NATIONAL CREDIT UNION ADMINISTRATION

Sunshine Act; Meeting Notice; Matter To Be Deleted From the Agenda of a Previously Announced Agency Meeting

TIME AND DATE: 11:30 a.m., Thursday, January 13, 2011.

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

STATUS: Closed.

1. MATTER TO BE DELETED: Insurance Appeals. Closed pursuant to exemptions (4), (6) and (7).

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

Mary Rupp,

Board Secretary.

[FR Doc. 2011–596 Filed 1–10–11; 11:15 am]

BILLING CODE P

NATIONAL SCIENCE FOUNDATION

Notice of Intent To Seek Approval To Renew an Information Collection

AGENCY: National Science Foundation.

ACTION: Notice and request for comments.

SUMMARY: The National Science Foundation (NSF) is announcing plans to request clearance of this collection. In accordance with the requirement of Section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995 (Pub. L. 104–13), we are providing opportunity for public comment on this action. After obtaining and considering public comment, NSF will prepare the submission requesting that OMB approve clearance of this collection for no longer than three years.

DATES: Written comments on this notice must be received by March 14, 2011 to be assured of consideration. Comments received after that date will be considered to the extent practicable.

For Additional Information or Comments: Contact Suzanne H. Plimpton, Reports Clearance Officer, National Science Foundation, 4201 Wilson Boulevard, Suite 295, Arlington, Virginia 22230; telephone (703) 292–7556; or send e-mail to *splimpto@nsf.gov.* Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1–800–877–8339 between 8 a.m. and 8 p.m., Eastern time, Monday through Friday. You also may obtain a copy of the data collection instrument and instructions from Ms. Plimpton.

SUPPLEMENTARY INFORMATION:

Title of Collection: NSF Surveys to Measure Customer Service Satisfaction.

OMB Number: 3145–0157.

Expiration Date of Approval: August 31, 2011.

Type of Request: Intent to seek approval to renew an information collection.

Abstract:

Proposed Project: On September 11, 1993, President Clinton issued Executive Order 12862, "Setting Customer Service Standards," which calls for Federal agencies to provide service that matches or exceeds the best service available in the private sector. Section 1(b) of that order requires agencies to "survey customers to determine the kind and quality of services they want and their level of satisfaction with existing services." The National Science Foundation (NSF) has an ongoing need to collect information from its customer community (primarily individuals and organizations engaged in science and engineering research and education) about the quality and kind of services it provides and use that information to help improve agency operations and services.

Estimate of Burden: The burden on the public will change according to the needs of each individual customer satisfaction survey; however, each survey is estimated to take approximately 30 minutes per response.

Respondents: Will vary among individuals or households; business or other for-profit; not-for-profit institutions; farms; federal government; state, local or tribal governments.

Estimated Number of Responses per Survey: This will vary by survey.

Comments: Comments are invited on (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Agency, including whether the information shall have practical utility; (b) the accuracy of the Agency's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information on respondents, including through the use of automated collection techniques or other forms of information technology; and (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Dated: January 7, 2011.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2011–524 Filed 1–11–11; 8:45 am]

BILLING CODE 7555–01–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.*

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 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 January 7, 2011.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2011–522 Filed 1–11–11; 8:45 am]

BILLING CODE 7555–01–P

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

SECURITIES AND EXCHANGE COMMISSION

Proposed Collection; Comment Request

Upon Written Request, Copies Available From: Securities and Exchange Commission, Office of Investor Education and Advocacy, Washington, DC 20549–0213.

Extension:

Rule 17a–4; SEC File No. 270–198; OMB Control No. 3235–0279.

Notice is hereby given that pursuant to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), the Securities and Exchange Commission ("Commission") is soliciting comments on the collection of information provided for in Rule 17a–4 (17 CFR 240.17a–4), under the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq.*). The Commission plans to submit this existing collection of information to the Office of Management and Budget for extension and approval.

Rule 17a–4 requires exchange members, brokers and dealers ("broker-dealers") to preserve for prescribed periods of time certain records required to be made by Rule 17a–3. In addition, Rule 17a–4 requires the preservation of records required to be made by other Commission rules and other kinds of records which firms make or receive in the ordinary course of business. These include, but are not limited to, bank statements, cancelled checks, bills receivable and payable, originals of communications, and descriptions of various transactions. Rule 17a–4 also permits broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be maintained under Rules 17a–3 and 17a–4.