

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@nitrdr.gov.

DATES: Workshop: May 17, 2011; Deadline: April 15, 2011. Apply via e-mail to assumptionbusters@nitrdr.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