Version Number: 01-2017

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

Privacy Impact Assessment
for the
Baldrige Performance Excellence Program (450-01)

Reviewed by: Susannah Schiller, Acting, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

09/30/2019

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 450-01

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe 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.

Another component supporting BPEP is 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. A 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 way the system operates to achieve the purpose(s) identified in Section 4
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.

(e) 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.

(f) 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 component provided contractually 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).

(g) Any information sharing conducted by the system
The system does not share information with other internal NIST business units.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a, The "Federal Information Security Management Act of 2002 (FISMA).

The Baldrige Awards Program was created under public law 100-107 The Malcolm Baldrige National Quality Improvement Act of 1987.

5 U.S.C. App.—Inspector General Act of 1978, § 2; 5 U.S.C. App.—Reorganization Plan of 1970, § 2; 13 U.S.C. § 2; 13 U.S.C. § 131; 15 U.S.C. § 272; 15 U.S.C. § 1151; 15 U.S.C. § 1501; 15 U.S.C. § 1512; 15 U.S.C. § 1516; 15 U.S.C. § 3704b; 16 U.S.C. § 1431; 35 U.S.C. § 2; 42 U.S.C. § 3121 et seq.; 47 U.S.C. § 902; 50 U.S.C. App. § 2401 et seq.; E.O. 11625; 77 FR 49699 (Aug. 16, 1012).

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

_x__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		c. File/Case ID	x	i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	x	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	x	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	x	Online	x
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Each user enters his/her own data, so they are responsible for its initial accuracy. Data inaccuracies are corrected via access and redress controls. In turn, this corrected data is pulled into the 450-01 system as accurate data. 450-01 has several checks through the agreement process including involvement from the data source (public) to verify accuracy. This ensures the highest data integrity/quality on 450-01 partners is maintained.

2.4 Is the information covered by the Paperwork Reduction Act?

x	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control #0693-0079 OMB Control #0693-0006 OMB Control #0693-0033
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	

For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The BEA web application collects General Personal Data (GPD) and Work-Related Data for applicants (e.g., members of the public) seeking the examiner role.

The BOSS web application enables review of program applicant information by the examiner role.

The contracted support receives paper-based program applicant information.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Unauthorized access could result in a breach of information.

Mitigating controls:
450-01 implements a data retention schedule and disposal plan. Only data required for the 450-01 mission is used in 450-01. All 450-01 users are subject annual training requirements and rules of behavior which can raise the necessary awareness to mitigate data mishandling. 450-01 use is strictly limited to the 450-01 purpose. Everyone who uses 450-01 is a NIST employee, contractor, or examiner selected through a rigorous process. Role based access is used. All users who have access are verified on a thorough, annual basis.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared

	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

X	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors	x		
Other (specify): Volunteer examiners and judges			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.nist.gov/privacy-policy	
x	Yes, notice is provided by other means.	Specify how: Applicants are notified in the application, to include consent for collection of photographs of Examiners and Judges.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals may decline to provide information by not completing the application process. However, doing so would result in an incomplete application which would not be accepted.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Individuals have opportunity to consent to particular uses of their information within the application process.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Since the award cycle is annual, information is updated in alignment with this cycle (reapplication occurs each year). However, individuals also have opportunity to review/update their information by contacting a BPEP manager.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access logs are kept and reviewed for anomalies.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 04/01/2019 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).

x	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

BEA is used by members of the public to apply to become examiners. It is located in the Public Sensitive Zone, and access from the internet is directed through a reverse proxy device. BOSS is used by NIST employees and examiners to create and manage a review of one applicant through the award process. Access is restricted based on a user's examiner assignment.

The application is accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies on an as needed basis. Data is stored on servers located at the NIST Gaithersburg, Maryland facility within the continental United States. Data on the servers is encrypted at rest and in motion.

When users access the system, PII is transferred in a secure fashion. To guard against the interception of communication over the network, the components use the Transport Layer Security (TLS) protocol which encrypts communications. Access to 450-01 requires NIST-issued credentials because access is restricted by user authentication. NIST remote and other agency users access 450-01 on an authorized DOC network, or via connecting to the NIST network through a Virtual Private Network (VPN).

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-23: Information Collected in Connection with Department of Commerce Activities, Events, and Programs
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: NIST Records Schedule N1-167-09-01: Malcolm Baldrige National Quality Award Program
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing		Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:

	Data Field Sensitivity	Provide explanation:
x	Context of Use	Provide explanation: General Personal Data and Work-Related Data collected is for the annual award cycle.
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Threats could arise from collecting more data than is necessary by not employing data minimization. Threats could exploit data secondary use (using personal information for a purpose other than the purpose for which it was collected). An administrator (data handler) could inadvertently combine multiple data sets resulting in aggregation (combining various pieces of personal information).

Mitigating controls:
450-01 implements a data retention schedule and disposal plan. Only data required for the 450-01 mission is used in 450-01. All 450-01 users are subject to annual training requirements and rules of behavior which can raise the necessary awareness to mitigate data mishandling.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.