The agenda will focus on the following topics:

- Workgroup Report-Outs and Open Committee Discussion
- Extended Discussion on Proposed Pre-Apprenticeship Framework
- Review of Available Data Capabilities
- Long-Term Planning
- Apprenticeship Community of Practice
- Public Comment

Any member of the public who wishes to speak at the meeting must indicate the nature of the intended presentation and the amount of time needed by furnishing a written statement to the Designated Federal Official, Mr. John V. Ladd, by Monday, May 9, 2011. The Chairperson will announce at the beginning of the meeting the extent to which time will permit the granting of such requests.

Signed at Washington, DC, this 22nd day of March 2011.

Jane Oates,

Assistant Secretary for the Employment and Training Administration.

[FR Doc. 2011–7153 Filed 3–25–11; 8:45 am]

BILLING CODE 4510–FR–P

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

[Notice: (11–026)]

NASA Advisory Council; Science Committee; Meeting

AGENCY: National Aeronautics and Space Administration.

ACTION: Notice of meeting.

SUMMARY: In accordance with the Federal Advisory Committee Act, Public Law 92–463, as amended, the National Aeronautics and Space Administration (NASA) announces a meeting of the Science Committee of the NASA Advisory Council (NAC). This Committee reports to the NAC. The Meeting will be held for the purpose of soliciting from the scientific community and other persons scientific and technical information relevant to program planning.

DATES: Thursday, April 21, 2011, 8:30 a.m. to 4 p.m., and Friday, April 22, 2011, 8:30 a.m. to 2 p.m., Local Time.

ADDRESSES: NASA Headquarters, 300 E Street, SW., Room 5H45, Washington, DC 20546.

FOR FURTHER INFORMATION CONTACT: Ms. Marian Norris, Science Mission Directorate, NASA Headquarters, Washington, DC 20546, (202) 358–4452, fax (202) 358–4118, or *mnorris@nasa.gov.*

SUPPLEMENTARY INFORMATION: The meeting will be open to the public up to the capacity of the room. This meeting is also available telephonically and by WebEx. Any interested person may call the USA toll free conference call number 888–381–5774, pass code Science Committee, to participate in this meeting by telephone. The WebEx link is *https://nasa.webex.com/,* meeting number on April 21 is 994 561 164, and password SC_Apr21; the meeting number on April 22 is 992 613 633, and password SC_Apr22. The agenda for the meeting includes the following topics:

—Planetary Science Decadal Survey.
—Fiscal Year 2012 Budget Request.
—Program and Subcommittee Updates.

It is imperative that the meeting be held on these dates to accommodate the scheduling priorities of the key participants. Attendees will be requested to sign a register and to comply with NASA security requirements, including the presentation of a valid picture ID, before receiving an access badge. Foreign nationals attending this meeting will be required to provide a copy of their passport, visa, or resident alien card in addition to providing the following information no less than 10 working days prior to the meeting: full name; gender; date/place of birth; citizenship; visa/green card information (number, type, expiration date); passport information (number, country, expiration date); employer/affiliation information (name of institution, address, country, telephone); title/position of attendee. To expedite admittance, attendees with U.S. citizenship can provide identifying information 3 working days in advance by contacting Marian Norris via e-mail at *mnorris@nasa.gov* or by telephone at (202) 358–4452.

Dated: March 22, 2011.

P. Diane Rausch,

Advisory Committee Management Officer, National Aeronautics and Space Administration.

[FR Doc. 2011–7138 Filed 3–25–11; 8:45 am]

BILLING CODE 7510–13–P

NATIONAL SCIENCE FOUNDATION

Assumption Buster Workshop: Distributed Data Schemes Provide Security

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

ACTION: Call for participation.

FOR FURTHER INFORMATION CONTACT: *assumptionbusters@nitrd.gov.*

DATES: Workshop: May 17, 2011; Deadline: April 15, 2011. Apply via e-mail to *assumptionbusters@nitrd.gov.* Travel expenses will be paid for selected participants who live more than 50 miles from Washington, DC, up to the limits established by Federal Government travel regulations and restrictions.

SUMMARY: The NCO, on behalf of the Special Cyber Operations Research and Engineering (SCORE) Committee, an interagency working group that coordinates cyber security research activities in support of national security systems, is seeking expert participants in a day-long workshop on the pros and cons of the Security of Distributed Data Schemes. The workshop will be held May 17, 2011 in Gaithersburg, MD. Applications will be accepted until 5 p.m. EST April 15, 2011. Accepted participants will be notified by April 27, 2011.

SUPPLEMENTARY INFORMATION:

Overview: This notice is issued by the National Coordination Office for the Networking and Information Technology Research and Development (NITRD) Program on behalf of the SCORE Committee.

Background: There is a strong and often repeated call for research to provide novel cyber security solutions. The rhetoric of this call is to elicit new solutions that are radically different from existing solutions. Continuing research that achieves only incremental improvements is a losing proposition.

We are lagging behind and need technological leaps to get, and keep, ahead of adversaries who are themselves rapidly improving attack technology. To answer this call, we must examine the key assumptions that underlie current security architectures. Challenging those assumptions both opens up the possibilities for novel solutions that are rooted in a fundamentally different understanding of the problem and provides an even stronger basis for moving forward on those assumptions that are well-founded. The SCORE Committee is conducting a series of four workshops to begin the assumption buster process. The assumptions that underlie this series are that cyber space is an adversarial domain, that the adversary is tenacious, clever, and capable, and that re-examining cyber security solutions in the context of these assumptions will result in key insights that will lead to the novel solutions we desperately need. To ensure that our discussion has the requisite adversarial flavor, we are inviting researchers who

develop solutions of the type under discussion, and researchers who exploit these solutions. The goal is to engage in robust debate of topics generally believed to be true to determine to what extent that claim is warranted. The adversarial nature of these debates is meant to ensure the threat environment is reflected in the discussion in order to elicit innovative research concepts that will have a greater chance of having a sustained positive impact on our cyber security posture.

