

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



**Privacy Threshold Analysis
for the
107-02 Public Affairs Office System**

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 107-02

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- 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 purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from 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 (Certain Registration System) 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 Ohio, 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.

There is an Application Programming Interface (API) integration between Certain Registration (SSP 107-02) and the Visitor Registration System (VRS) (SSP 137-01) to automatically pull NIST-1260 information for foreign event/conference attendees. All visitors will be checked against the pre-registered data through the Visitor's Center application during check-in.

d) The purpose that the system is designed to serve

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.

e) The way the system operates to achieve the purpose

NIST staff administers a web registration site using an application.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

Identifying numbers, general personal data (GDP), and work-related data are collected, maintained, used, or disseminated by the system.

g) Identify individuals who have access to information on the system

NIST staff administers a web registration site using an application.

h) How information in the system is retrieved by the user

Information in the system is not retrieved by the application user (e.g., conference participant). NIST administrators have access to those application users who registered.

i) 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.

The VRS interfaces with Certain via an API web service to automatically pull NIST-1260 information and then push that data to the NAIS for DOC OSY review and approval.

Questionnaire:**1. Status of the Information System****1a. What is 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 01-2017 or later). (Skip questions and complete certification.)

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

1b Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Activities
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

4. Personally Identifiable Information (PII)**4a. Does the IT system collect, maintain, or disseminate sensitive personally identifiable information (PII)?**

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

The IT system collects, maintains, or disseminates sensitive PII about:

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.

Is a PIA Required?	Yes
--------------------	------------

CERTIFICATION

X The criteria implied by one or more of the questions above **apply** to the 107-02 Public Affairs Office System and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

The criteria implied by the questions above **do not apply** to the 107-02 Public Affairs Office System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Huergo, Jennifer Office: 101/A0907 Phone: 301-975-6343 Email: Jennifer.huergo@nist.gov Signature: _____ Date signed: _____	Chief Information Security Officer Name: Heiserman, Blair Office: 225/A155 Phone: 301-975-3667 Email: nist-itso@nist.gov Signature: _____ Date signed: _____
Co-Authorizing Official Name: Mroz, Joseph Office: 101/A1040 Phone: 202-7943923 Email: joseph.r.mroz@nist.gov Signature: _____ Date signed: _____	Authorizing Official Name: Sastry, Chandan Office: 225/B222 Phone: 301-975-6500 Email: chandan.sastry@nist.gov Signature: _____ Date signed: _____
Privacy Act Officer Name: Fletcher, Catherine Office: 101/A523 Phone: 301-975-4054 Email: catherine.fletcher@nist.gov Signature: _____ Date signed: _____	Chief Privacy Officer Name: Barrett, Claire Office: 225/B226 Phone: 301-975-2852 Email: claire.barrett@nist.gov Signature: _____ Date signed: _____