

U.S. Department of Commerce
NIST



Privacy Threshold Analysis
for the
NIST Associate Information System (NAIS) Web System

U.S. Department of Commerce Privacy Threshold Analysis

NIST/NAIS-Web

Unique Project Identifier: 100-03

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 of the information system in a way that a non-technical person can understand.*

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).

The NIST Associates Information System (NAIS-Web) electronically processes and tracks NIST Associates’ information regarding their project, funding, work location, sponsor, and living arrangement while associated with NIST. The system also prepares the requisite security documentation for background investigations and requirements related to foreign guests.

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

The NAIS-Web is a major application.

b) *System location*

The NAIS-Web is 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)*

The NAIS-Web is a standalone system.

d) *The purpose that the system is designed to serve*

The NIST Associates Information System (NAIS-Web) electronically processes and tracks NIST Associates’ information regarding their project, funding, work location, sponsor, and living arrangement while associated with NIST. The system also prepares the requisite security documentation for background investigations and requirements related to foreign guests.

e) *The way the system operates to achieve the purpose*

The following are examples of transactions using the NAIS-Web:

- Initiate and create a new work agreement, update or extend an existing work agreement;
- Enable business workflow and approvals by internal organizations and the Associate;
- Create required security documentation for background investigation;
- Track required Visa information (applicable to foreign Associates);
- Activate the work agreement upon arrival;
- Initiate badge and information technology issuance; and
- Terminate the work agreement through completion, cancellation, or process deletion.

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

Identifying Numbers and General Personal Data are used in the NAIS-Web.

g) *Identify individuals who have access to information on the system*

NIST and DOC federal staff have access to the information within NAIS-Web.

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

Authorized users may retrieve information based on their role using a web browser to access the NAIS-Web.

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

Information is manually input and retrieved by authorized users of the system through an application interface.

Questionnaire:

1. What is the status of this information system?

 This is a new information system. *Continue to answer questions and complete certification.*

 X This is an existing information system with changes that create new privacy risks.

Complete chart below, continue to answer questions, and complete certification.

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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					
Additional personal Identifying Numbers and General Personal Data.					

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. *Continue to answer questions and complete certification.*

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 or later). *Skip questions and complete certification.*

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.

Yes. *Please describe the activities which may raise privacy concerns.*

No

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.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

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

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC (NIST Associates)

Members of the public

No, this IT system does not collect any PII.

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

4b. 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.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. 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.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NIST Associate Information System (NAIS) Web System (100-03) 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 NIST Associate Information System (NAIS) Web System (100-03) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Owner (ISO): Claire Saundry

Signature of ISO: CLAIRE SAUNDRY Digitally signed by CLAIRE SAUNDRY
Date: 2019.09.18 14:57:38 -04'00' Date: _____

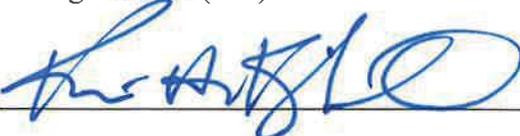
Name of Information System Owner (ISO): Paul Zielinski

Signature of ISO: PAUL ZIELINSKI Digitally signed by PAUL ZIELINSKI
Date: 2019.09.18 15:37:55 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): K. Rob Glenn

Signature of ITSO: KENNETH GLENN Digitally signed by KENNETH GLENN
Date: 2019.09.18 08:14:29 -04'00' Date: _____

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

Signature of AO:  Date: 9/23/19

Name of Co-Authorizing Official (AO) /Bureau Chief Privacy Officer (BCPO): Susannah Schiller, Acting

Signature of BCPO: SUSANNAH SCHILLER Digitally signed by SUSANNAH
SCHILLER
Date: 2019.09.18 08:19:25 -04'00' Date: _____