PRIVACY IMPACT ASSESSMENT (PIA)

National Institute of Standards and Technology
NIST Laboratories Support Systems

Unique Project Identifier (UPI): 006-55-01-26-02-7021-00

Project Description

The mission of the NIST Laboratories is to develop technical standards for scientific disciplines, perfect new and better techniques for measuring adherence to those technical standards, and develop new ways to disseminate those scientific measurement techniques to the scientific research and business communities.

.

This is a consolidated PIA for the IT systems listed in the table below that support the activities of the NIST Laboratories, Research Centers, and associated research support activities..

Name of System	Social Security Numbers?	Other Personally Identifiable Information (PII)?	Business Identifiable Information?
NIST 200 01 - Technology Services Headquarters	Yes	Yes	Yes
NIST 210 03 - National Voluntary Lab Accreditation Program (NVLAP) Interactive Web Site	Yes	Yes	Yes
NIST 230 01 - Measurement Services Division System	No	Yes	Yes
NIST 230 03 - Information System to Support Calibrations (ISSC)	No	Yes	Yes
NIST 610 02 - NIST Center for Neutron Research- Lab and Admin Systems	Yes	Yes	No
NIST 620 01 - Center for Nanoscale Science and Technology System	No	Yes	No
NIST 820 01 - Manufacturing Engineering Laboratory Managed Infrastructure	Yes	Yes	Yes
NIST 830 01 - Chemical Science and Technology Laboratory Headquarter System	Yes	Yes	Yes
NIST 831 01 - Biotechnology Division System	Yes	Yes	Yes
NIST 836 01 - Process Measurements Division System	Yes	Yes	Yes
NIST 837 01 - Surface and Microanalysis Science Division System	Yes	Yes	No
NIST 838 02 - Physical and Chemical Properties Division System (Gaithersburg)	Yes	Yes	Yes
NIST 838 03 - Physical and Chemical Properties Division System (Boulder)	Yes	Yes	Yes
NIST 840 05 - Physics Administrative Support System	Yes	Yes	No

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 except for the following:

OMB NO: 0693-0003, National Voluntary Laboratory Accreditation Program (NVLAP) Information Collection System, for NIST 210-03.

OMB NO: 0693-0043, Generic Clearance for Usability Data Collections, which applies to all systems that involve information collection.

OMB NO: 0693-0046, U.S. Measurement Systems Biophotonics Survey.

1. What information is being collected?

NIST Laboratories support systems contain Personally Identifiable Information (PII), including Social Security Numbers (SSN), and Business Identifiable Information (BII) as a result of the following activities:

- NIST receives and processes applications from scientific researchers to visit NIST laboratories or participate in NIST research activities. The researcher must provide SSN or passport number, home address and phone number, and other PII to facilitate admission to the facility and temporary appointment as a research associate. Many NIST laboratories have vigorous visitor and research associate programs to facilitate the dissemination of NIST research and maintain professional relationships with researchers in the United States and foreign countries.

- NIST also receives and processes applications from corporations, partnerships, government organizations, and sole proprietorships for NIST accreditation as an associated laboratory or research center. In the case of a sole proprietor, this would require providing SSN and other PII such as home phone number or cell phone number, along with BII. As an example, the National Voluntary Laboratory Program (NVLAP) Interactive Web Site (NIWS) is the portal through which non-NIST laboratories may apply for NIST to accredit them to perform specific tests and calibrations.

- The administration and management of NIST employees, including contractors, also involves the collection and maintenance of the SSN, name, date of birth, performance rating, and other PII that relates to the employee or contractor.

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 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 is 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 may be shared with other NIST or Department of Commerce systems, 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 individuals grant consent?

NIST employees must provide information as a requirement of federal employment. Visitors are not required to provide personal identification information if they make their own travel arrangements. For the Divisions' BII data, the data provided is required to provide NIST calibration services. If such information is not provided, the calibration can not be performed. For laboratory accreditation, the data is in integral part of the voluntarily accreditation process.

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 to perform instrument calibrations 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 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 Plan on file with the NIST IT Security Officer contains additional details.

All users are authenticated via the NIST domain and have password-sensitive screen savers enabled. All systems are running Antivirus software, desktop management software, and spy-ware elimination software.

7. How is the data extract Log and Verify requirement being 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 Laboratories Support Systems are scheduled under these 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, 33, 34, 35, 36, and 59; and N1-167-98-1, items 1 through 4.
Electronic copies - N1-167-00-01, item 1; and N1-167-00-02, 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

Point of Contact:

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