

**U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)**



**Privacy Threshold Analysis
for the
450-01 Baldrige Performance Excellence Program System (BPEP)**

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 450-01

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) Whether it is a general support system, major application, or other type of system*
- b) System location*
- c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) The purpose that the system is designed to serve*
- e) The way the system operates to achieve the purpose*
- f) A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) Identify individuals who have access to information on the system*
- h) How information in the system is retrieved by the user*
- i) How information is transmitted to and from the system*

The Baldrige Performance Excellence Program (BPEP) oversees the nation’s only Presidential award for performance excellence while offering a wide array of award-winning products and services, including the world-renowned Baldrige Excellence Framework. The function/purpose of the system is to support the electronic needs and activities of the internal and external customers in support of this mission. Components of this system include the Baldrige Examiner Applicant (BEA), Baldrige Online Scorebook Solution (BOSS), and the Baldrige Secure On-line Ordering Application.

American Society for Quality (ASQ) provides contractual support for the Malcolm Baldrige National Quality Award (MBNQA) Award Cycle.

a. Whether it is a general support system, major application, or other type of system
450-01 is a general support system.

b. System location

The system is located at the NIST Gaithersburg, Maryland facility within the continental United States. The ASQ component resides in a datacenter in Milwaukee, Wisconsin.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The Baldrige system is a standalone system. Authorized users enter and retrieve data directly from the components in the system.

d. The purpose that the system is designed to serve

The purpose of 450-01 is for administrative matters. Specifically, the function/purpose of the system is to support the electronic needs and activities of the Baldrige Performance Excellence Program for internal and external customers. These activities include providing structured database access for NIST staff within NIST Infrastructure environment to information relevant to the processes related to the Baldrige team activities. Shared files and print services are available to staff members.

e. The way the system operates to achieve the purpose

Various significant components comprise the 450-01 parent system, these include: servers, web applications, managed clients, and social networking services. Thus, internal/external customer needs are met. A structured database for NIST staff within a NIST infrastructure environment is offered for the Baldrige team activities.

f. A general description of the type of information collected, maintained, use, or disseminated by the system

The system collects award applications, applications for individuals to be examiners, review information about award applications, and information needed to process orders for Baldrige materials.

g. Identify individuals who have access to information on the system

Baldrige employees and contractors, as well as individuals who have been selected to be Examiners and Judges, have role-based access to information in the system.

h. How information in the system is retrieved by the user

Users must authenticate to each system component. Access to information is restricted based on the user's role.

i. How information is transmitted to and from the system

- **BEA is a public-facing web application that allows potential Baldrige examiners (external users) to complete an online application. It also includes an internal portion that is used to administer the site and review the examiners.**
- **BOSS is a public-facing web application that allows examiners and judges to create and manage review of applicants throughout the award process.**

- **The Secure On-line Ordering Application provides external users with the ability to purchase Baldrige Performance Excellence Program Criteria online in a secure manner, with a secure protected view for BPEP staff.**
- **The ASQ component provides management support, typesetting, printing, and distribution of program documents, Award Cycle Evaluation Stages (including receipt of eligibility and Award applications, Examiner assignments, scorebook checks, Judges' meetings notebook preparation, and site visit logistics).**

Questionnaire:

1. The status of this information system:

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

(Skip questions and complete certification)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Activities
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

4. Personally Identifiable Information (PII)

- 4a. Does the IT system collect, maintain, or disseminate sensitive personally identifiable information (PII)?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

The IT system collects, maintains, or disseminates sensitive PII about:

If the answer is "yes" to question 4a, please respond to the following questions.

- 4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

- 4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

- 4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

Is a PIA Required?	Yes
--------------------	------------

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the 450-01 Baldrige Performance Excellence Program System (BPEP) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the 450-01 Baldrige Performance Excellence Program System (BPEP) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Ambrosi, Ronald

Signature of SO: _____ Date: _____

Name of Co-Authorizing Official (Co-AO):

Fangmeyer, Robert

Signature of Co-AO: _____ Date: _____

Name of Chief Information Security Officer (CISO):

Heiserman, Blair

Signature of CISO: _____ Date: _____

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: _____ Date: _____

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: _____ Date: _____

Name of Chief Privacy Officer (CPO):

Barrett, Claire

Signature of CPO: _____ Date: _____