U.S. Department of Commerce
NIST

Privacy Impact Assessment
for the
Applications Systems Division (ASD) Moderate Applications System
(183-01)

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2017.09.28 17:26:10 -04'00'

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

Unique Project Identifier: 183-01

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.

(a) a general description of the information in the system

The Applications Systems Division (ASD) Moderate Applications System provides the following enterprise-wide infrastructure components:

- The Central People Repository (CPR) is a collection of central database tables which contain information about NIST staff (i.e., Federal employee and Associate).
- The Web Content Management (WCM) component includes a public facing Organization of Scientific Area Committees (OSAC) Membership Application, which allows members of the public to apply for membership.
- The WebLogic component is an application infrastructure for developing, integrating, securing, and managing distributed applications.
- The Reporting Tools component provides reporting capabilities for various applications used throughout NIST.

The components are located at the NIST Gaithersburg, Maryland facility within the continental United States.

(b) a description of a typical transaction conducted on the system

The following are examples of transactions which may contain Personally Identifiable Information (PII) or Business Identifiable Information (BII):

1. The CPR records the arrival and departure, general locator, and identifier information of NIST staff (i.e., employee and associate). The CPR component is used to populate enterprise services and applications such as Active Directory, LDAP, and processing of NIST reorganizations. It also assists in the monitoring and closing of information technology accounts.
2. Members of the public may submit, through the external website, ab OSAC Membership Application.
3. The WebLogic component hosts various applications that support the day-to-day activities of NIST. Hosting includes an environment for developing, integrating, securing, and managing distributed applications.
4. The Reporting Tools component consists of a single commercial-off-the-shelf (COTS) application which consists of a suite of tools used to provide rapid development,

integration and reporting capability across all of the data/information stored within various databases.

(c) any information sharing conducted by the system

The system shares information with other internal NIST business units, and other DOC units serviced by NIST.

(d) a citation of the legal authority to collect PII and/or BII

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.

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 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).

(e) the Federal Information Processing Standard (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 and there are no changes that create new privacy risks.					

_X_ This is an existing information system without any changes which create new privacy risks.

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*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID	X	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: SSN is used by the CPR component to ensure unique and identifiable records for NIST employees and associates, as these fields are used to uniquely identify NIST employees and associates in other systems that feed the CPR.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	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): country of citizenship					

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		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	X	c. Date Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run	X	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	X	Other DOC Bureaus		Other Federal Agencies	X
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 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			
To determine eligibility		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	X	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 CPR increases the use of Federal services online by serving as an authoritative enterprise source for applications such as Active Directory, LDAP, and processing of NIST reorganizations. It also assists in the monitoring and closing of information technology accounts. Information within this component supports NIST staff (i.e., employees and associates).

The Web Content Management component permits members of the public to submit, through the external website, an OSAC Membership Application. This supports improving Federal services online.

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	X		
DOC bureaus		X	
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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.

X	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: The CPR shares information with the following NIST information system: 1. 100-03, NIST Associate Information Web System (NAIS) 2. 172-01, Human Resources System 3. 189-01, Identity, Credential and Access Management (ICAM)
	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			
Other (specify):			

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. The WCM component (e.g., Application) can be found at https://www.nist.gov/osac-application-form.	
	Yes, notice is provided by other means.	Specify how:
X	No, notice is not provided.	Specify why not: For CPR, data is inherited by other systems which present the requisite notice.

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: The WCM component (e.g., Application) identifies a NIST point of contact if an individual does not wish to accept the risk of submitting information.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For CPR, data is inherited by other systems which present opportunity to decline.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The WCM component (e.g., Application) identifies how the information submitted will be used. There are no other uses. For CPR, data is inherited by other systems which address consent of particular uses.

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: For WCM, individuals have opportunity to review/update their information by contacting the identified NIST point of contact. For CPR, internal processes are in place to permit users (e.g., federal staff and associates) to review/update their information through a Directory Request Form.
	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.)*

	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 to PII is restricted to only those users who require access and access is monitored and tracked through audit logging functionality.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/28/16 ☐ 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 (POAM).
	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.

The system components are administered on internal NIST networks, and protected by multiple layers of firewalls and perimeter defenses. Network access controls are employed. The components are located at the NIST Gaithersburg, Maryland facility within the continental United States. Access logs are kept and reviewed for anomalies on an as needed basis. Transactional audit logging functionality is available to track viewing, modification, and deletion of PII within CPR. Use of the CPR and Reporting Tool components are restricted by user authentication, and role-based access is employed across all components. For CPR, sensitive fields are encrypted using FIPS 140-2 encryption. To guard against the interception of communications over the network, the component uses the Transport layer Security (TLS) protocol which encrypts communications. PII/BII is transferred in a secure fashion using FIPS 140-2 encryption.

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 and number *(list all that apply)*: NIST-1, NIST Associates COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs COMMERCE/DEPT-25, Access Control and Identity Management System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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: GRS 3.1 General Technology Management Records
	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:

X	The CPR component contains referential data.

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

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

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

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.

	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.)*

X	Identifiability	Provide explanation: The CPR component stores and processes sensitive PII for all NIST employees and associates. The OSAC Membership Application within the WCM Subsystem stores and processes non-sensitive PII for members of the public applying for OSAC membership.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: The CPR stores and processes sensitive PII for all NIST employees and associates.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.

