SUPPORTING STATEMENT

U.S. Department of Commerce

National Institute of Standards and Technology

NIST Associates Information System (NAIS)

OMB Control No. 0693-0067

SUPPORTING STATEMENT PART A

Abstract

NIST Associates (NA) will include guest researchers, research associates, contractors, and other non-NIST employees that require access to NIST campuses or NIST resources. The NIST Associates Information System (NAIS) information collection instrument(s) are completed by the incoming NAs. The NAs will be requested to provide personal identifying data including home address, date and place of birth, gender, passport number, Issuing Country, employer name and address, and basic security information, and provide CV/Resume along with other pertinent data information.

The data provided by the collection instruments will be inputted into NAIS, which automatically populates the appropriate forms, and is routed through the approval process. NIST's Office of Security receives security forms through the NAIS process and is able to allow preliminary access to NAs to the NIST campuses or resources. The data collected will also be the basis for further security investigations as necessary.

Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

The National Institute of Standards and Technology (NIST) has an imperative to know who has access to the NIST facility for safety, security, and compliance with Federal laws and regulations. NIST Associates (NA) are given access to NIST facilities to advance NIST's mission but this entails a level of security risk. NIST sites include a nuclear reactor, sophisticated equipment, proprietary information, sensitive and classified information, and information related to U.S. businesses. NIST performs advanced research in many areas controlled by export control regulations and requires background information to ensure compliance. NIST facilities have lasers, reactors, hazardous materials, and other safety concerns that are a necessary part of research. Providing access to this equipment involves a safety risk and NIST must ensure safety of both the associates and NIST staff. This requires an understanding of the background and qualifications of associates who will work on the NIST campus and information in case accident or emergency. In addition, intellectual property developed during research is controlled by several laws and it is important for NIST to

understand the background and affiliation of associates to make a determination of intellectual property rights and government use rights resulting from work performed in collaboration with NIST staff.

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The agency operates in two locations: Gaithersburg, Md., (headquarters - 234-hectare/578-acre campus) and Boulder, Colorado, (84-hectare/208-acre campus). NIST employs about 3,000 scientists, engineers, technicians, and support and administrative personnel. NIST works collaboratively with many organizations in support of our mission. The NIST Organic Act (15 USC 272 (c)(7)) specifically allows NIST to “accept research associates… from industry, and also engage with industry in research to develop new basic and generic technologies for traditional and new products and for improved production and manufacturing”. NIST hosts approximately 2,800 associates and facility users from academia, industry, and other government agencies in support of its mission.

NAs include foreign and domestic guest researchers, research associates, contractors, and other non-NIST employees that require access to the NIST campuses or resources and contribute to the NIST mission. NAs are located in every part of NIST’s organization and each NA contributes to NIST’s mission in a unique way. Guest Researchers work collaboratively with NIST scientists on research and development projects of mutual interest or to transfer NIST "know-how," methodologies, procedures, and best practices. Research associates work at NIST under a Cooperative Research and Development Agreement (CRADA), a partnering tool that allows federal laboratories to work with U.S. industries, academia, and other organizations on cooperative research and development projects. Contractors and other non-NIST employees provide specific services that NIST has identified as essential to their mission. The activities of NAs range from highly-technical work in laboratories to construction and maintenance of facilities.

The NIST Associates Information System (NAIS) is an automated system that supports the process of bringing NIST Associates (NAs) to the NIST campus or allowing them access to NIST resources. NAIS automates the preparation, review, and approval of all NA agreements, records, extensions, and security forms. NAIS simplifies the information collection process by allowing for a single collection of data that is used on multiple forms therefore reducing transfer errors and decreasing time required.

NAIS is jointly owned by the Technology Partnerships Office (TPO) and the International and Academic Affairs Office (IAAO). TPO and IAAO are respectively responsible for domestic and foreign associates. NAIS supports TPO’s mission of promoting both formal and informal collaboration opportunities and enabling technology transfer from NIST to promote US competitiveness. IAAO verifies the visa status of all foreign associates and their program and offers scientists from around the world the opportunity to work collaboratively with NIST scientists. The NAIS team consists of staff from TPO, IAAO and Office of Information Systems Management’s Applications Systems Division. The NAIS team plans and implements all aspects of the system including assisting users and generating reports.

The appropriate collection instrument, based on the type of NA and the access needed, is forwarded to the NA by their NIST host. The NA will return the completed collection instrument to NIST for processing prior to their arrival. The information collected through NAIS collection instruments will be input into NAIS, which will automatically populate the appropriate forms, and routes them through the approval process.

Prior to the arrival of a NA, the NIST host division determines the length of stay, develops a work plan, determines financial assistance (if applicable), reviews any funding agreement, and establishes the need for a security investigation.

