visits will allow for improved law enforcement oversight and compliance. In addition to monitoring atoll species, a remote camera system will also provide better management and documentation of any unauthorized entry to the Refuge. The Refuge will remain closed to the general public, with entry only allowed via special use permit.

Refuge staff will provide outreach and interpretation opportunities and develop an environmental education program focusing on ''bringing the refuge to the people.'' Appropriate cultural practices will also be facilitated through expanding refuge management activities related to cultural resources. We will work with the American Samoa Historical Preservation Office and other partners to conduct archaeological surveys at Rose Atoll NWR, integrate cultural resources into interpretation, and increase dialogue with the Office of Samoan Affairs and local villagers, among other activities.

Public Availability of Documents

In addition to any methods in **ADDRESSES**, you can view or obtain documents at the Feleti Barstow Public Library, National Park Office in Ofu, the High School in Ta'u and other places of public access in American Samoa.

Dated: July 30, 2014.

Stephen J. Zylstra,

Acting Regional Director, Pacific Region, Portland, Oregon.

[FR Doc. 2014–21667 Filed 9–17–14; 8:45 am]

BILLING CODE 4310–55–P

NATIONAL SCIENCE FOUNDATION

Agency Information Collection Activities: Comment Request

AGENCY: National Science Foundation.

ACTION: Submission for OMB Review; Comment Request.

SUMMARY: Under the Paperwork Reduction Act of 1995, Public Law 104–13 (44 U.S.C. 3501 et seq.), and as part of its continuing effort to reduce paperwork and respondent burden, the National Science Foundation (NSF) is inviting the general public and other Federal agencies to comment on this proposed continuing information collection. This is the second notice for public comment; the first was published in the **Federal Register** at 79 FR 26779 and no comments were received. NSF is forwarding the proposed submission to the Office of Management and Budget (OMB) for clearance simultaneously with the publication of this second notice. The full submission may be found at: *http://www.reginfo.gov/public/do/PRAMain.*

DATES: Comments regarding these information collections are best assured of having their full effect if received by OMB within 30 days of publication in the **Federal Register**.

ADDRESSES: Written comments regarding (a) whether the collection of information is necessary for the proper performance of the functions of NSF, including whether the information will have practical utility; (b) the accuracy of NSF's estimate of burden including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility and clarity of the information to be collected; or (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology should be addressed to: Office of Information and Regulatory Affairs of OMB, Attention: Desk Officer for National Science Foundation, 725—17th Street, NW. Room 10235, Washington, DC 20503, and to Suzanne H. Plimpton, Reports Clearance Officer, National Science Foundation, 4201 Wilson Boulevard, Suite 1265, Arlington, Virginia 22230 or send email to *splimpto@nsf.gov.* Copies of the submission may be obtained by calling (703) 292–7556.

FOR FURTHER INFORMATION CONTACT: Suzanne H. Plimpton, NSF Reports Clearance Officer at (703) 292–7556 or send email to *splimpto@nsf.gov.* Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1–800–877–8339, which is accessible 24 hours a day, 7 days a week, 365 days a year (including Federal holidays).

An agency may not conduct or sponsor a collection of information unless the collection of information displays a currently valid OMB control number and the agency informs potential persons who are to respond to the collection of information that such persons are not required to respond to the collection of information unless it displays a currently valid OMB control number.

SUPPLEMENTARY INFORMATION:

Title of Collection: Graduate Research Fellowship Application.

OMB Control No.: 3145–0023.

Abstract: Section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1861 et seq.), as amended, states that ''The Foundation is authorized to award, within the limits of funds made available . . . scholarships and graduate fellowships for scientific study or scientific work in the mathematical, physical, biological, engineering, social, and other sciences at accredited U.S. institutions selected by the recipient of such aid, for stated periods of time.''

The Graduate Research Fellowship Program has two goals:

- To select, recognize, and financially support individuals early in their careers with the demonstrated potential to be high achieving scientists and engineers;
- To broaden participation in science and engineering of underrepresented groups, including women, minorities, persons with disabilities, and veterans.

