PRIVACY IMPACT ASSESSMENT (PIA)

National Institute of Standards and Technology
NIST Other Financial Management Systems

Unique Project Identifier (UPI): 006-55-01-01-02-7011-00

Project Description

The mission of NIST Other Financial Management Systems is to support the central financial operations of NIST.

This is a consolidated PIA for the IT systems listed in the table below.

Name of System	Social Security Numbers?	Other Personally Identifiable Information (PII)?	Business Identifiable Information?
NIST 107 01 - Public and Business Affairs Web Server	No	Yes	No
NIST 107 03 - Conference Registration System	No	Yes	Yes
NIST 160 01 - CFO/CHCO/CFMO Office System	No	Yes	No
NIST 162 03 - Travel Manager	Yes	Yes	No
NIST 162 05 - Corporate Information System	Yes	Yes	No
NIST 172 01 - Human Resources System	Yes	Yes	No
NIST 194 02 - Physical Security Boulder System	No	Yes	No
NIST 200-02 – NIST Associates Information System (NAIS)	Yes	Yes	Yes

OMB Control Numbers: Most of the information in these systems does not involve the collection of information from the public; therefore, Office of Management and Budget approval is not required.

1. What information is being collected?

NIST systems contain Personally Identifiable Information (PII), including Social Security Numbers (SSN), or Business Identifiable Information (BII) as a result of the following activities and as detailed in the preceding table:

- NIST host an array of conferences which are open to the public as well as invited guests. The registrants must provide name, title, address, US citizenship status, and other PII to facilitate admission to the NIST facility. In addition registrants must provide payment for the conference. When payment is made by credit card the card type, number and expiration date is required. All of this information is collected in the Conference Registration System.

- The administration and management of NIST employees, including contractors, and associates, also involves the collection and maintenance of the SSN, name, date of birth, performance rating, and other PII that relates to the employee, contractor, or associate. The NIST Associates Information System (NAIS) is collection point for all non-NIST associate information.

2. Why is the information being collected?

PII about researchers and visitors is collected to make travel arrangements, facilitate entry to NIST laboratories and use of facilities, and to ensure building security. Personal information about NIST employees and NIST associates (contractors, guest researchers, etc) is collected and maintained as part of the routine administrative functions of the federal government. BII is collected as part of the NIST accreditation and research activities.

3. What is the intended use of the information?

PII and BII are used to facilitate NIST research programs, to provide for the comfort and security of visitors, and to conduct the administration and management of NIST employees.

4. With whom will the information be shared?

Information may be shared with other NIST or Department of Commerce systems, in accordance with the Privacy Act and as specified in the system of records notices (SORNs) identified in the response to Question 8 below.

5. What opportunities do individuals or businesses have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can they grant consent?

NIST employees must provide information as a requirement of federal employment. Employees have the opportunity to consent to particular uses of the information when they accept employment with NIST. Conference registrants have the opportunity to pay by means other than credit card (check, postal money order, or cash). When applicants apply for employment online they are consenting to supply personal information. They can choose not to use the online application system.

6. How will the information be secured?

As required by FIPS 199, the NIST Laboratories systems and all their components were reviewed for the sensitivity of the information in them, and were determined to require protection appropriate for Moderate or Low Impact systems. All relevant policies, procedures and guidelines, including NIST Special Publication 800-53, have been followed to ensure the security of the systems and the information in them. The System

Security Plans on file with the NIST IT Security Officer contains additional details.

The systems are located in the NIST Gaithersburg Central Computing Facility (CCF) or the Boulder Data Center. Both data centers have key card control limiting access to authorized staff members.

All PII data is secured through the use of user identification and authentication (e.g., userid, password), and other access controls, as detailed in the appropriate System Security Plan.

7. How will the data extract Log and Verify requirement be met?

NIST is in the process of developing a Web based centralized logging system which will be in place by the end of September 2008. This system will track the following categories of information:

a. Who performed the extract,
b. When extract was done,
c. What was the extract,
d. Where was the extract taken from,
e. Has the extract been deleted and,
f. If not deleted after 90 days, to monitor that it is still needed in 90 day intervals.

Until this system is implemented NIST is using the following compensating controls to protect PII data:

a. No extracts of sensitive data may be copied on to portable media without a waiver approved by the DoC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.
b. All laptop computers allowed to store sensitive data must have full disk encryption.
c. All remote access to public NIST systems containing sensitive data must be encrypted. All remote access to internal NIST systems containing sensitive data must fully comply with DoC Remote Access Policy requirements.
d. All flexiplace/telework agreements for working off site require that adequate data protection be in place.
e. All Human Resource staff, Timekeepers, and Administrative Officers have signed Rules of Behavior that allow access to Time and Attendance data only via encrypted government computers.

8. Is a system of records being created under the Privacy Act (5 U.S.C. 552a)?

No, records contained in these systems do not constitute a new system of records within the meaning of the Privacy Act. However, the existing Privacy Act system of records notices (SORNs) apply to the following systems:

DEPT-1; Attendance, Leave, and Payroll Records of Employees and Certain Other

Persons
- 162-03 Travel Manager
- 162-05 Corporate Information System
- 172-01 Human Resources System

DEPT--2 Accounts Receivable
- 107-03 Conference Registration System
- 164-01 Commerce Standard Acquisition Standard Acquisition

DEPT--9 Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
- 162-03 Travel Manager

NBS--1 NBS Guest Workers
- 200-02 NIST Associates Information System

OPM/Govt-5 Recruiting, Examining, and Placement Records
- 172-01 Human Resources System

9. Are these records covered by an approved records control schedule?

Records created by individual areas using NIST Other Financial Management Systems are scheduled under the following National Archives and Records Administration (NARA) approved records retention schedules:
Paper copies/record copies - N1-167-92-1 Items 1, 2, 3, 6, 9, 10, 54, 55, 56, 59, 64, 69, 72, and 73; electronic copies - N1-167-00-01 Item 1, and 167-00-02 Item 1.
Paper copies/record copies - GRS 1 Item 4, 23, 25, 29, 30, 32, and 33; electronic copies - Item 43.
Paper copies/record copies - GRS 6 Item 1a; electronic copies - Item 12.
Paper copies/record copies - GRS 23 Item 1, 5, 7; electronic copies - Item 10.
Paper copies/record copies - GRS 18 Items 17 through 23; electronic copies - Item 30.

Point of Contact:

Bruce K. Rosen
Chief, Telecommunications and CIO Support Division
301-975-3299
bruce.rosen@nist.gov