The NAIS system will populate the following forms and fields from the data collected:

NIST 1296 – Domestic Guest Researcher Agreement
Name, Citizenship, Employer/Home Organization Name and address, Sponsor Name and Address, Emergency Personal Contact, Education (institution name, address, years attended, subjects studied, and degree)

NIST 1291- Foreign Guest Researcher Agreement
Name, Citizenship, Date of Birth, Place of Birth, Social Security Number, Employee/Home Organization Name and Address, Sponsor Name and Address, Emergency Personal Contact, Education (institution name, address, years attended, subjects studied, and degree)

NIST-1085 – Request for Security Assurance
Name, Date of Birth, Email, Place of Birth, Social Security Number, Other Names Used, Sex, Citizenship, Worked at NIST in Past, Foreign National Coming Directly From Homeland, Previous U.S. Government Clearances

NIST-1260 - Report of Foreign Visitor, Guest, and Conference Attendee
Name, Date of Birth, Place of Birth, Employer/Sponsor Name and Address, Citizenship

NIST-351 – Request for Federal Credential or NIST Site Badge
Name, Date of Birth, Social Security Number, Citizenship, Home Address

Release – Fair Credit Reporting Act of 1970
Name, Social Security Number

OFI-86C – Special Agreement Checks (SAC)
Name, Date of Birth, Place of Birth, Social Security Number, Other Names Used, U.S. Passport Number

Authorization for Release of Information (Attachment to OFI-86C)
Name, Other Names Used, Home Address and Phone Number

OF-306 – Declaration for Federal Employment

Name, Social Security Number, Place of Birth, Citizenship, Date of Birth, Other Names Used, Phone Numbers

OSY Form 207-12-A (Foreign National Request Form), OMB No. 0690-0033
Name, Social Security Number, Place of Birth, Citizenship, Last 3 Entries into U.S. in Past 5 Years

Forms NIST-1296 and NIST-1291 are used respectively by NIST's Technology Partnerships Office (TPO) and International and Academic Affairs Office (IAAO) for intellectual property purposes. The forms list the terms of agreement and describe procedures for disclosure of any inventions made during the NA's time at NIST. IAAO also uses the NIST 1291 to process any required visa paperwork. The form is signed by the NA upon their arrival at NIST. All other forms are required by DOC/NIST Office of Security (OSY).

The process Initiator, usually a group secretary, will input into NAIS the information collected through the data collection instrument. The NAIS information will be routed within the Operating Units (OU) for approval. The NAIS process provides OU management with information about who will be working in their OU and their purpose for being at NIST. No NA will be allowed access to NIST facilities and/or resources without approval in NAIS. Guest researcher information will be routed through the Administrative Officer, Host, Division Chief, OU Director, Foreign National Approver, and Senior Administrative Official as appropriate. Information on other NA types will be routed through the Administrative Officer and OU Director. After OU approval, the information for all domestic associates will be routed to TPO, manager of domestic NAs. The information for all foreign associates will be routed to the IAAO, manager of all foreign NAs and the Security Review Committee. The information for foreign associates that receive subsistence will be routed to the Finance group. The opt-out collection instrument (titled: General Information for NIST Associates) will be used by the NIST employee or office hosting the NA if it is determined, before the form is provided to the associate, that any investigation or additional processing is not necessary. These NAs will not receive a badge, not have access to NIST information technology resources, and will be escorted at all times while on the NIST campuses.

After the OU approval process is complete, the DOC/NIST OSY will receive the security forms through the NAIS process to allow preliminary access for NAs to the NIST campuses or resources. The data collected will also be the basis for further security investigations as necessary, including attempts to locate previous background investigations, registration into the DOC Management Application for Security (MAPS), and invitation to the NA into Electronic Application for Investigations Processing (e-APP).

NIST uses Electronic Application for Investigations Processing (e-APP) to collect information required by Forms SF-85, SF-85P and SF-86. e-APP is an automated system that facilitates the processing of standard investigative forms for background processing. This process occurs outside of the NAIS process and NIST uses the NAIS information only to register the NA in e-APP. The NA is invited into e-APP only after their process has been approved in NAIS and only when an investigation is necessary. Using e-APP allows NAs to transmit their personal information in a private and secure manner. Data exclusive to the SF-85, SF-85P or the SF-86

forms is intentionally excluded from collection in NAIS since it is not required as part of the NAIS process.

The Authorization and Release form provides the authority for the collection, purpose of the collection, routine uses and consequences of not providing information as required by 5 U.S.C. 5521(e)(3).

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

Information will be collected by the NIST Operating Units (OUs) for each associate. The information collected will be used for NA agreements and security/background investigations. Only general demographic information will be used publicly— for example, a speech at the University of Maryland may contain the number of NAs currently at NIST from the University.