The list of GRFP Fellows sponsored by the Foundation may be found via FastLane through the NSF Web site: *http://www.fastlane.nsf.gov.* The GRF Program is described in the Solicitation available at: *http://www.nsf.gov/publications/pub_summ.jsp?WT.z_pims_id=6201&ods_key=nsf14590.*

Estimate of Burden: This is an annual application program providing three years of support to individuals, usable over a five-year fellowship period. The application deadline is in early November. It is estimated that each submission is averaged to be 16 hours per respondent, which includes three references (on average) for each application. It is estimated that it takes two hours per reference for each applicant.

Respondents: Individuals.

Estimated Number of Responses: 15,000.

Estimated Total Annual Burden on Respondents: 240,000 hours.

Frequency of Responses: Annually.

Dated: September 12, 2014.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2014–22241 Filed 9–17–14; 8:45 am]

BILLING CODE 7555–01–P

NATIONAL SCIENCE FOUNDATION

Request for Information (RFI)—National Privacy Research Strategy

AGENCY: The National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD).

ACTION: Notice.

FOR FURTHER INFORMATION CONTACT: Tomas Vagoun at *vagoun@nitrd.gov* or (703) 292–4873.

DATES: To be considered, submissions must be received no later than October 17, 2014.

SUMMARY: Agencies of the Federal Networking and Information Technology Research and Development (NITRD) Program are planning to develop a joint National Privacy Research Strategy. On behalf of the agencies, the Cyber Security and Information Assurance Research and Development Senior Steering Group seeks public input on the vital privacy objectives that should be considered for the goals of the strategy. The National Privacy Research Strategy will be used to guide federally-funded privacy research and provide a framework for coordinating research and development in privacy-enhancing technologies.

SUPPLEMENTARY INFORMATION:

Background

Life in the 21st century is inextricably interconnected with cyberspace and information systems. The computing revolution is enabling advances in many sectors of the economy, but at the same time our social realm has been profoundly affected by the rise of the Internet. Privacy in the digital era is challenged by our capabilities to store and process vast quantities of information. On the one hand, large-scale data analytics is indispensable to progress in science and engineering, but on the other hand, when information about us and our activities in cyberspace can be tracked and repurposed without our understanding, opportunities for crime, discrimination, and misuse are created.

Respect for privacy is a cornerstone principle of our democracy. A variety of laws and policies guide collection and use of data by the government, corporations, and organizations. However, because technology advances can outpace law, respect for privacy must be a guiding principle in the technological domain and our information systems must be designed to provide the means for protecting privacy.

Privacy harms to individuals can arise from actions taken with personal information, including from unapproved disclosure of personal information, to tracking and profiling of our actions, preferences, and habits in cyberspace, to analytical inferences from unrelated data sources. Protection of privacy in this context will require the development of both specific technologies targeted for particular use, as well as foundational science and engineering to develop the capabilities to be able to analyze the situations in the digital realm that might lead to privacy harms, and respond with actions and technologies to prevent or mitigate them.

The Federal Government already plays an important role in protecting certain aspects of privacy, as directed by various legislation (e.g., HIPAA, COPPA), and this Administration has further championed a number of initiatives (such as the ''Consumer Privacy Bill of Rights'' proposal) to improve the state of privacy. In the technical domain, Federal agencies already fund research aimed at a wide range of privacy aspects, from basic research to specific technologies (see [1] for a summary of Federal research in privacy). Nevertheless, privacy in the digital age is a topic of national (and global) importance and more needs to be done. Many challenges remain in areas such as privacy-preserving solutions for data integration and data mining, methods and solutions for managing privacy in electronic health information systems, usage-based controls on privacy and techniques to express user preferences related to data use, or methods for quantifying risks and harms to privacy of individuals. Furthermore, new technologies such as wearable computing (e.g., glasses with cameras, biomedical sensors), embedded computing (e.g., Internet of Things), or cyber-physical systems (e.g., the Smart Grid) create new contexts in which privacy can be challenged and that require targeted technologies to support personal privacy.

