collected; and (4) ways to minimize the burden of the collection of information on respondents, including automated collection techniques or the use of other forms of information technology.

Brenda Maxwell,

NASA PRA Clearance Officer.

[FR Doc. 2010–11379 Filed 5–12–10; 8:45 am]

BILLING CODE P

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Notice of Information Collection

AGENCY: National Aeronautics and Space Administration (NASA).

NOTICE: (10–050).

ACTION: Notice of information collection.

SUMMARY: The National Aeronautics and Space Administration, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995 (Pub. L. 104–13, 44 U.S.C. 3506(c)(2)(A)).

DATES: All comments should be submitted within 30 calendar days from the date of this publication.

ADDRESSES: All comments should be addressed to Brenda Maxwell, Mail Code JF000, National Aeronautics and Space Administration, Washington, DC 20546–0001.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument(s) and instructions should be directed to Brenda Maxwell, NASA PRA Officer, NASA Headquarters, 300 E Street, SW., Mail Code JF000, Washington, DC 20546, (202) 358–4616, *Brenda.Maxwell@nasa.gov*.

SUPPLEMENTARY INFORMATION:

I. Abstract

Information collection is required to evaluate bids and proposals from offerors to award contracts with an estimated value less than $500,000 for required goods and services in support of NASA's mission.

II. Method of Collection

NASA collects this information electronically where feasible, but information may also be collected by mail or fax.

III. Data

Title: NASA acquisition process, bids and proposals for contracts with an estimated value less than $500,000.

OMB Number: 2700–0087.

Type of Review: Renewal of a currently approved collection.

Affected Public: Business or other for-profit; Not-for-profit institutions; and State, Local or Tribal Government.

Estimated Number of Respondents: 3,772.

Estimated Annual Responses: 3,772.

Estimated Time per Response: 325 hours.

Estimated Total Annual Burden Hours: 1,225,900.

Estimated Total Annual Cost: $0.

IV. Request for Comments

Comments are invited on: (1) Whether the proposed collection of information is necessary for the proper performance of the functions of NASA, including whether the information collected has practical utility; (2) the accuracy of NASA's estimate of the burden (including hours and cost) of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including automated collection techniques or the use of other forms of information technology.

Brenda J. Maxwell,

NASA PRA Clearance Officer.

[FR Doc. 2010–11377 Filed 5–12–10; 8:45 am]

BILLING CODE P

NATIONAL SCIENCE FOUNDATION

Toward a Federal Cybersecurity Research Agenda: Three Game-Changing Themes

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

ACTION: Notice, request for public comment.

FOR FURTHER INFORMATION CONTACT: Tomas Vagoun at *Vagoun@nitrd.gov* or (703) 292–4873. Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1–800–877–8339 between 8 a.m. and 8 p.m., Eastern time, Monday through Friday.

DATES: Comments must be received by 5 p.m. EDT on June 18, 2010.

SUMMARY: With this notice, the National Coordination Office for Networking and Information Technology Research and Development (NITRD) requests input from the public regarding the Federal cybersecurity game-change research and development agenda. This request for information will be active from May 19, 2010 to June 18, 2010. Respondents are invited to respond online via the Cybersecurity R&D Kickoff forum at *http://cybersecurity.nitrd.gov/*, or may submit responses via electronic mail. Electronic mail responses will be re-posted on the online forum.

ADDRESSES: Submit comments by one of the following methods:

1. *Cybersecurity R&D Kickoff forum: http://cybersecurity.nitrd.gov/.*
2. *Via e-mail: cybersecurity@nitrd.gov.*
3. *Mail:* National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD), 4201 Wilson Blvd., Suite II–405, Arlington, VA 22230, *attn:* Tomas Vagoun.

Comments submitted in response to this notice may be made available to the public online or by alternative means. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you submit an e-mail comment, your e-mail address will be captured automatically and included as part of the comment that is placed in the public docket and made available on the Internet.

SUPPLEMENTARY INFORMATION:

Overview: This notice is issued by the National Coordination Office for the Networking and Information Technology Research and Development (NITRD) Program. In concert with the White House Office of Science and Technology Policy, agencies of the NITRD Program have identified three initial research and development (R&D) themes to exemplify and motivate future Federal cybersecurity game-change research activities: (a) Tailored Trustworthy Spaces, (b) Moving Target, (c) Cyber Economic Incentives. On Wednesday May 19, 2010, from 1:30 p.m.–5:00 p.m. PDT, representatives from the National Science Foundation, the Department of Homeland Security, and other agencies, will present the three themes at the Claremont Hotel, 41 Tunnel Road, Berkeley, CA 94705. This event will be webcast. For the event agenda, information about the webcast, and additional information, go to: *http://www.nitrd.gov/CSThemes.aspx*. This event will be the first discussion of these Federal cybersecurity game-change R&D objectives and will provide insights into the priorities that are shaping the direction of Federal research activities. Following this event, an on-line forum will be opened at *http://cybersecurity.nitrd.gov/* to provide an opportunity for comments and feedback.

