PRIVACY IMPACT ASSESSMENT (PIA)

National Institute of Standards and Technology
NIST IT Central Support for Science

Unique Project Identifier (UPI): 006-55-01-26-01-7045-00

Project Description

The mission of the NIST IT Central Support for Science is to 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 PIA is for the IT system listed in the table below.

Name of System	Social Security Numbers?	Other Personally Identifiable Information (PII)?	Business Identifiable Information?
NIST 184 12 - NIST Central Computing Facility	No	Yes	Yes

OMB Control Numbers: Information in this system 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?

This NIST system contains Personally Identifiable Information (PII) and Business Identifiable Information (BII) as a result of the following activities:

- 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.
- The administration and management of NIST employees, including contractors, also involves the collection and maintenance of name, date of birth, performance rating, and other PII that relates to the employee or contractor, such as home address, home phone number, etc.

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, the comfort and security of visitors, and the administration and management of NIST employees, as indicated above.

4. With whom will the information be shared?

Information stored within these systems 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.

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 such 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. 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.

6. How will the information be secured?

As required by FIPS 199, the NIST IT Central Support for Science 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 Plan on file with the NIST IT Security Officer contains additional details.

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 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, these records do not constitute a system of records within the meaning of the Privacy Act, and a system of records notice (SORN) is not required.

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

Records created by individual areas using NIST IT Central Support for Science 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