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.*

a new dimension for Defense-in-Depth along the lifecycle of an attack.

Defense-in-Depth can provide robust information assurance properties if implemented along multiple dimensions; however, we must consider whether layers of sometimes ineffective defense tools may result in delaying potential compromise without providing any guarantee that compromise will be completely prevented. In today's highly networked world, Defense-in-Depth may best be viewed as a practical way to defer harm rather than a means to security. It is worth considering whether the Defense-in-Depth strategy tends to contribute more to network survivability than it does to mission assurance.

Intrusions into DoD and other information systems over the past decade provide ample evidence that Defense-in-Depth provides no significant barrier to sophisticated, motivated, and determined adversaries given those adversaries can structure their attacks to pass through all the layers of defensive measures. In the meantime, kinetic Defense-in-Depth of weapons platforms (such as aircraft) evolved into a life-cycle strategy of stealth (prevent), radars (detect), jammers and chaff (mitigate), fire extinguishers (survive) and parachutes (recover), a strategy that could provide value in the cyber domain.

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 February 10, 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 February 28, 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 February 2, 2011.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2011–2580 Filed 2–4–11; 8:45 am]

BILLING CODE 7555–01–P

NUCLEAR REGULATORY COMMISSION

[Docket No. 52–017; NRC–2008–0149]

Virginia Electric and Power Company D/B/A/ Dominion Virginia Power and Old Dominion Electric Cooperative, North Anna Power Station Combined License Application; Notice of Intent To Prepare a Supplemental Environmental Impact Statement and Conduct Scoping Process

On June 28, 2010, Virginia Electric Power Company d/b/a Dominion Virginia Power and Old Dominion Electric Cooperative (jointly referred to as Dominion) submitted a revision to its combined license (COL) application to build and operate a new reactor at its North Anna Power Station (NAPS) site located in Louisa County, Virginia. The NAPS property is located on the shore of Lake Anna approximately 64 km (40 mi) north-west of Richmond. The proposed new reactor, Unit 3, would be located adjacent to the existing NAPS Units 1 and 2.

Dominion's revision to its COL application, which included an environmental report (ER), changed the referenced reactor technology from the Economic Simplified Boiling Water Reactor Design (ESBWR) to the U.S. Advanced Pressurized Water Reactor (US–APWR). This change in reactor technology by Dominion occurred after the U.S. Nuclear Regulatory Commission (NRC) staff completed its environmental review, which is documented in NUREG–1917, "Supplemental Environmental Impact Statement for the Combined License (COL) for North Anna Power Station, Unit 3." A notice of availability of the final supplemental environmental impact statement (SEIS) for the COL application (NUREG–1917) was published in the **Federal Register** by the Environmental Protection Agency (EPA) on March 26, 2010 (75 FR 14594). The environmental impacts analyzed within NUREG–1917 are based, in part, on the design, construction, and operation of an ESBWR at the North Anna site.

The NUREG–1917 supplemented the final environmental impact statement (FEIS) developed for the Dominion Nuclear North Anna, LLC Early Site Permit (ESP), which the NRC issued on November 27, 2007. A notice of availability of NUREG–1811, "Environmental Impact Statement for an Early Site Permit at the North Anna ESP Site," was published in the **Federal Register** by the EPA on December 22, 2006 (71 FR 77014).

The purpose of this notice is to inform the public that the NRC staff will prepare a supplement to NUREG–1917 pertaining to the change in the reactor design. In the supplement, the staff intends to identify any significant changes to the previous evaluation of environmental impacts arising from the change in referenced reactor design. Additionally, the NRC staff is providing the public an opportunity to participate in the environmental scoping process for this supplement. The scoping opportunity affords the public an occasion to provide comments concerning the revisions to the application.

This notice advises the public that the NRC staff intends to gather information pertaining to the June 28, 2010, revisions to Dominion's ER and to include this information in the new supplement to be prepared in support of the COL review. In accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 51.45 and 51.50, the revised ER need not contain information or analysis submitted in the ER for the ESP stage or resolved in the FEIS for the ESP stage. This notice is being published in accordance with the National Environmental Policy Act of 1969, as amended (NEPA), and NRC regulations found in 10 CFR Part 51. As set forth in 10 CFR 51.92(a), the staff is directed to prepare a supplement to an FEIS when a proposed action has not been taken and if: (1) There are substantial changes in the proposed action that are relevant to environmental concerns, or (2) there is new and significant information or circumstances relevant to environmental concerns and bearing on the proposed action or its impacts. In addition, 10 CFR 51.92(c) permits the staff to prepare a supplement to a FEIS when, in its opinion, preparation of a supplement will further the purposes of NEPA.

The NRC will conduct a scoping process on the revisions to the ER, and, as soon as practicable thereafter, will prepare a draft SEIS for public comment. Participation in the scoping process by members of the public and local State, Tribal, and Federal government agencies is encouraged. The scoping opportunity will be used to accomplish the following: