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

183-01, Application Systems Division (ASD) Moderate Applications Systems, is made up of several enterprise-wide infrastructure subsystems. Following are 183-01 subsystems that may involve PII/BII related data:

- The Central People Repository (CPR) subsystem is a collection of central database tables which contain information about NIST staff.
- 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.

Of note is that Web Application Server, Reporting Tools and Attachment Application are subsystems that do not process PII/BII data directly, though such data may be transmitted by these subsystems in support of the NIST systems that these components support.

a. Whether it is a general support system, major application, or other type of system 183-01 is a general support system.

b. System location
The components, except for WCM, are located at the NIST Gaithersburg, Maryland facility within the continental United States. The WCM sites are located in the Acquia Cloud environment which is itself hosted on the Amazon Web Services (AWS) platform.

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 additional NIST systems. These other interconnected systems, not 183-01, are responsible for the security of this data as it enters their accreditation boundaries respectively.
• WCM has separate internal and external implementations –

For WCM Intranet Implementation, interconnection in place is:
• 183-01 CPR - synces data from CPR subsystem through a cron job to provide data for internal phone directory search—it has a CPR database view for purposes of retrieving the needed CPR data for phone directory search functionality.

For WCM External Implementation, the following key interconnections are in place:
• 600-01 NIKE - 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 ‘People Search’ component of the public website.
• 107-02 Kaltura - storing videos that are accessible through the public website.

Web Application Server, Reporting Tools, and the Attachment Application 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 custom applications in a secure repository. 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 employees and Associates). The CPR receives data from two human resources applications, the Human Resources Arrival and Departure System (HRADS) and NIST Associates Information System (NAIS-Web). Data such as staff arrival and departure dates, general locator, and identifier information of NIST staff (i.e., employee and associate) are recorded in CPR. These data are 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.

In contrast to other 183-01 components, 183-01 actually owns CPR data.

- WCM component provides NIST operating units (OUs) with a standardized web content management toolset for the creation, approval, and publication of NIST websites.

Specific to WCM public facing implementation, there is a public facing Organization of Scientific Area Committees (OSAC) Membership Application. This OSAC application allows members of the public to submit required data to apply for membership. The collected data are accessible only by internal NIST users through the internal WCM component.

- 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
• Data such as staff arrival and departure dates, general locator, and identifier information of NIST staff (i.e., employee and associate) are recorded in CPR. CPR system serves to provide data feed to other NIST enterprise services and applications as mentioned in previous paragraphs. The system includes a Central People Application (CPA), which allows management of CPR data elements.

• 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.

**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.

• WCM – Organization of Scientific Area Committees (OSAC) Membership Application data collected is accessible only by internal NIST users through the internal WCM component.

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

• CPR data is retrieved through the Central People Application (CPA) as mentioned above.

• For WCM, Phone directory search data is accessed via forms-based directory search capabilities on NIST’s public website and Intranet by end users of those sites. Data is submitted to the OSAC Membership Application via a form on NIST’s public website and is accessible to a small number of authorized NIST staff on the OSAC selection committee (submitted data is not accessible publicly in any way).

**i. How information is transmitted to and from the system**

TLS is used to protect data in transmission to and from the components.
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 01-2015).

   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.

   No

   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.)."

   No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)
4a. Does the IT system collect, maintain, or disseminate 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."

   Yes, the IT system collects, maintains, or disseminates PII.

   The IT system collects, maintains, or disseminates PII about:
   DOC employees
   Contractors working on behalf of DOC
   Members of the public

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

5
4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

No, the IT system does not collect, maintain, or disseminate 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?

Yes, the IT system collects, maintains, or disseminates 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.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

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  SEAN SELL
Digital signature: SEAN SELL
Date: 2020.06.11 14:19:09 -04'00'

Signature of SO: ________________________________ Date: __________

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

Signature of Co-AO: _______ N/A ________________________________ Date: _______

Name of Information Technology Security Officer (ITSO):
Glenn, K. Robert  KENNETH GLENN
Digital signature: KENNETH GLENN
Date: 2020.06.09 16:02:40 -04'00'

Signature of ITSO: ____________________________ Date: _______

Name of Authorizing Official (AO):
Sastry, Chandan  CHANDAN SASTRY
Digital signature: CHANDAN SASTRY
Date: 2020.06.09 17:18:29 -04'00'

Signature of AO: ____________________________ Date: _______

Name of Privacy Act Officer (PAO):
Fletcher, Catherine  CATHERINE FLETCHER
Digital signature: CATHERINE FLETCHER
Date: 2020.06.11 11:25:46 -04'00'

Signature of PAO: ____________________________ Date: _______

Name of Bureau Chief Privacy Officer (BCPO):
Schiller, Susannah  SUSANNAH SCHILLER
Digital signature: SUSANNAH SCHILLER
Date: 2020.06.10 13:01:43 -04'00'

Signature of BCPO: ____________________________ Date: _______