The third topic to be explored in this series is "Distributed Data Schemes Provide Security." The workshop on this topic will be held in Gaitherburg, MD on May 17, 2011.

Assertion: "Distributed Data Schemes Provide Security".

Distributed data architectures, such as cloud computing, offer very attractive cost savings and provide new means of large scale analysis and information sharing. There has been much discussion about securing such architectures, and it is generally felt that distribution, and the replication that is usually associated with it, provides some inherent protection; adversaries will have difficulty locating your data in the cloud, and by breaking it up and replicating different segments throughout the platform we send the adversary on a wild goose chase to find and reassemble all the relevant bits. It is also felt that cryptographic mechanisms like bound tags, encryption, and keyed access control can be used to develop distributed platforms with a high level of assurance. There are several applications of distributed architectures that offer non-sensitive peer to peer TV services. Applications are also offered for potentially sensitive uses like document collaboration. Yet it is unclear whether these applications can safely be extended to highly sensitive uses. Could we readily support a distributed electronic health care system that securely supports ad hoc consultations or remote surgery with full access to patient history while protecting patient privacy, for example?

To answer this question we need to take a closer look at the protection provided inherently and cryptographically. With respect to the former, we must think about how the architecture can be designed to provide secure availability to friend and not foe. We must examine the impact of the design for security, resilience, and availability and understand the trades we are implicitly making among these attributes. We must consider whether the data about data that is required by these architectures introduces a new data risk. We must think about the multiplicity of paths provide by these architectures. We must figure how to do risk analysis on a system when key information like data location is unavailable by design. With respect to the latter, we must consider whether the key management strategy is robust enough to operate in a distributed architecture. We have to think about the assurance of tag binding and access update and revocation. We must consider the vulnerabilities of the platforms that host the cryptographic mechanisms and the distribution of those functions in the architecture.

In this workshop, we will explore the implications of distributed data on security. We will consider what effect the introduction of the notion of a determined adversary has on our analysis of data security requirements. In the first session, we will discuss the properties of distributed platforms that are thought to make such architectures inherently more secure. In the second, we will discuss the issue of cryptography and distributed platforms.

How To Apply

If you would like to participate in this workshop, please submit (1) a resume or curriculum vita of no more than two pages which highlights your expertise in this area and (2) a one-page paper stating your opinion of the assertion and outlining your key thoughts on the topic. The workshop will accommodate no more than 60 participants, so these brief documents need to make a compelling case for your participation.

Applications should be submitted to *assumptionbusters@nitrd.gov* no later than 5 p.m. EST on April 15, 2011.

Selection and Notification: The SCORE committee will select an expert group that reflects a broad range of opinions on the assertion. Accepted participants will be notified by e-mail no later than April 27, 2011. We cannot guarantee that we will contact individuals who are not selected, though we will attempt to do so unless the volume of responses is overwhelming.

Submitted by the National Science Foundation for the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD) on March 18, 2011.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2011–7173 Filed 3–25–11; 8:45 am]

BILLING CODE 7555–01–P

NATIONAL SCIENCE FOUNDATION

Advisory Committee for Engineering; Notice of Meeting

In accordance with the Federal Advisory Committee Act (Pub. L. 92–463, as amended), the National Science Foundation announces the following meeting:

Name: Advisory Committee for Engineering Meeting, #1170.

Date/Time: April 13, 2011: 12 p.m. to 6 p.m., April 14, 2011: 8 a.m. to 12 p.m.

Place: National Science Foundation, 4201 Wilson Boulevard, Suite 1235, Arlington, Virginia 22230.

Type of Meeting: Open.

Contact Person: Deborah Young, National Science Foundation, 4201 Wilson Boulevard, Suite 505, Arlington, Virginia 22230.

Purpose of Meeting: To provide advice, recommendations and counsel on major goals and policies pertaining to engineering programs and activities.

Agenda: The principal focus of the meeting on both days will be to discuss emerging issues and opportunities for the Directorate for Engineering and its divisions and review Committee of Visitors Reports.

Dated: March 23, 2011.

Susanne Bolton,

Committee Management Officer.

[FR Doc. 2011–7175 Filed 3–25–11; 8:45 am]

BILLING CODE 7555–01–P

NUCLEAR REGULATORY COMMISSION

[NRC–2009–0476; DC/COL–ISG–018]

Office of New Reactors; Final Interim Staff Guidance on Standard Review Plan, Section 17.4, "Reliability Assurance Program"

AGENCY: Nuclear Regulatory Commission (NRC).

ACTION: Notice of availability.

SUMMARY: The NRC staff is issuing its Final Interim Staff Guidance (ISG) DC/COL–ISG–018 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML103010113). The purpose of this ISG is to clarify the NRC staff guidance on the design reliability assurance program (RAP). This ISG updates the guidance provided to the staff in Standard Review Plan (SRP), Section 17.4, "Reliability Assurance Program," of NUREG–0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," March 2007. This ISG revises the NRC staff's review responsibilities and further clarifies the acceptance criteria and evaluation findings contained in the SRP Section 17.4 in support of the NRC reviews of