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