Objectives

Reports by the White House and the President's Council of Advisors on Science and Technology (PCAST) on big data and privacy [2] and [3], and reports on Federal networking and information technology research [4] and [5], call for serious increases in investments for research and development (R&D) in privacy-enhancing technologies and in encouraging multi-disciplinary research involving computer science, social science, and legal disciplines. The White House and PCAST cite challenges to personal privacy in the digital era as a significant impairment that is undermining societal benefits from large-scale deployments of networking and IT systems.

At the request of the White House Office of Science and Technology Policy (OSTP), the Cyber Security and Information Assurance Research and Development Senior Steering Group (CSIA R&D SSG) of the Federal Networking and Information Technology Research and Development (NITRD) Program [6] will lead the development of a National Privacy Research Strategy (NPRS). The NPRS will establish objectives and prioritization guidance for federally-funded privacy research, provide a framework for coordinating R&D in privacy-enhancing technologies, and encourage multi-disciplinary research that recognizes the responsibilities of the Government, the needs of society, and enhances opportunities for innovation in the digital realm. The NPRS will be a catalyst to concentrate Federal research resources against critical privacy challenges and to provide enduring objectives for research in privacy-enhancing technologies. The strategy will be developed by interagency collaboration and in a partnership with commercial and academic sector stakeholders and citizens interested in addressing the privacy needs of the nation.

The CSIA R&D SSG is issuing this Request for Information (RFI) to solicit input from the public on defining the most important goals for privacy in the digital world. As a strategy, the NPRS must focus research activities toward relevant and impactful objectives, and this RFI seeks to inform our understanding of societal needs where privacy-enhancing technologies would be beneficial. While there are social and legal solutions to many digital privacy issues, they are out of scope for the NPRS; our focus will be on the research directions for privacy-enhancing technologies, designs, and methods to enable privacy-preserving information systems. The submissions received under this RFI will be used as inputs in structuring the strategy.

Request

Through the NPRS, the CSIA R&D SSG seeks to establish objectives for research and a framework for organizing ideas to achieve the research purpose. Responders are asked to answer one or more of the following questions:

1. *Privacy objectives:* Describe one or more scenarios that illustrate a critical issue concerning privacy; describe what privacy problems arise in the scenario; describe why it is important to overcome the identified problems; describe the needed privacy and what capabilities are required to achieve it; and describe what barriers exist to achieving the needed privacy in the scenario. The use of particular domains in the scenario (e.g., healthcare, education, social media) to describe the desired privacy state is encouraged.

2. *Assessment capabilities:* Discuss concepts, methods, and constructs needed to assess privacy; discuss capabilities and models that can: Express privacy requirements, assess and quantify risks/benefits to privacy, evaluate effects of privacy risk

mitigation, and determine the fulfillment of privacy requirements.

3. *Multi-disciplinary approach:* Discuss how privacy challenges and objectives might be framed to bring many disciplines (e.g., computer science, economics, social and behavioral sciences, and law disciplines) together to jointly and collaboratively work to both strengthen privacy and support innovation in cyberspace and information systems; discuss how diverse national/cultural perspectives on privacy can be accommodated.

4. *Privacy architectures:* (a) The Big Data report [2] recommends adoption of a ''responsible use framework'' [pg. 61] that would provide greater focus on the use of data and hold entities that utilize data accountable for responsible use of the data. Describe an architecture implementing a ''responsible use framework'' incorporating the three questions above and taking into account issues as: Encoding privacy policies in machine-checkable forms and ensuring their compliance and auditability; managing the collection, retention, and dissemination of sensitive data; and ensuring the confidentiality and integrity of sensitive data, while enabling desired uses of them. (b) Describe other privacy architectures that would be effective for the design and implementation of privacy-preserving information systems. (c) Describe technological advances that can change privacy perceptions and how those advances would be incorporated into the ''responsible use framework'' architecture or other architectures submitted for 4(b).

