that may be accumulated throughout an agency. This notice provides the control number assigned to each schedule, the total number of schedule items, and the number of temporary items (the records proposed for destruction). It also includes a brief description of the temporary records. The records schedule itself contains a full description of the records at the file unit level as well as their disposition. If NARA staff has prepared an appraisal memorandum for the schedule, it too includes information about the records. Further information about the disposition process is available on request.

Schedules Pending:

1. Department of the Interior, Office Surface Mining and Reclamation Enforcement (N1- 471–10–5, 2 items, 1 temporary item). Master files of an electronic information system used to document unfunded high priority coal reclamation projects. Proposed for permanent retention are snapshots of the master files.

2. Department of Justice, Federal Bureau of Investigation (N1–65–10–14, 3 items, 2 temporary items). Records of the Domestic Emergency Support Team in the Critical Incident Response group, including files related to training, exercises, and responses to events as well as administrative files. Proposed for permanent retention are policy files.

3. Department of Justice, Federal Bureau of Investigation (N1–65–10–17, 1 item, 1 temporary item). Master files of electronic information systems used to analyze large volumes of evidence to facilitate case processing. Evidence used in an investigation is filed in the appropriate investigation case file.

4. Department of Justice, Federal Bureau of Investigation (N1–65–10–19, 3 items, 1 temporary item). Records of the Foreign Emergency Report Team in the Critical Incident Response Group, including deployment files for protection at overseas meetings, events, training, and exercises. Proposed for permanent retention are deployment files related to terrorist incidents and other high-profile incidents.

5. Department of Justice, Federal Bureau of Investigation (N1–65–11–8, 5 items, 5 temporary items). Records of the Office of Congressional Affairs, including calendars, reference material, routine constituent inquiries, and master files of an electronic information system used to track correspondence.

6. Department of Justice, Federal Bureau of Investigation (N1–65–11–9, 2 items, 2 temporary items). Records of the Institutional Review Board relating to research projects undertaken within the agency, including research proposals, informed consent forms, and other administrative management records.

7. Department of Justice, Federal Bureau of Investigation (N1–65–11–12, 1 item, 1 temporary item). Records of the Critical Incident Response Group, including case files related to counterterrorism preparedness for special events.

8. Administrative Office of the United States Courts, United States Bankruptcy Courts (N1–578–11–1, 11 items, 2 temporary items). Non-electronic bankruptcy case files and adversary proceedings files not selected as permanent by random sampling or by historical selection criteria. Proposed for permanent retention are case files dated 1940 and earlier; cases filed under the Bankruptcy Acts of 1800, 1841, and 1867; cases files under the Bankruptcy Acts of 1898 and 1978 under Chapter VIII, Section 75 (Agricultural), Chapter VIII, Section 77 (Railroad Reorganization), Chapter IX (Political Subdivisions), Chapter X (Corporate Reorganizations), Chapter XV (Railroad Adjustments), Chapter 7, Subchapters III (Stockbroker) and IV (Commodity Broker), Chapter 9 (Municipality), Chapter 11, Subchapter IV (Railroad Reorganization), case files containing orders pursuant to Chapter XIV of the Bankruptcy Act of 1898 or Section 908 of Title IX of the Merchant Marine Act; Chapter 12 of the Congressional Act of 1986 (Family Farms and Family Fishermen); historically significant cases; cases selected in a random sample; and adversary proceedings that go to trial, are historically significant, and are selected by a random sample.

9. Administrative Office of the United States Courts, United States District Courts (N1–21–11–1, 6 items, 2 temporary items). Criminal case files for misdemeanors, petty offenses, non-trial cases from 1970 or after. Proposed for permanent retention are trial cases; cases relating to treason, national security, or crimes by public officials; and historically significant cases.

10. Federal Maritime Commission, Agency-wide (N1–358–10–1, 2 items, 2 temporary items). Master files of an electronic information system containing copies of commission issuances and public filings for public use. Also included is the agency website containing information about the agency and its programs.

Dated: April 20, 2011.

Sharon G. Thibodeau,

Deputy Assistant Archivist for Records Services—Washington, DC.

[FR Doc. 2011–10023 Filed 4–22–11; 8:45 am]

BILLING CODE 7515–01–P

NATIONAL SCIENCE FOUNDATION

Assumption Buster Workshop: Abnormal Behavior Detection Finds Malicious Actors

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

ACTION: Call for participation.

