Version Number: 01-2019

U.S. Department of Commerce
National Institute of Standards and Technology (NIST)

Privacy Impact Assessment
for the
107-02 Public Affairs Office System

Reviewed by: Susannah Schiller, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.08.13 16:02:28 -04'00' 08/12/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 107-02

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The Public Affairs Office (PAO) provides communications support to help NIST share its research results, services, and programs; to assist policymakers in learning about NIST's role and activities; and to advise and assist NIST managers on public affairs and policy strategies. In support of this mission, the Public Affairs Office System includes a cloud-based application that enable marketing and event management professionals to administer and track events through marketing automation, payment processing, and reporting.

a) Whether it is a general support system, major application, or other type of system
The Public Affairs Office System is a general support system.

b) System location
The component utilizes cloud services based in California, with facilities located in: Virginia, California, Oregon, and Ohio.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
Attendance information is shared amongst conference participants if they provide consent. NIST shares attendee information with other internal NIST information systems. Payment is sent directly to pay.gov.

d) The way the system operates to achieve the purpose(s) identified in Section 4
NIST staff administers a web registration site using an application.

e) How information in the system is retrieved by the user
Information is not retrieved by the user.

f) How information is transmitted to and from the system
Members of the public register for attendance at a conference hosted at the NIST facility. The registration process requires setup of a profile, to include information regarding payment for the conference, and required information for facility access. Mobile application access is afforded to enable efficiency when on-site registering.

g) Any information sharing conducted by the system
Attendance information is shared amongst conference participants if they provide consent. NIST shares attendee information with other internal NIST information systems. Payment is sent directly to pay.gov.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.
5 U.S.C. 301; 44 U.S.C 3101.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system is Moderate

Section 1: Status of the Information System

1.1 The status of this information system:

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
Passport
Other identifying numbers:

Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)
Name
Gender
Date of Birth
Place of Birth
Home Address
Telephone Number
Email Address
Other general personal data
Other general personal data:
Passport issuing country, citizenship, country of residence, permanent US. residency.

Work-Related Data (WRD)
Occupation
Job Title
Work Address
Work Telephone Number
Work Email Address
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
Other system administration/audit data:

Other Information

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
Hard Copy - Mail/Fax
Online
Other:

Government Sources
Other:
Passport issuing country, citizenship, country of residence, permanent US. residency.

Non-government Sources
Other:

2.3 Describe how the accuracy of the information in the system is ensured.

The registration process requires setup of a profile, to include information regarding payment for the conference, and required information for facility access. The accuracy of this information is up to the registrant. If a payment information is not correct, notification is sent to the registrant, verifying the accuracy of payment data.

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

No

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?

No

The IT system supported activities which raise privacy risks/concerns.

Activities
Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
For administrative matters
Other:

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Personally Identifiable Information and Work-Related Data is used for registering members of the public for conferences and facility access, which may include federal employees/contractors. **For U.S. citizens, information collected includes name, business address, business phone, and business email address.** **For foreign nationals, information collected also includes date of birth, place of birth, passport number, issuing country, business title, employee's sponsor, gender, citizenship, country of residence.**

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data). **lnformation collected is directly from the attendee, and is limited to only that which is needed for conference registration, payment, and access to the event. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.**

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Case-by-Case - Within the bureau
Other:

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
Government Employees
Other:

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. **Yes, notice is provided by a Privacy Act statement and/or privacy policy.**
The Privacy Act statement and/or privacy policy can be found at:
The Privacy Act statement and/or privacy policy can be found at: https:www.nist.gov/privacy-policy
The reason why notice is/is not provided:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

Yes, individuals have an opportunity to decline to provide PII/BII.
The reason why individuals can/cannot decline to provide PII/BII:
Individuals have an opportunity to decline, but in doing so will not be registered to attend a conference, nor provided facility access.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

Yes, individuals have an opportunity to consent to particular uses of their PII/BII.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
Individuals have an opportunity to consent to sharing their information with other conference attendees. **If consent is not given, the individual will be removed from the shared conference participant list, and their information will not be shared with internal NIST systems.**

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
After registering, individuals have opportunity to review/update information pertaining to them directly in the system.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

Staff (employees and contractors) received training on privacy and confidentiality policies and practices.

Access to the PII/BII is restricted to authorized personnel only.

Access to the PII/BII is being monitored, tracked, or recorded.
The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).

A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

Reason why access to the PII/BII is being monitored, tracked, or recorded:

Access logs are kept and reviewed for anomalies on an as needed basis.

The information is secured in accordance with FISMA requirements.

Is this a new system? No
Below is the date of the most recent Assessment and Authorization (A&A).
04/30/2019

Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies on an as needed basis. Authorized users must initiate access from NIST- owned devices. To guard against the interception of communication over the network, the components use the Transport Layer Security (TLS) protocol which encrypts communications between the application and the public.

Sensitive information is encrypted at rest. The component utilizes cloud services located in: Virginia, California, Oregon, and Ohio.

Payment information is sent directly to pay.gov.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?
Yes

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
Commerce/DEPT-2: Accounts Receivable **Commerce/DEPT-6: Visitor Logs and Permits for Facilities Under Department Control** **Commerce/DEPT-23: Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs**
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
General Record Schedule 6.4 (GRS 6.4/020) **NIST Records Schedules items 51 - 53**
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Shredding **Deleting**
Other disposal method of the PII/BII:

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Data Field Sensitivity**	**Identifiability-Users registering in the system could be identified by name.** **Data Field Sensitivity-The data collected through the data fields during registration are considered to be PII.**

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data). **Information collected is directly from the attendee, and is limitcd to only that which is needed for conference registration, payment, and access to the event. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

No, the conduct of this PIA did not result in any required business process changes.
Explanation

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

No, the conduct of this PIA did not result in any required technology changes.
Explanation