

## PRIVACY IMPACT ASSESSMENT (PIA)

### National Institute of Standards and Technology NIST Baldrige National Quality Program

**Unique Project Identifier (UPI): 006-55-01-22-02-7030-00**

#### Project Description

The mission of the NIST Baldrige National Quality Program (BNQP) is to enhance the competitiveness, quality, and productivity of U.S. organizations for the benefit of all residents. The BNQP is a customer-focused federal change agent that: develops and disseminates evaluation criteria and manages the Malcolm Baldrige National Quality Award; promotes performance excellence; and provides global leadership in the learning and sharing of successful strategies and performance practices, principles, and methodologies.

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 102-01 – National Quality Program System	No	Yes	Yes

**OMB Control Numbers:** The collection of information in this system is covered by the Office of Management and Budget OMB No: 0693-0006, Malcolm Baldrige National Quality Award and Examiner Applications.

#### 1. What information is being collected?

The BNQP system contains Personally Identifiable Information (PII) and Business Identifiable Information (BII) because NIST receives and processes applications from Examiners and prospective Baldrige Award recipients. The information provided by the Examiners includes name, home/business address, home/business phone, education experience. A variety of applicant-specific proprietary/business sensitive information is stored in the system from the Baldrige Award application.

Additionally the administration and management of NIST employees, including contractors, also involves the collection and maintenance Continuity of Operations Plan (COOP) data, and other PII that relates to the employee or contractor.

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

PII is collected from potential Examiners to be used in the Examiner selection process, and then to later be used during the evaluation portion of the BNQP.

Personal information about NIST employees and associates is collected and maintained as part of the routine administrative functions of the federal government. Specifically COOP contact list are required for the functioning of the organization.

BII is collected as part of NIST BNQP Award process.

### **3. What is the intended use of the information?**

PII and BII are used to facilitate the Examiners review of the Award applications and prepare a scorebook of the applicants based on the applicant's responses to criteria. Also the PII obtained is used to ensure the comfort and security of visitors and the administration and management of NIST employees.

### **4. With whom will the information be shared?**

Information may be shared with BNQP staff, Examiners, and the Panel of Judges. The information may be accessed by staff from the American Society of Quality (ASQ), a contractor who supports the entire award application process, and by APPLYYOURSELF (AY), a developer and host of Baldrige Examiners application and related processes. All shared information 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 and how can they grant such consent?**

Examiner and Award applicants provide their information on a voluntary basis. However, to be considered for an Award, applicants must submit the required information. Applicants are informed of the intended uses of the information. NIST employees and contractors provide COOP contact information on a voluntary basis.

### **6. How will the information be secured?**

As required by FIPS 199, the NIST BNQP 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 on file with the NIST IT Security Officer contains additional details.

### **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; however, the existing NBS-3 Research Associates Privacy Act System of Records notice (SORN) does apply to some of the records in the system.

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

Records created by individual areas using NIST Baldrige National Quality Program System are scheduled under National Archives and Records Administration (NARA) approved record retention schedules:

Paper copies/record copy - N1-167-92-2 Items 1 through 10.

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