FOR FURTHER INFORMATION CONTACT: *assumptionbusters@nitrd.gov.*

DATES: *Workshop:* June 20, 2011; *Deadline:* May 13, 2011. Apply via e-mail to *assumptionbusters@nitrd.gov.* Travel expenses will be paid at the government rate for selected participants who live more than 50 miles from Washington DC.

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 abnormal and malicious behavior detection. The workshop will be held June 20, 2011 in the Washington DC area. Applications will be accepted until 5 p.m. EDT, May 13, 2011. Accepted participants will be notified by May 25, 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 fourth topic to be explored in this series is "Abnormal Behavior Detection Finds Malicious Actors." The workshop on this topic will be held in the Washington, DC area on June 20, 2011.

Assertion: "Abnormal Behavior Detection Finds Malicious Actors."

In an effort to reduce losses due to fraud, financial services companies have been fairly successful in establishing fraud detection analytics, based on abnormal behavior identification, which identify financial transactions that seem out of norm for a particular financial services customer. For example, credit card companies acting on this information will contact cardholders to validate anomalous behavior, or if costs are high, and users unavailable, can freeze accounts until the anomaly is investigated. In this way, they can curtail the loss due to prolonged invalid use of a credit card. Fraud detection algorithms (based on user behavior models) and procedures immediately set off account alarms and/or deny additional transactions after they have detected a fraudulent or suspicious transaction. Depending upon the fraud method (*e.g.,* automated gasoline purchase), they may not always block the first fraudulent transaction on a given card.

Online banking financial institutions employ similar behavioral models to monitor the size and destinations of financial transfers, and/or on-line transactions (such as change of address or payee) will delay transfers until the customer can be reached to confirm the transactions and/or provide additional authentication. Despite the use of best available behavior modeling and monitoring, financial institutions continue to sustain significant financial loss from fraud. Can the field of fraud detection (and cybersecurity in general) be improved by new technology and approaches?

Fraud detection works on the assumption that malicious fiscal behavior is a subset of abnormal behavior—if the fraudulent user mimics the financial behavior of the authorized user, these methods do not work. Detection methods do not assume that malicious behavior is automatically distinguishable from unusual behavior on the part of authorized users. The fraud detection algorithms use the financial services customer's history to build a profile of "normal" transactions and develop thresholds for unusual behavior. The volume of transactions allows for reasonable thresholds to be established. Fraud detection methods rely on strong models of normal behavior, or known criminal behavior characteristics. The development of many of these models is aided by the fact that the value of a transaction is numeric and allows sets of values to be analyzed with well understood algorithms. For example, credit card purchases have relatively small and fixed semantics: Store names are typed, businesses are categorized, relationships among businesses and purchases by card users are fairly easy to establish (e.g., people who buy plane tickets may also purchase luggage, or may eat out more when they are away, or may spend more in general while traveling). These models enable gradual change in behavior to be learned and help drive down false alerts.

Many cyber intrusion detection techniques, or insider threat detection techniques, aim to achieve similar results by using abnormal behavior detection as a starting point. Yet, it is an open question whether these techniques can expect to attain the same broad-based success when applied in the broader cyber security domain. The domains share an adversarial dynamic that might indicate that similar analyses could be effective. But do the assumptions of the relationship between malicious and normal behavior hold true? Can we establish a solid footing in terms of models of normal transaction semantics and transaction value? Does the real time nature of cyber decision making, and the ease of dynamic changes in the criminal's attack signature, present insurmountable challenges for behavioral techniques?

In this workshop, representatives from government and industry financial organizations will present different financial services fraud detection mechanisms, strengths, and areas needing further development. This will allow workshop participants to have a common understanding of the state of fraud detection practice.

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 exploring new ideas to improve fraud detection specifically, and malicious cyber behavior in general. 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. EDT on May 13, 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 May 25, 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 April 19, 2011.

Suzanne H. Plimpton,

Reports Clearance Officer, National Science Foundation.

[FR Doc. 2011–9877 Filed 4–22–11; 8:45 am]

BILLING CODE 7555–01–P

NUCLEAR REGULATORY COMMISSION

[Docket No. 70–0036; NRC–2009–0278]

Notice of Availability of Draft Environmental Assessment and Finding of No Significant Impact for a License Amendment to Materials, License No. SNM–33, Westinghouse Electric Company, LLC, Hematite Decommissioning Project, Festus, Missouri (TAC NO. J00357)

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice of Availability.

DATES: The public comment period on the draft Environmental Assessment and Finding of No Significant Impact (FONSI) closes on May 25, 2011. Written comments should be submitted as described in the **ADDRESSES** section of