PRIVACY IMPACT ASSESSMENT (PIA)

National Institute of Standards and Technology
NIST Technology Innovation Program

Unique Project Identifier (UPI): 006-55-01-27-02-7040-00

Project Description

The mission of the NIST Technology Innovation Program (TIP) is to provide cost-shared funding to industry to accelerate the development and broad dissemination of challenging, high risk technologies that promise significant commercial payoffs and wide spread benefits for the nation. The TIP General Support System provides automated support for receipt, evaluation, and selection of technology proposals from companies applying for TIP funding.

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

Name of System	Social Security Numbers?	Other Personally Identifiable Information (PII)?	Business Identifiable Information?
NIST 470-01 Advanced Technology General Support System	No	Yes	Yes
NIST 470-02 Advanced Technology Public Submission System	No	No	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 except for the following:

OMB NO: 0693-0009, Advanced Technology Program.

1. What information is being collected?

The TIP system contains Personally Identifiable Information (PII) and Business Identifiable Information (BII) because NIST receives and processes applications from companies seeking TIP funding. The proprietary and confidential information provided by the companies includes a variety of business information including detailed technical description of the project and company financial information; evaluations of technical performance and business reports on funded projects; and business reports from funded companies. The majority of this information is BII.

The names, phone numbers and addresses for individuals who perform reviews for TIP are also collected and stored in System 470-01.

System 470-02 serves as a staging area for holding data submitted to NIST from outside sources. Accordingly the BII it contains is only held in that system for a very few minutes until it is transferred to System 470-01.

The administration and management of NIST employees, including contractors, also involves the collection and maintenance of Continuity of Operations (COOP) data, and other PII that relates to the employee or contractor. That data is maintained in System 470-01.

2. Why is the information being collected?

Personal information about NIST employees and associates is collected and maintained as part of the routine administrative functions of the federal government. Specifically COOP contract lists are required for the functioning of the organization. PII and BII from outside sources are collected as part of the NIST TIP funding project.

3. What is the intended use of the information?

PII and BII are used to facilitate the work done under the NIST TIP.

4. With whom will the information be shared?

PII data is not shared with any other organizations, public or private. Reviewer information is shared only with TIP staff as needed. BII data may be published as aggregate statistics biannually in TIP's publication, "Measurements TIP Impact: Report on Economic Progress." The data is also used in an annual budget report of performance.

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 and how can they grant such consent?

NIST employees provide COOP contract information on a voluntary basis.

For the BII data, the data provided is required in order to be reviewed and considered for funding from the TIP. Submitting the application is voluntary, however, if such information is not provided, the company cannot receive funding. The companies give prior consent for information TIP publishes. The Economic Assessment Office of NIST TIP secures company approval of items published before making it public. Reviewer data is voluntary.

6. How will the information be secured?

As required by FIPS 199, the NIST TIP system and all components were reviewed for the sensitivity of the information in them, and were determined to require protection appropriate for Moderate 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 (470-01) on file with the NIST IT Security Officer contains additional details.

In addition to the common physical and environmental controls in place at NIST, TIP uses cipher locks for physical access control to the servers, access control for display medium, emergency shutoff, emergency power, temperature and humidity controls. All technical controls used for identification and authentication (e.g., userid, password), access control, audit and accountability, and system and communications protection are listed in section 4 of the 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 TIP are scheduled under National Archives and Records Administration (NARA) approved record retention schedules:

Paper copies/record copy - ATP Funded and Non-funded Proposals - N1-167-92-1 Items 37a. and b.
Electronic copies - N1-167-00-02 Item 1, and N1-167-00-01 Item 1.

Point of Contact:

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