passport/visa, passport or government identification number, dates of birth, photograph), travel information (air/ground transportation, lodging), representational information; personal preferences (e.g. dietary restrictions) or occupational information (resumes, curricula vitae, portfolio samples, work references.)

(b) What are the sources of the PII?

The source of information is individuals submitting their personal details into the system. In some cases, a U.S. government official may be designated as a liaison officer ("LO") to work in a coordination capacity with a foreign delegation or a group of individuals, and would then be responsible for collecting and verifying information on the group's behalf. In such cases, after clearing and verifying the compiled information with their foreign or Embassy counterpart, the LO would submit directly to Cvent, or to an administrator from the Office of Chief of Protocol or Major Events and Conferences Staff for manual upload to the application.

(c) From which individuals is the information collected?

The application collects from individuals applying for registration or accreditation to these events, including members of the general public and private sector; foreign government officials and members of the Diplomatic Corp; news media; members of the military and/or federal, state or local government agencies.

(d) Does this collection of information require compliance with the Paperwork Reduction Act (PRA) and, if so, how will the Department comply with the statute?

The collection of information will require compliance with the Paperwork Reduction Act; M/MECS is currently in consultation with OMB and A/GIS/DIR for the package submission associated with PRA public comment, justification and clearance/approval and will update this PIA accordingly once completed.

3) Intended or expected use of PII

(a) How will the Department use the PII described in Section 2 above?

The information will be collected to maintain a list of individuals invited to or participating in an event; the PII will be used to comply or comport with event security parameters maintained by the U.S. Department of State's Diplomatic Security Service (DSS) or U.S. Secret Service (USSS), including background or access namechecks performed by either respective security agency.

(b) Provide specific examples of how the PII may be used.

During an event or function with high-level principal participation (e.g. The President, Secretary of State, etc.), the U.S. Secret Service Dignitary Protection Division

(USSS/DPD) will often require personally identifiable information to assess the criminal history of attendees, personnel and the news media through a "namecheck." This is secondary and complimentary to the primary registration and accreditation of the event, which requires a significant amount of non-PII (e.g. contact details, attendance or dietary preferences, travel accommodations, etc.) to be collected. The system will allow for significantly stronger security by requiring only a single point collection from each individual and ensure participant data is coordinated and maintained in a single repository instead of multiple and overlapping databases.

4) Sharing or disclosing PII

(a) With what entities or persons inside or outside the Department will the PII be shared and for what purpose will the PII be disclosed?

The PII may be shared with federal, state or local law enforcement or security agencies, including the military and the Executive Office of the President, and in limited cases, private entities. The majority of information sharing is for security agencies requiring PII to conduct background checks for close proximity to high-level principals or for venue/property access. In many other cases, information may be required to share for the logistics associated with hosting an event (e.g. identification of individuals for seating and/or catering needs; coordination of transportation or accommodations for event participants); or preparatory activities in the lead-up to a function (e.g. issuance of invitation, selecting applicants for participation), which may require coordination or collaboration with a private entity.

The information would be provided upon request and approval of the Office of the Major Events and Conferences Staff (M/MECS) or the Office of the Chief of Protocol (S/CPR).

(b) How will the PII be transmitted or disclosed to internal or external entities or persons?

When applicable, the information would be exported to an MS Excel report and transmitted directly with the internal/external point of contact.

(c) What safeguards will be in place to prevent uses other than those legally authorized and described in this PIA?

Risks to privacy are mitigated by limited release of personal information and only when necessary, in addition to limited access to the system governed by the principles of separation of duties and least privilege. Personnel with system access are limited to authorized Department of State employees.

Cloud-based collection or storage of information poses risks related to confidentiality (e.g. security or malicious compromise), integrity (e.g. version control or inadvertent duplication of data), availability (e.g. operational issues or discontinuation in service provisioning), legal (e.g. geolocation of datacenter and associated regulatory frameworks).