The information will be collected, maintained, and used in a way that is consistent with the applicable NIST Chief Information Officer (CIO) Information Quality Guidelines and Standards. Only general demographic information will be disseminated publicly.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

The collection instruments are available as a fillable printable questionnaire on NIST's internal website (https://inet.nist.gov/tpo/services/nais). The NAIS process Initiator or the NIST employee hosting the associate will provide the applicable form to the NA. The NA will complete the form and submit it via fax or in hard copy format. The NAIS process Initiator will then enter the information into the system for use in generation of the necessary security forms and agreements. A planned enhancement is to provide the collection instrument as a fillable, public-facing interface that will allow for importation of the data into NAIS thus eliminating data entry by NIST staff.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

The collected information is specific to each NA and is not available elsewhere. The NAIS information collection process is designed to reduce and prevent duplication. Respondents will complete the information collection instrument and their information will then be input into the NAIS database. The NAIS database will use the information to populate all required forms without the need for the respondent to complete additional forms, information collections, or respond to further requests for the same information.

The following forms will be populated with the data collected and generated by NAIS. No NA

may come to NIST without approval of documentation in NAIS. The Domestic Guest Researcher Agreement, NIST 1296, is used by NIST TPO for determination of intellectual property issues should any invention be made during time at NIST. It includes the statement "The Privacy Act of 1974 (5 U.S.C. 552A) requires that you be given certain information in connection with the request for information on this form. The authority for the collection of this data is 5 U.S.C. 301." The Foreign Guest Researcher Agreement, NIST 1291, is used by NIST IAAO for determination of intellectual property issues should any invention be made during time at NIST.

NAIS will populate and generate the following forms for security purposes. Request for Security Assurance, NIST-1085, is required by DOC/NIST OSY for background investigation as mandated by Executive Order 10450. Report of Foreign Visitor, Guest, and Conference Attendee, NIST-1260, is required by DOC/NIST OSY. Request for Federal Credential or NIST Site Badge, NIST-351, is required by DOC/NIST OSY and NIST's Emergency Services Division to request and prepare a Personal Identity Verification (PIV) and/or site badge. Fair Credit Reporting Act Release is a standard federal government form. Special Agreement Checks, OFI 86C, is a security form from the U.S. Office of Personnel Management Investigative Services. Declaration for Federal Employment, OF 306, is approved by OMB (OMB No. 3206 0182).

The following data will be collected by these information collection instruments for uses other than the forms described above and in response to Question 1. Mother's maiden name will be used to verify a unique name/individual. Employer/home organization, address, sponsor name, sponsor address will be used to determine intellectual property rights but also have programmatic and statistical analysis uses such as reporting on the number of NAs from a particular organization or state. Email address will be used by DOC/NIST OSY to contact the NA for an invitation to e-APP. Employed by another federal agency and education date have programmatic uses such as providing quick access to the number of NAs that are federal employees or from a specific university. Emergency personal contact and employer/home organization contact will be used for emergency purposes only.

Existing systems such as the USAccess, which is used for issuing identification badges, are insufficient for NIST needs. As stated in the paragraphs above, the information needed for the forms and agreements required as part of the NA approval process and the information needed for purposes of intellectual property rights are not collected in the USAccess information collection, and that information is needed prior to the initiation of the badging process. In addition, not all NAs are required to have an identification badge, therefore, they will never need to provide information for purposes of the USAccess. NIST's Office of Security (OSY) was an integral part of NAIS planning and implementation. OSY developed the system security requirements and performed testing on the security section. The NAIS team continues to meet with OSY on a bi-weekly basis to discuss any issues or needs.

Within NIST the NAIS record will be used as the authoritative identity for all NAs. All Information Technology and Telecommunications access will tie back to the NA record. This will ensure that that access provided is commensurate with the agreement the NA is operating under and all logical (IT) access is terminated when the NIST Agreement is terminated.

The NAIS NA record will be used to control physical access: For NAs receiving PIV badges the US Access system is audited to ensure that badges are terminated with an Agreement and for NAs receiving site access the physical security system is linked to the term, status and authorizations within the NAIS system.

5. If the collection of information impacts small businesses or other small entities, describe any methods used to minimize burden.

Small businesses are not involved in this information collection.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

The information will only be collected when a NA is initially coming to NIST and will be updated if/when their agreement is extended (typically annually).
The information collected is critical to the administrative and security processing of NAs, who are essential to the successful accomplishment of NIST's mission. Due to security, tax law and visa/State department requirements it is not possible to process NAs without collecting the data. Modifying the process to have the NA provide the information on multiple forms for individual purposes would result in data inconsistencies, increased errors, increased burden on the respondents to provide the same information multiple times, and significantly increased processing burden to NIST. This would in turn lengthen the time required to bring NAs on board and negatively impact the NIST mission.

