SUPPORTING STATEMENT
U.S. Department of Commerce
National Institute of Standards and Technology (NIST)
NIST Associates Information System (NAIS)
OMB Control No. 0693-XXXX

A. JUSTIFICATION

This is a request of a new information collection. During the review of this request, OMB provided comments to NIST. The comments and responses to the comments have been included in the request.

1. Explain the circumstances that make the collection of information necessary.

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 2,900 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 2,600 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 organization 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
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

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, Division Chief, and OU Director. 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. The information for foreign associates that receive subsistence will be routed to the Finance group. The opt-out collection instrument 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 Questionnaires for Investigations Processing (e-QIP).

2. Explain how, by whom, how frequently, and for what purpose the information will be used. If the information collected will be disseminated to the public or used to support information that will be disseminated to the public, then explain how the collection complies with all applicable Information Quality Guidelines.

Information will be collected in the NIST Operating Units for each associate. The information collected will be used for NA agreements and security/background investigations. Only general demographic information will be used publically— 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 publically.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological techniques or other forms of information technology.

The collection instruments are available as a fillable printable questionnaire on NIST's internal website. 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. <u>Describe efforts to identify duplication</u>.

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-QIP. 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 involves small businesses or other small entities, describe the methods used to minimize burden.

Not applicable.

6. Describe the consequences to the Federal program or policy activities if the collection is not conducted or is conducted less frequently.

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 require the collection to be conducted in a manner inconsistent with OMB guidelines.

Not applicable.

8. Provide information of the PRA Federal Register Notice that solicited public comments on the information collection prior to this submission. Summarize the public comments received in response to that notice and describe the actions taken by the agency in response to those comments. Describe the efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

A notice soliciting public comments was published in the Federal Register on March 28, 2012 (Vol. 77, Number 60, page 18791). No comments were received.

9. Explain any decisions to provide payments or gifts to respondents, other than remuneration of contractors or grantees.

Not applicable.

10. Describe any assurance of confidentiality provided to respondents and the basis for assurance in statute, regulation, or agency policy.

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. 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.

This collection of information falls under the Systems of Record, NBS-1 NBS Guest Workers and NBS-3 Research Associates (SORNs). The Federal Register Notices for these Systems of Record were published on December 31, 1981, Volume 46, Number 251, pages 63532 and 63533. The SORNs, are currently in the process of being updated and are expected to be

completed during Fiscal Year 2014. SORs NBS-1 and NBS-3 will be combined and the new title is 'NIST Associates.' The revised draft SORN has been included as part of this request.

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.

Not applicable.

12. Provide an estimate in hours of the burden of the collection of information.

NIST estimates 4,000 NAs will be processed x 30 minutes per responses = 2,000 burden hours.

13. Provide an estimate of the total annual cost burden to the respondents or record-keepers resulting from the collection (excluding the value of the burden hours in Question 12 above).

None.

14. Provide estimates of annualized cost to the Federal government.

There are no costs beyond the normal labor costs for staff.

15. Explain the reasons for any program changes or adjustments.

This is a new information collection.

16. For collections whose results will be published, outline the plans for tabulation and publication.

The results will not be published.

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

Not applicable.

18. Explain each exception to the certification statement.

Not applicable.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

This collection does not employ statistical methodology.