# SUMMARY PRIVACY IMPACT ASSESSMENT (PIA)

## National Institute of Standards and Technology
## NIST Management Resources Systems

### Project Description

The mission of NIST Management Resources is to support central financial operations and provide an IT infrastructure that meets the general-purpose and high-end scientific computing needs of NIST scientists and engineers in a cost-effective, efficient and secure manner.

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 100 01 – Director's Office (DO) System | No | Yes | No |
| NIST 100 02 – Associate Directors' (AD) Office | No | Yes | Yes |
| NIST 107 02 - Public and Business Affairs System | No | Yes | No |
| NIST 107 03 - Conference Registration System (CRS) and Federal Business Conferences, Inc. (FBC) | No | Yes | Yes |
| NIST 160 01 - CFO/CHCO/CFMO Office System | Yes | Yes | Yes |
| NIST 162 01 – Commerce Business System (CBS) | Yes | Yes | Yes |
| NIST 162 03 - Travel Manager | Yes | Yes | Yes |
| NIST 162 05 – Corporate Information System | Yes | Yes | No |
| NIST 164 01 – Commerce Standard Acquisition Reporting System (CSTARS) | No | Yes | Yes |
| NIST 165 01 – Grants Management Information (GMIS) | No | Yes | Yes |
| NIST 172 01 - Human Resources System | Yes | Yes | No |
| NIST 180 01 – OISM Support System | Yes | Yes | Yes |
| NIST 181 01 – NIST Network Security | No | Yes | Yes |
| NIST 182 01 – NIST Managed Desktop System | No | Yes | Yes |
| NIST 183 01 – Applications Systems Division (ASD) Moderate Applications. | No | Yes | Yes |
| NIST 183 06 – Application Servers and Database System | No | Yes | Yes |
| NIST 184 10 – Internal Windows Enterprise Server | No | Yes | Yes |
| NIST 184 12 – NIST Central Computing Facility | No | Yes | Yes |
| NIST 190 01 – OFPM Office System | Yes | Yes | Yes |
| NIST 191 01 – Physical Security System Gaithersburg | Yes | Yes | No |

| Name of System | Social Security Numbers? | Other Personally Identifiable Information (PII)? | Business Identifiable Information? |
|---|---|---|---|
| NIST 191 02 – Emergency Notification System | No | Yes | No |
| NIST 194 02 – Physical Security (Boulder) System | Yes | Yes | No |

**OMB Control Numbers:** The information in these systems does not involve the general 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.

- The NIST Central Computing Facility includes the NIST data centers, the Central Computing Facility (CCF), and the Boulder Data Center, along with the Advanced Measurements Laboratory (AML) and the telephone switch room in Gaithersburg, MD.

- Data stored on these systems includes scientific computing/research, Tivoli System Management (TSM) backup data from registered NIST computers, Corporate Time (CT) calendaring, and email.

**2. Why is the information being collected?**

- The administrative data is being stored on these systems to support administrative computing services to NIST management, administrative, and financial offices/ staff in support of NIST activities and programs.

- The scientific data is stored on these systems to support the NIST technical staff in conducting both theoretical and experimental components of NIST scientific and engineering programs.

- PII about researchers and visitors is collected to make travel arrangements, facilitate entry to NIST laboratories and use of facilities, and ensure building security. Personal information about NIST employees is collected and maintained as part of the routine administrative functions of the federal government. BII is collected as part of 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 stored within the NIST Central Computing Facility is used within NIST for NIST personnel. The data is shared with National Finance Center (NFC) for the NIST payroll/benefits systems. All data shared within NIST and NFC systems is in accordance with the Privacy Act. 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?**

The information stored on these systems is controlled by application administrators. Opportunities are available within the individual systems for individuals or businesses to consent to particular uses of data. However, 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.

Visitors who provide information to facilitate travel are informed of the use of the information when it is requested and may decline to provide personal information.

Businesses which contract with NIST give their consent as part of the business arrangements needed to complete these transactions.

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.

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.

***Operational Controls:***

The IT systems are located at the NIST Gaithersburg Central Computing Facility (CCF), the Boulder Laboratories Data Center and the Advanced Measurements Laboratory, all of which have key card controls limiting access to authorized individuals.

NIST has implemented the following minimum requirements. Access to all systems is controlled, with access limited to only those support personnel with a demonstrated need for access. Systems are kept in a locked room accessible only by specified management and system support personnel. Each system requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination that grants access to the room housing the systems, and all visitors are escorted while in this room. All systems are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to automated information system resources caused by fire, electricity, water and inadequate climate controls.

***Technical controls:***

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 implemented web based centralized logging system that tracks:

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.

**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
- 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

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 Management Resources* 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.

*NIST Central Computing System* records created by individual areas using NIST Management Resources are scheduled under National Archives and Records Administration (NARA) approved record retention schedules:

Paper copies/record copies - N1-167-92-1 Items 9, 10, 25, 27, 28, 30, 31, 31, and 59.

Electronic copies - N1-167-00-01 Item 1, and 167-00-02 item 1.

Paper copies/record copies - GRS 1 Item 23; electronic copies - Item 43.
Paper copies/record copies - GRS 23 Item 1, 5, and 7; electronic copies - Item 10.
Paper copies/record copies - GRS 24 Items 1 through 11; electronic copies - Item 12.

**Point of Contact:**

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