The Bayh-Dole Act of 1980 and Executive Order 12591 permit a university, business, or non-profit institution to elect to pursue ownership of an invention created under federally funded research projects in preference to the government. Lack of knowledge of the employer/home organization of a NA will compromise the determination of intellectual property rights for both the NA and the federal government.

If this information were not collected or collected less frequently, unauthorized persons could gain access to NIST's secured campus or resources and/or NIST's mission would be jeopardized.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner: requiring respondents to report information to the agency more often than quarterly; requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it; requiring respondents to submit more than an original and two copies of any document; requiring respondents to retain records, other than health, medical, government contract; grant-in-aid, or tax records, for more than three years; in connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study; requiring the use of a statistical data classification that has not been reviewed and approved by OMB; that includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are

consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or requiring respondents to submit proprietary trade secrets, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

The collection will be conducted in a manner consistent with OMB guidelines. Expiration date and public burden statement will be included on the instruments.

8. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Consultation with representatives of those from whom information is to be obtained or those who must compile records should occur at least once every 3 years - even if the collection of information activity is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

A 60-Day Federal Register Notice to solicit public comments was published on January 8, 2024, on pages 904-905, Vol. 89, No. 5. No comments were received.

A 30-Day Federal Register Notice to solicit public comments was published on April 29, 2024, on pages 33330-33331, Vol. 89, No. 83.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

No payments or gifts are offered to participants.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy. If the collection requires a system of records notice (SORN) or privacy impact assessment (PIA), those should be cited and described here.

No assurances of confidentiality will be given. However, NAIS is governed by the provisions of 5 U.S.C. 522a (known as the Privacy Act of 1974), and selected provisions of other Federal statutes, regulations, Department of Commerce (DOC), and National Institute of Standards and Technology (NIST) policies, procedures and guidelines. Appropriate Privacy Act Statement is provided on the collection instruments and details appropriate SORNs. NAIS Rules of Behavior are not intended to supersede any such statutes, regulations, etc., nor are these rules intended to conflict with these pre-existing statutes and regulations. Rather, these rules of behavior are intended to enhance and further define the specific procedures each user must follow while accessing NAIS, consistent with the NAIS Privacy, Security and Access Policy.

In accordance with the privacy provisions of the E-Government Act of 2002, a Privacy Impact Assessment (PIA) is required for NIST system 100-03, where this data resides. The collection and maintenance of NAIS is outlined in the PIA for 100-03 and is approved by the Department of Commerce's Senior Agency Official for Privacy (SAOP) and is public. The PIA is available on the Department's privacy program page at: https://osec.doc.gov/opog/privacy/NIST-pias.html.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

NIST will not collect sensitive data.

12. Provide estimates of the hour burden of the collection of information.

NIST estimates 4,000 NAs will be processed per year. It is estimated that it will take 30-50 minutes to complete the appropriate collection instrument for a total of 2,167 burden hours.

Collection Instrument	Number of Respondents	Number of Minutes to Complete the Collection Instrument	Number of Burden Hours
General Information for NIST Associates	1,800	30 minutes	900 hours
General Information for NIST Associates with Opt-Out	200	30 minutes	100 hours
General Information for NIST Foreign National Associates (FNAs)	500	50 minutes	417 hours
General Information for Domestic Guest Researchers	1,500	30 minutes	750 hours
TOTALS	4,000	30-50 minutes	2,167 hours

13. Provide an estimate for the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden already reflected on the burden worksheet).

There is no cost to the respondent.

14. Provide estimates of annualized costs to the Federal government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), and any other expense that would not have been incurred without this collection of information. Agencies may also aggregate cost estimates from Items 12, 13, and 14 in a single table.

NIST estimates that approximately 40 hours of time would be involved for the Analyst managing the efforts of this information collection. That estimated cost is $2,200.00.

15. Explain the reasons for any program changes or adjustments reported on the burden worksheet.

The collection of these new items will further facilitate the processing of associates at NIST.

The additional information collected on the templates, and changes are:

- Associate Phone Number. (On all 4 templates)

- Associate Gender. (On all 4 templates)

- Passport Expiration Date. (Foreign Template)

- US-CIS#. (Foreign Template)

- Passport ID page as an attachment. (Foreign Template)

- Home Address: provide “to Present” date. (Foreign and Domestic Templates)

- Affiliations. (Domestic Template)

- Other Funding Sources (Domestic Template)

- CV/Resume as an attachment. (Domestic Template)

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

The results of this collection will not be published.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

The OMB Control number and expiration date will be displayed.

18. Explain each exception to the topics of the certification statement identified in "Certification or Paperwork Reduction Act Submissions."

NIST does not require any exceptions.