Submission Instructions

Page limitation: All submissions must be 20 pages or less. Comments can be submitted by any of the following methods:

(a) *Email: nprs@nitrd.gov.*

(b) *Fax:* (703) 292–9097, Attn: National Privacy Research Strategy.

(c) *Mail:* Attn: National Privacy Research Strategy, NCO, Suite II–405, 4201 Wilson Blvd., Arlington, VA 22230.

Deadline for Submission under this RFI is October 17, 2014.

Responses to this RFI may be posted without change online, at *http://www.nitrd.gov*. The CSIA R&D SSG therefore requests that no business proprietary information, copyrighted information, or personally identifiable information be submitted in response to this RFI.

In accordance with FAR 15.202(3), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI.

References

[1] ''Report on Privacy Research within NITRD,'' April 2014, *http://www.nitrd.gov/Pubs/Report_on_Privacy_Research_within_NITRD.pdf.*

[2] ''Big Data: Seizing Opportunities, Preserving Values,'' May 2014, *http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.*

[3] ''Big Data and Privacy: A Technological Perspective,'' May 2014, *http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.*

[4] ''Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology,'' January 2013, *http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd2013.pdf.*

[5] ''Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology,'' December 2010, *http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf.*

[6] Networking and Information Technology Research and Development (NITRD) Program provides a framework in which many U.S. Government agencies come together to coordinate networking and information technology research and development efforts. More information is available at *http://www.nitrd.gov*.

Submitted by the National Science Foundation for the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD) on September 12, 2014.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2014–22239 Filed 9–17–14; 8:45 am]

BILLING CODE 7555–01–P

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Public Meetings of the National Science and Technology Council; Committee on Technology; Nanoscale Science, Engineering, and Technology Subcommittee; National Nanotechnology Coordination Office

ACTION: Notice of Public Meetings.

SUMMARY: The National Nanotechnology Coordination Office (NNCO), on behalf of the Nanoscale Science, Engineering, and Technology (NSET) Subcommittee of the Committee on Technology, National Science and Technology Council (NSTC) and in collaboration with the European Commission, will host meetings for the U.S.-EU Communities of Research (CORs) on the topic of environmental, health, and safety issues related to nanomaterials (nanoEHS) between the publication date of this Notice and September 30, 2015. The CORs are a platform for scientists to develop a shared repertoire of protocols and methods to overcome research gaps and barriers. The co-chairs for each COR will convene meetings and set meeting agendas with administrative support from the European Commission and the NNCO.

DATES: The CORs will hold multiple webinars and/or conference calls between the publication date of this Notice and September 30, 2015.

ADDRESSES: Teleconferences and web meetings for the CORs will take place periodically between the publication date of this Notice and September 30, 2015. Meeting dates, call-in information, and other COR updates will be posted on the Community of Research page at *http://us-eu.org/*.

FOR FURTHER INFORMATION CONTACT: For information regarding this Notice, please contact Stacey Standridge at National Nanotechnology Coordination Office, by telephone (703–292–8103) or email (*sstandridge@nnco.nano.gov*). Additional information about the CORs and their upcoming meetings is posted at *http://us-eu.org/*.

SUPPLEMENTARY INFORMATION: There are currently six CORs addressing complementary themes:

- Exposure through Product Life, with Material Characterization
- Ecotoxicity Testing and Predictive Models, with Material Characterization
- Predictive Modeling for Human Health, with Material Characterization
- Databases and Ontologies
- Risk Assessment
- Risk Management and Control

The CORs directly address Objectives 4.1.4 (''Participate in international efforts, particularly those aimed at generating [nanoEHS] best practices'') and 4.2.3 (''Participate in coordinated international efforts focused on sharing data, guidance, and best practices for environmental and human risk assessment and management'') of the 2014 National Nanotechnology Initiative Strategic Plan. However, the CORs are not envisioned to provide any government agency with advice or recommendations.

Registration: Individuals wishing to participate in any of the CORs should send the participant's name, affiliation, and country of residence to *sstandridge@nnco.nano.gov* or mail the information to Stacey Standridge, 4201