Points of Contact and Signatures

Information System Security Officer or System Owner	**Information Technology Security Officer**
Name: L. Dale Little Office: 225 B216 Phone: 301-975-8982 Email: dale.little@nist.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed:	Name: K. Robert Glenn Office: 225/A155 Phone: 301-975-3667 Email: robert.glenn@nist.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Date signed: _____
Authorizing Official	**Co-Authorizing Official** **Bureau Chief Privacy Officer**
Name: Susannah Schiller Office: 225 B226 Phone: 301-975-6500 Email: Susannah.schiller@nist.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Date signed:	Name: Susannah Schiller, Acting Office: 225/B222 Phone: 301-975-6500 Email: cpo@nist.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
NIST

Privacy Impact Assessment
for the
Applications Systems Division (ASD) Moderate Applications System
(183-01)

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

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

Unique Project Identifier: 183-01

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.

(a) a general description of the information in the system

The Applications Systems Division (ASD) Moderate Applications System provides the following enterprise-wide infrastructure components:

- The Central People Repository (CPR) is a collection of central database tables which contain information about NIST staff (i.e., Federal employee and Associate).
- The Web Content Management (WCM) component includes a public facing Organization of Scientific Area Committees (OSAC) Membership Application, which allows members of the public to apply for membership.
- The WebLogic component is an application infrastructure for developing, integrating, securing, and managing distributed applications.
- The Reporting Tools component provides reporting capabilities for various applications used throughout NIST.

The components are located at the NIST Gaithersburg, Maryland facility within the continental United States.

(b) a description of a typical transaction conducted on the system

The following are examples of transactions which may contain Personally Identifiable Information (PII) or Business Identifiable Information (BII):

1. The CPR records the arrival and departure, general locator, and identifier information of NIST staff (i.e., employee and associate). The CPR component is used to populate enterprise services and applications such as Active Directory, LDAP, and processing of NIST reorganizations. It also assists in the monitoring and closing of information technology accounts.
2. Members of the public may submit, through the external website, ab OSAC Membership Application.
3. The WebLogic component hosts various applications that support the day-to-day activities of NIST. Hosting includes an environment for developing, integrating, securing, and managing distributed applications.
4. The Reporting Tools component consists of a single commercial-off-the-shelf (COTS) application which consists of a suite of tools used to provide rapid development,

integration and reporting capability across all of the data/information stored within various databases.

(c) any information sharing conducted by the system

The system shares information with other internal NIST business units, and other DOC units serviced by NIST.

(d) a citation of the legal authority to collect PII and/or BII

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.

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 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).

(e) the Federal Information Processing Standard (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 and there are no changes that create new privacy risks.					

_X_ This is an existing information system without any changes which create new privacy risks.

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*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID	X	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: SSN is used by the CPR component to ensure unique and identifiable records for NIST employees and associates, as these fields are used to uniquely identify NIST employees and associates in other systems that feed the CPR.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	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): country of citizenship					

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		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	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run	X	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	X	Other DOC Bureaus		Other Federal Agencies	X
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 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			
To determine eligibility		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	X	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 CPR increases the use of Federal services online by serving as an authoritative enterprise source for applications such as Active Directory, LDAP, and processing of NIST reorganizations. It also assists in the monitoring and closing of information technology accounts. Information within this component supports NIST staff (i.e., employees and associates).

The Web Content Management component permits members of the public to submit, through the external website, an OSAC Membership Application. This supports improving Federal services online.

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	X		
DOC bureaus		X	
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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.

X	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: The CPR shares information with the following NIST information system: 1. 100-03, NIST Associate Information Web System (NAIS) 2. 172-01, Human Resources System 3. 189-01, Identity, Credential and Access Management (ICAM)
	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			
Other (specify):			

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. The WCM component (e.g., Application) can be found at https://www.nist.gov/osac-application-form.	
	Yes, notice is provided by other means.	Specify how:
X	No, notice is not provided.	Specify why not: For CPR, data is inherited by other systems which present the requisite notice.

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: The WCM component (e.g., Application) identifies a NIST point of contact if an individual does not wish to accept the risk of submitting information.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For CPR, data is inherited by other systems which present opportunity to decline.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII BII.	Specify why not: The WCM component (e.g., Application) identifies how the information submitted will be used. There are no other uses. For CPR, data is inherited by other systems which address consent of particular uses.

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: For WCM, individuals have opportunity to review/update their information by contacting the identified NIST point of contact. For CPR, internal processes are in place to permit users (e.g., federal staff and associates) to review update their information through a Directory Request Form.
	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.)*

	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 to PII is restricted to only those users who require access and access is monitored and tracked through audit logging functionality.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/28/16 ☐ 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 (POAM).
	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.

The system components are administered on internal NIST networks, and protected by multiple layers of firewalls and perimeter defenses. Network access controls are employed. The components are located at the NIST Gaithersburg, Maryland facility within the continental United States. Access logs are kept and reviewed for anomalies on an as needed basis. Transactional audit logging functionality is available to track viewing, modification, and deletion of PII within CPR. Use of the CPR and Reporting Tool components are restricted by user authentication, and role-based access is employed across all components. For CPR, sensitive fields are encrypted using FIPS 140-2 encryption. To guard against the interception of communications over the network, the component uses the Transport layer Security (TLS) protocol which encrypts communications. PII/BII is transferred in a secure fashion using FIPS 140-2 encryption.

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 and number *(list all that apply)*: NIST-1, NIST Associates COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs COMMERCE/DEPT-25, Access Control and Identity Management System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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: GRS 3.1 General Technology Management Records
	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:

X	The CPR component contains referential data.

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

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

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

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.

	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.)*

X	Identifiability	Provide explanation: The CPR component stores and processes sensitive PII for all NIST employees and associates. The OSAC Membership Application within the WCM Subsystem stores and processes non-sensitive PII for members of the public applying for OSAC membership.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: The CPR stores and processes sensitive PII for all NIST employees and associates.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.