ADDRESS: National Archives and Records Administration, 700 Pennsylvania Avenue, NW., Archivist's Reception Room, Room 105, Washington, DC 20408.

SUPPLEMENTARY INFORMATION: This meeting will be open to the public. However, due to space limitations and access procedures, the name and telephone number of individuals planning to attend must be submitted to the Information Security Oversight Office (ISOO) no later than Friday, February 25, 2011. ISOO will provide additional instructions for gaining access to the location of the meeting.

FOR FURTHER INFORMATION CONTACT: David O. Best, Senior Program Analyst, ISOO, National Archives Building, 700 Pennsylvania Avenue, NW., Washington, DC 20408, telephone number (202) 357–5123, or at *david.best@nara.gov*. Contact ISOO at *ISOO@nara.gov* and the NISPPAC at *NISPPAC@nara.gov.*

Dated: February 2, 2011.

Mary Ann Hadyka,

Committee Management Officer.

[FR Doc. 2011–2729 Filed 2–4–11; 8:45 am]

BILLING CODE 7515–01–P

NATIONAL CREDIT UNION ADMINISTRATION

Sunshine Act Notice; Cancellation of Meeting

TIME AND DATE: 5:30 p.m., Wednesday, February 2, 2011.

PLACE: Board Room, 7th Floor, Room 7047, 1775 Duke Street, Alexandria, VA 22314–3428.

STATUS: Closed.

FOR FURTHER INFORMATION CONTACT: Mary Rupp, Secretary of the Board, Telephone: 703–518–6304.

Mary Rupp,

Board Secretary.

[FR Doc. 2011–2697 Filed 2–3–11; 11:15 am]

BILLING CODE P

NATIONAL SCIENCE FOUNDATION

Assumption Buster Workshop: Defense-in-Depth Is a Smart Investment for Cyber 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:* March 22, 2011; *Deadline:* February 10, 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 Defense-in-Depth strategy for cyber security. The workshop will be held March 22, 2011 in the Washington DC area. Applications will be accepted until 5 p.m. EST February 10, 2011. Accepted participants will be notified by February 28, 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 first topic to be explored in this series is "Defense-in-Depth Is a Smart Investment." The workshop on this topic will be held in the Washington DC area on March 22, 2011.

Assertion: "Defense-in-Depth is a smart investment because it provides an environment in which we can safely and securely conduct computing functions and achieve mission success."

This assertion reflects a commonly held viewpoint that Defense-in-Depth is a smart investment for achieving perfect safety/security in computing. To analyze this statement we must look at it from two perspectives. First, we need to determine how the cyber security community developed confidence in Defense-in-Depth despite mounting evidence of its limitations, and second, we must look at the mechanisms in place to evaluate the cost/benefit of implementing Defense-in-Depth that layers mechanisms of uncertain effectiveness.

Initially developed by the military for perimeter protection, Defense-in-Depth was adopted by the National Security Agency (NSA) for main-frame computer system protection. The Defense-in-Depth strategy was designed to provide multiple layers of security mechanisms focusing on people, technology, and operations (including physical security) in order to achieve robust information assurance (IA).[1] Today's highly networked computing environments, however, have significantly changed the cyber security calculus, and Defense-in-Depth has struggled to keep pace with change. Over time, it became evident that Defense-in-Depth failed to provide information assurance against all but the most elementary threats, in the process putting at risk mission essential functions. The 2009 White House Cyberspace Policy Review called for "changes in technology" to protect cyberspace, and the 2010 DHS DOD MOA sought to "aid in preventing, detecting, mitigating and recovering from the effects of an attack," suggesting

[1] *Defense-in-Depth: A practical strategy for achieving Information Assurance in today's highly networked environments.*