

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



**Privacy Impact Assessment  
for the  
NIST Associate Information System (NAIS) Web System**

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

for Dr. Catrina D. Purvis **LISA MARTIN** Digitally signed by LISA MARTIN  
Date: 2019.10.21 10:19:18 -0400

10/02/2019

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: 100-03**

### **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 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 does not interface with other systems, but resides on infrastructure systems.

*(d) The way the system operates to achieve the purpose(s) identified in Section 4*

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.

*(e) 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.

(f) *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.

(g) *Any information sharing conducted by the system*

The NAIS-Web shares information with other internal NIST business units to process NIST Associates. The NAIS-Web provides direct access within NIST to authorized users for purposes of processing background investigations, which is further shared on a case by case within NIST to provide access to resources (i.e., IT or physical access). For processing prospective foreign associates when the Visa type is J-1 and sponsorship is provided by NIST, information is collected and shared to satisfy U.S. Department of State requirements.

(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.

(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):				
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.

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.)

<b>Identifying Numbers (IN)</b>					
a. Social Security*	X	e. File/Case ID	X <sup>1</sup>	i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
National Identity Number*					
Immigration and Naturalization Service (INS) number <sup>1</sup>					
U.S. Department of State SEVIS ID number <sup>1</sup>					
U.S. Department of State Visa type and sponsor					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
SSN and National Identity Number are required to process transactions necessary for preparation of the agreement and for performing a security background investigation.					
The INS, SEVIS ID, and Visa type and sponsor are required for processing foreign associates (reference DoS form DS-2019, Certificate of Eligibility for Exchange Visitor (J-1 status)).					

<b>General Personal Data (GPD)</b>					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	X <sup>2</sup>
d. Gender	X	j. Telephone Number	X	p. Military Service	X
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):					
Citizenship					
Emergency Contact Name and Phone Number					
Other Names Used & Dates					
Security Clearance Background Information (e.g., prior investigation conducted, agency office)					
Health insurance company name and policy expiration date for prospective foreign associates <sup>2</sup>					

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

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice		f. Vascular Scan		i. Dental Profile	

Recording/Signatures				
j. Other distinguishing features/biometrics (specify):				

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

<b>Other Information (specify)</b>

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

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

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

<b>Non-government Sources</b>				
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.

Accuracy of the information within NAIS-Web is supported through several opportunities for review in the agreement process (e.g., initiation, review, approval, processing). Specifically, NAIS-Web Initiators can manually make corrections identified by the individual Associate.
--

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 Number 0693-0067
	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):			

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):			

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).

Information is necessary for preparation of the agreement and for performing a security background investigation for prospective Associates (e.g., domestic and foreign, contractors, etc.) and visitors. Additional Visa information is collected for foreign Associates.

- 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.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data). Information collected is directly from the Associate and is limited to only that which is needed for the service.

Mitigating controls include employing and monitoring administrative access, periodic review of roles, training for administrators and users, issuance of rules of behavior for roles, and assurance of compliance to records management schedules.

**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		X
DOC bureaus			
Federal agencies	X		
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.

	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	NIST System 183-01, Applications System Division (ASD) Moderate Applications NIST System 183-06, Application Servers and Databases System
	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.)*

<b>Class of Users</b>			
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 Policy can be found at: <a href="https://www.nist.gov/privacy-policy">https://www.nist.gov/privacy-policy</a> . A Privacy Act Statement is located on templates provided to the prospective Associate.	
	Yes, notice is provided by other means.	Specify how:
	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 have opportunity to decline to provide PII/BII by not completing the required template. Failure to provide PII/BII generally results in a failure to obtain a background investigation, which affects the acceptance of the work agreement or access to NIST resources (i.e., IT resources or physical access).
	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	Specify how: Individuals have opportunity to consent to particular uses of
---	---	---

	PII/BII.	their PII/BII by reviewing the Privacy Act Statement on the required template. Failure to provide PII/BII generally results in a failure to obtain a background investigation, which affects the acceptance of the work agreement or access to NIST resources (i.e., IT resources or physical access).
	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: Individuals have opportunity to review/update PII/BII pertaining to them by informing their NIST sponsor whom initiates action to update within the NAIS-Web.
	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.
	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): October 15, 2018 <input type="checkbox"/> 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.
	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).*

The NAIS-Web is administered on internal NIST networks protected by multiple layers of firewalls. Automated audit reduction, monitoring, and reporting is employed on the system. The component is located at the NIST Gaithersburg, Maryland facility within the continental United States.

Unauthorized use of the system is restricted by user authentication, and role-based access is employed. Access logs are kept and reviewed for anomalies. Data archive processes are run monthly.

PII/BII is transferred securely using FIPS 140-2 encryption. Encryption is employed on data-at-rest. To guard against the interception of communication over the network, the Transport Layer Security (TLS) protocol is used to encrypt communications.

**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. <i>(list all that apply):</i>  NIST-1 NIST Associates
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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 Associates Records Schedule <u>DAA-0167-2016-0006</u>
	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.)*

<b>Disposal</b>			
Shredding		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.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	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.) --see other PIAs for this as well for explanation language.*

X	Identifiability	Provide explanation: The aggregation of data elements can be used to identify specific individuals, their characteristics, background, etc.
X	Quantity of PII	Provide explanation: There exists a large volume of conference attendees recorded in the system. Due to conference registration of personnel over many years with varying PII/BII collection mechanisms (e.g., hard copy sign in sheet or over unsecured phone lines).
X	Data Field Sensitivity	Provide explanation: There are numerous data fields required for processing NAIS agreements, and specific requirements for processing those for foreign associates.
X	Context of Use	Provide explanation: The use it to determine eligibility and administrative processing (to include personnel security).
X	Obligation to Protect Confidentiality	Provide explanation: The organization is obligated to protect the data within the application.
X	Access to and Location of PII	Provide explanation: The system is located at the NIST Gaithersburg, Maryland facility within the continental United States.
	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 about the type or quantity of information collected and the sources providing the information 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.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data).

Information collected is directly from the employee and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.

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.