

generalized to the population of study. This feedback will provide insights into customer or stakeholder perceptions, experiences and expectations, provide an early warning of issues with service, or focus attention on areas where communication, training or changes in operations might improve delivery of products or services. These collections will allow for ongoing, collaborative and actionable communications between the Agency and its customers and stakeholders. It will also allow feedback to contribute directly to the improvement of program management.

Feedback collected under this generic clearance will provide useful information, but it will not yield data that can be generalized to the overall population. This type of generic clearance for qualitative information will not be used for quantitative information collections that are designed to yield reliably actionable results, such as monitoring trends over time or documenting program performance. Such data uses require more rigorous designs that address: The target population to which generalizations will be made, the sampling frame, the sample design (including stratification and clustering), the precision requirements or power calculations that justify the proposed sample size, the expected response rate, methods for assessing potential non-response bias, the protocols for data collection, and any testing procedures that were or will be undertaken prior fielding the study. Depending on the degree of influence the results are likely to have, such collections may still be eligible for submission for other generic mechanisms that are designed to yield quantitative results.

The Agency received no comments in response to the 60-day notice published in the **Federal Register** of December 22, 2010 (75 FR 80542).

Below we provide the National Science Foundation's projected average estimates for the next three years:¹

Current Actions: New collection of information.

Type of Review: New collection.

Affected Public: Individuals and households, businesses and

organizations, State, Local or Tribal Government.

Average Expected Annual Number of Activities: 10.

Respondents: 500 per activity.

Annual Responses: 5,000.

Frequency of Response: Once per request.

Average Minutes per Response: 30.

Burden hours: 2,500.

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid Office of Management and Budget control number.

Dated: February 22, 2011.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2011-4274 Filed 2-24-11; 8:45 am]

BILLING CODE 7555-01-P

NATIONAL SCIENCE FOUNDATION

Assumption Buster Workshop: Trust Anchors Are Invulnerable

AGENCY: The National Coordination Office (NCO) for the Networking and Information Technology Research and Development (NITRD) Program.

ACTION: Call for participation.

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 use and implementation of trust anchors. The workshop will be held April 27, 2011 in the Savage, MD area. Applications will be accepted until 5 p.m. EST March 18, 2011. Accepted participants will be notified by March 30, 2011.

DATES: *Workshop:* April 27, 2011; *Deadline:* March 18, 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.

FOR FURTHER INFORMATION CONTACT: assumptionbusters@nitrd.gov.

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 second topic to be explored in this series is "Trust Anchors are Invulnerable." The workshop on this topic will be held in the Savage, MD area on April 27, 2011.

Assertion: "Trust anchors are invulnerable thus users who faithfully deploy reliable trust anchors can be confident that they are immune from the attacks."

This assertion underlies significant cyber security research and development that is aimed at developing and implementing invulnerable trust anchors, security keystones that cannot be circumvented, and that assure that trust in a system is well grounded. Numerous trust anchors are proffered at different levels of assurance and for different aspects of the system. Platform trust is assured by

¹ The 60-day notice included the following estimate of the aggregate burden hours for this generic clearance Federal-wide:

Average Expected Annual Number of activities: 25,000.

Average number of Respondents per Activity: 200.

Annual responses: 5,000,000.

Frequency of Response: Once per request.

Average minutes per response: 30.

Burden hours: 2,500,000.

the Trusted Platform Module. Trusted authentication is provided by tokens. The padlock on the browser assures we can trust web interactions since they are protected by SSL. Close-held keys and strong key management systems assure cryptographic trust.

At the workshop we will explore what assurances these trust anchors do and do not provide, what they depend upon, how they do or do not interact with the rest of the system, how they typically fail, and what needs to be addressed to enable effective use of them.

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 March 18, 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 March 30, 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 22, 2011.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2011-4272 Filed 2-24-11; 8:45 am]

BILLING CODE 7555-01-P

POSTAL SERVICE

International Product Change— International Business Reply Service Contract

AGENCY: Postal Service™.

ACTION: Notice.

SUMMARY: Postal Service gives notice of filing a request with the Postal Regulatory Commission to add International Business Reply Service Competitive Contract 3 to the

Competitive Products List pursuant to 39 U.S.C. 3642.

DATES: February 25, 2011.

FOR FURTHER INFORMATION CONTACT: Margaret M. Falwell, 202-268-2576.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that it has filed with the Postal Regulatory Commission a Request of United States Postal Service To Add International Business Reply Service Competitive Contract 3 to the Competitive Products List, and Notice of Filing Contract (Under Seal). Documents are available at <http://www.prc.gov>, Docket Nos. MC2011-21 and CP2011-59.

Neva R. Watson,

Attorney, Legislative.

[FR Doc. 2011-4209 Filed 2-24-11; 8:45 am]

BILLING CODE 7710-12-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-63936; File No. SR-DTC-2011-03]

Self-Regulatory Organizations; the Depository Trust Company; Notice of Filing and Immediate Effectiveness of Proposed Rule Change Regarding Providing Participants With a New Optional Settlement Web Interface

February 22, 2011.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (“Act”),¹ notice is hereby given that on February 7, 2011, The Depository Trust Company (“DTC”) filed with the Securities and Exchange Commission (“Commission”) the proposed rule change as described in Items I and II below, which Items have been prepared primarily by DTC. DTC filed the proposed rule change pursuant to Section 19(b)(3)(A)(iii) of the Act² and Rule 19b-4(f)(4)³ thereunder so that the proposal was effective upon filing with the Commission. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Self-Regulatory Organization’s Statement of the Terms of Substance of the Proposed Rule Change

The proposed rule change will establish a new browser-based interface, the “Settlement Web,” that allows Participants to view their settlement-related activity.

¹ 15 U.S.C. 78s(b)(1).

² 15 U.S.C. 78s(b)(3)(A)(iii).

³ 17 CFR 240.19b-4(f)(4).

II. Self-Regulatory Organization’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, DTC included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. DTC has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

DTC Participants have the ability to view all of their settlement related activity using different functions in the Participant Browser System (“PBS”).⁴ Based on request from its Participants, DTC has created a more user-friendly interface called Settlement Web that allows Participants to view their settlement related activity. The Settlement Web will reduce the amount of time that Participants spend in PBS by increasing the efficiency in searching for settlement activity. Participants that chose to use the Settlement Web will have access to a Navigation Bar that will provide Participants with improved inquiry and update capabilities for their settlement transactions. Participants will also have the ability to view different settlement related activities using the Dashboard in the Settlement Web homepage. Additionally, Participants will have the option to use an alert function located within the Settlement Web’s dashboard to provide them to set alerts regarding settlement related events.⁵ Participants will be able to customize the function to control which events for which they want to be notified. These alerts will reduce the amount of time spent in PBS because Participants will no longer have to manually check multiple settlement functions to be made aware of various settlement events. Notifications will be made available to Participants through the alerts window in the dashboard or by e-mail. The e-mail will notify the

⁴ In 2008, DTCC completed a multi-year initiative to transition all Participant Terminal System (“PTS”) functions to PBS. Now, rather than toggle between the two tools, Participants can manage all their needs through the web-based PBS, which is more flexible than PTS while offering greater functionality. However, Participants are still able to use PTS for most of their settlement activities.

⁵ Events, which include, for example, settlement extension broadcasts and the receipt of a specific delivery, are regularly scheduled processing milestones associated with a given settlement cycle.