Cvent Inc. system architecture is designed for logical segregation, and utilizes columnar encryption – through a dual-key management - and filtering to ensure data separation within their multi-tenant cloud. Additionally, Cvent is complimenting these efforts through an impending migration that will encrypt all customer data at rest under AES 256 standards. Additional infrastructure measures at the U.S.-based datacenter (including 24/7/365 monitoring by security officers, exterior fencing and asset protection, biometric authentication for facility entrance, individualized secure space with restricted access to pre-authorized Cvent personnel only, and continuous closed-circuit camera surveillance) assure physical safeguards of the PII within the cloud.

A limited number of Cvent system administrators – those achieving a data security corporate certification and satisfactory completion of a background check -- can access data records within the system. All activity by Cvent system administrators is closely logged and audited, and Cvent expects the aforementioned forthcoming system migration will consequently restrict all access to user/client records.

MECS is working with Cvent to implement necessary contractual modifications to ensure the company shall limit and appropriately monitor the number of personnel in order to protect data and PII against unauthorized access, disclosure or modification.

5) Maintenance and retention of PII

(a) How will the Department maintain the PII and for what time period?

As the proposed system is currently unscheduled, the system and any records must be retained indefinitely. M/MECS is consulting with A/GIS/IPS and NARA officials to develop an appropriate records disposition schedule. However, M/MECS and S/CPR propose that sensitive PII, once no longer needed for an event, would be destroyed or deleted.

(b) Is there a records disposition schedule covering this collection? If so, what is the retention period?

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.

6) Securing PII

(a) Will the Department's privacy and security officials collaborate to develop methods for securing PII?

Yes, MECS and CPR are engaged with IRM (OCA, A) to discuss further security

measures and protocols (e.g. administrative, technical, physical) and the A Bureau (A/GIS/IPS) to safeguard contained PII.

(b) Describe how a user will access the third party application.

Access to the system is limited to authorized staff requiring the information in the performance of their official duties. M/MECS and S/CPR will develop user access agreements, advising relevant personnel to abide by the following standard procedures for handling PII:

- Do not inspect, search or browse records of PII in files or databases unless you are authorized to do so in the performance of your official duties and you have a need to do so to accomplish your assigned work.
- Do not alter or delete records containing PII unless it is necessary in the performance of your official duties.
- Do not disclose PII to others, including other authorized users, verbally or otherwise, unless there is a need to do so in the performance of your official duties.
- Do not reveal your password to others or allow them to log on under your account.
- Do not leave your work area without first locking your computer.
- Do not store PII in shared electronic folders or shared network files.
- Do not email PII in an unencrypted form without first evaluating the potential harm to the individuals if their PII was unexposed.
- Do not leave hard copy PII records exposed and subject to theft.

Department of State employees access the system web-based user interface requiring password protection, a single sign-on (SSO) configuration adhering to SAML 1.1/2.0 protocols.

7) Identifying and mitigating other privacy risks

What other privacy risks exist and how will the Department mitigate those risks?

Overall privacy risks associated with the system are related to the accuracy of individual data input into Cvent, unauthorized access and inappropriate dissemination of participant data, longevity of data retention, external sharing of participant data, and risks associated with individual access to stored information. M/MECS has developed mitigation strategies to address all of the identified privacy risks, most of which are discussed in this PIA.

8) Creating or modifying a system of records

(a) Is there an existing system of records to cover this collection of records as required under the Privacy Act of 1974?

Yes

(b) If "yes" to the question above, which system of records notice (SORN) covers this collection? (For a list of all Department published SORNS, go to www.state.gov/m/a/ips/c25533.htm).

State-33, "Protocol Records" (as published Friday, September 6, 2013 and will be updated and republished early 2016)

If there is no existing Department SORN to cover this collection, one must be created. Please contact SornTeam@state.gov for guidance.

(c) Is notice provided to the record subjects, other than through the SORN (e.g., through a Privacy Act statement or privacy notice)?

Event participants or applicants will be notified prior to collection of their information through a privacy notice posted to the online registration/submission portal home screen. At the home screen, individuals will also be notified they may be added to contact lists for further information about the event, or that limited contact details may be provided to additional involved stakeholders, and will have the option to opt-in.

In the case of U.S. Liaison Officers compiling information, individuals would be informed of the information submission requirements and reasons for collection through various guidance documents, briefings, or correspondence by U.S. counterparts (e.g. Summit delegation or Event Information guides, invitational logistics briefings etc.)