Version Number: 01-2019

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

Privacy Threshold Analysis
for the
183-01 Applications System Division (ASD) - Moderate Applications

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 183-01

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

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

183-01, Application Systems Division (ASD) Moderate Applications Systems is a general support system made up of several enterprise-wide infrastructure subsystems. The following are 183-01 subsystems that may contain PII/BII related data:

- **The Central People Repository (CPR) subsystem is a collection of central database tables which contain information about NIST Federal employees, contractors and associates, as well as NIST Foreign National Visitors.**
- **The Web Content Management (WCM) subsystem provides a common management tool for NIST operating units (OUs) to create, approve and publish**

public and internal web pages. WCM includes both implementations that support NIST's public website and NIST's Intranet. The public web pages also host an Organization of Scientific Area Committees (OSAC) Membership Application which allows users to apply for OSAC membership.

- **The Web Application Server subsystem is an application infrastructure for developing, integrating, securing, and managing distributed applications.**
- **The Reporting Tools subsystem provides reporting capabilities for various applications used throughout NIST.**
- **The Attachment Application subsystem provides an application infrastructure for storing attachments that relates to various NIST's ServiceNow custom applications in a secure repository.**
- **The SecurityManager SMSLink Client is a DOC hosted application to support personnel and administrative security processes. The web service automates the transfer of biographic, demographic, and employment data between NIST and SecurityManager. The service facilitates new applicant hiring and internal position upgrades in NIST by automating personnel security preliminary or additional background checks. This service also automates NIST Associates and Foreign National Visitor and Guest Access Requests as implemented in SecurityManager per DOC Department Administrative Order (DAO) 207-12. A SMSLink API Client is implemented at NIST to invoke the SecurityManager SMSLink web-service to support the data integration between NIST and DOC SecurityManager.**

Of note is that Web Application Server, Reporting Tools, Attachment Application, and SecurityManager SMSLink Client do not process PII/BII data directly, although they may transmit such data to or from one of the NIST systems that they support.

b. System location

The WCM sites are located in the Acquia Cloud environment which is itself hosted on the Amazon Web Services (AWS) platform. The Reporting Tools servers are hosted on the Amazon Web Services (AWS) platform and on-premise at the NIST Gaithersburg, Maryland facility within the continental United States. SecurityManager is located at the Herbert C. Hoover building (HCHB), and all remaining components are located at the NIST Gaithersburg, Maryland facility within the continental United States.

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

- **CPR interconnects with many NIST systems. These other interconnected systems, not 183-01, are responsible for the security of this data as it enters their accreditation boundaries respectively.**
- **CPR also has an interconnection with DOC OS018 General Support System (Security Manager). CPR will automatically push data to SecurityManager using Security Manager's SMSLink web services via HTTPS, including biographical and employment data for NIST Federal employees, contractors and associates, as well as NIST Foreign National Visitor (FNV) data. During the same connection,**

the NIST system will automatically pull NIST Federal employee's, contractor's and associate's PIV/PIV-I card information and background investigation results.

- **WCM subsystem has an internal and external implementation –**

For WCM Intranet Implementation, interconnection in place is:

- **183-01 CPR - syncs data from CPR subsystem through a cron job to provide non-sensitive data for internal phone directory search through the Organizational Chart Application. It has a CPR database view for purposes of retrieving the needed data for phone directory search functionality.**

For WCM External Implementation, the following key interconnections are in place:

- **600-01 NIST Publication System (NPS) - obtain copies of approved NIST publications for purposes of allowing users to access those publications through the 'Publications Search' component of the public website.**
- **183-01 CPR - obtain directory data for NIST employees and associates for purposes of displaying that data through the OCA component of the public website.**
- **107-02 Kaltura - storing videos that are accessible through the public website.**
- **NIST AWS S3 bucket for FCD (aka HRR) data (s3://nist-el-nfrlhrr/HRR)**

Web Application Server, Reporting Tools, Attachment Application, and SecurityManager SMSLink Client interconnect with several other NIST systems. These other interconnected systems, not 183-01, are responsible for the security of this data as it enters their accreditation boundaries respectively.

Notes: These interconnections do not involve direct access to any NIST internal systems and leverage pre-existing capabilities for retrieving data for purposes of displaying that data through the public website.

d. The purpose that the system is designed to serve

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 Federal employees, contractors and associates, as well as NIST Foreign National Visitors (FNV).**
- **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 Web Application Server 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 Attachment App component provides an application infrastructure for storing attachments that relates to various NIST's ServiceNow and or SharePoint custom applications in a secure repository.**

e. The way the system operates to achieve the purpose
Refer to section d

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

- **The CPR receives data from two human resources applications, the Human Resources Arrival and Departure System (HRADS), NIST Associates Information System (NAIS-Web), and DOC's OS-18 IT Infrastructure System. Data such as staff arrival and departure dates, general locator, and identifier information of NIST staff are recorded in CPR. CPR also receives background investigation results from DOC's SecurityManager application. The CPR system serves to provide data feed to other NIST enterprise services and applications as mentioned in previous paragraphs. CPR data cannot be retrieved directly by typical NIST users. The system includes a Central People Application (CPA), which allows management of CPR data elements. CPA access is provided to a limited group of users with specific roles and privileges defined.**
- **In WCM public facing implementation, there is an Organization of Scientific Area Committees (OSAC) Membership Application which allows members of the public to submit required data to apply for membership. Once collected, the data are accessible only by internal NIST users through the internal WCM component.**

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

- **CPR data cannot be retrieved directly by typical NIST users. The system includes a Central People Application (CPA), which allows management of CPR data elements. CPA access is provided to a limited group of users with specific roles and privileges defined. CPR data is also accessible via the Reporting Tools. However, access to this data is restricted to specific users and is further restricted to data for specific organizations for each user.**
- **WCM Organization of Scientific Area Committees (OSAC) Membership Application data - collected data are accessible only by internal NIST users through the internal WCM component.**

h. How information in the system is retrieved by the user
Refer to answer in g

i. How information is transmitted to and from the system
TLS is used to protect data in transmission to and from the subsystems.

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 183-01 Applications System Division (ASD) - Moderate Applications 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 183-01 Applications System Division (ASD) - Moderate Applications and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Sell, Sean

Signature of SO: SEAN SELL Digitally signed by SEAN SELL Date: 2021.09.27 06:46:29 -04'00' Date: ___________

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

Signature of Co-AO: _____N/A__________________________________ Date: ___________

Name of Chief Information Security Officer (CISO):

Heiserman, Blair

Signature of CISO: Digitally signed by BLAIR HEISERMAN Date: 2021.09.27 10:51:46 -04'00' Date: ___________

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2021.09.24 14:33:20 -04'00' Date: ___________

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2021.09.27 16:45:30 -04'00' Date: ___________

Name of Chief Privacy Officer (CPO):

Barrett, Claire

Signature of CPO: CLAIRE BARRETT Digitally signed by CLAIRE BARRETT Date: 2021.09.27 15:32:11 -04'00' Date: ___________