Background: With the increased attention to cybersecurity, the President's Cyberspace Policy Review challenges the Federal community to develop a framework for R&D strategies that focus on game-changing technologies that can significantly enhance the trustworthiness of cyberspace (by "cyberspace" we mean the globally interconnected network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors in critical industries). Achieving enduring trustworthiness of the cyberspace requires new paradigms that re-balance security asymmetries of today's landscape: The cost of simultaneously satisfying all the requirements of an ideal cybersecurity solution in a static system is impossibly high, and so we must enable sub-spaces in cyberspace to support different security policies and different security services for different types of interactions; the cost of attack is asymmetric, favoring the attacker, and so defenders must increase the cost of attack and must employ methods that enable them to continue to operate in the face of attack; the lack of meaningful metrics and economically sound decision making in security misallocates resources, and so we must promote economic principles that encourage the broad use of good cybersecurity practices and deter illicit activities. The research agenda will be built by initially focusing on the three themes and on enabling component technologies supportive of, or required by these themes.

Invitation to Comment: Input is welcomed to refine these themes so that they can form the basis of an enhanced research agenda, enriching our understanding of how to design and build a more trustworthy cyberspace. Questions that individuals may wish to address include, but are not limited to the following:

1. How might the three themes be refined or enhanced to further improve cyberspace?
2. What are the research, development, implementation and other challenges in achieving the goals under each theme?
3. What state-of-the-art activities and use-cases can be cited in support of the three themes?
4. How would your organization's future vision support or incorporate the three themes?
5. Should there be a private sector organization to act as a partner to the public sector in a continuing game-change process?

Relevant input received through this request will be shared with the Federal agencies of the NITRD Program.

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

Dated: May 10, 2010.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2010–11443 Filed 5–12–10; 8:45 am]

BILLING CODE 7555–01–P

NATIONAL SCIENCE FOUNDATION

Toward a Federal Cybersecurity Research Agenda: Three Game-changing Themes

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. Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1–800–877–8339 between 8 a.m. and 8 p.m., Eastern time, Monday through Friday.

DATES: May 19, 2010.

SUMMARY: Representatives from Federal research agencies will present themes to exemplify and motivate future Federal cybersecurity research activities.

SUPPLEMENTARY INFORMATION:

Overview: This notice is issued by the National Coordination Office for the Networking and Information Technology Research and Development (NITRD) Program. In concert with the White House Office of Science and Technology Policy, agencies of the NITRD Program have identified three initial research and development (R&D) themes to exemplify and motivate future Federal game-change cybersecurity research activities: (a) Tailored Trustworthy Spaces, (b) Moving Target, (c) Cyber Economic Incentives. On Wednesday May 19, 2010, from 1:30 p.m.–5:00 p.m. PDT, representatives from the National Science Foundation, the Department of Homeland Security, and other agencies, will present the three themes at the Claremont Hotel, 41 Tunnel Road, Berkeley, CA 94705. This event will be webcast. For the event agenda and information about the webcast, go to: *http://www.nitrd.gov/CSThemes.aspx*. This event will be the first discussion of these Federal cybersecurity game-change R&D objectives and will provide insights into the priorities that are shaping the direction of Federal research activities. Following this event, an on-line forum will be opened at *http://cybersecurity.nitrd.gov/* to provide an opportunity for comments and feedback.

Background: With the increased attention to cybersecurity, the President's Cyberspace Policy Review challenges the Federal community to develop a framework for R&D strategies that focus on game-changing technologies that can significantly enhance the trustworthiness of cyberspace (by "cyberspace" we mean the globally interconnected network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors in critical industries). Achieving enduring trustworthiness of the cyberspace requires new paradigms that re-balance security asymmetries of today's landscape: the cost of simultaneously satisfying all the requirements of an ideal cybersecurity solution in a static system is impossibly high, and so we must enable sub-spaces in cyberspace to support different security policies and different security services for different types of interactions; the cost of attack is asymmetric, favoring the attacker, and so defenders must increase the cost of attack and must employ methods that enable them to continue to operate in the face of attack; the lack of meaningful metrics and economically sound decision making in security misallocates resources, and so we must promote economic principles that encourage the broad use of good cybersecurity practices and deter illicit activities. The research agenda will be built by initially focusing on the three themes and on enabling component technologies supportive of, or required by these themes. The Federal research community welcomes feedback to refine these themes so that they can form the basis of an enhanced research agenda. In the pursuit of these three initial themes, we expect new themes, possibly complementary and possibly overlapping, will emerge, enriching our understanding of how to design and build a more trustworthy cyberspace.

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