POLICY ISSUE
NOTATION VOTE

July 13, 2011 SECY-11-0094

FOR: The Commissioners

FROM: R. W. Borchardt
Executive Director for Operations

SUBJECT: ADVANTAGES AND DISADVANTAGES OF CHANGING THE CURRENT AUTHENTICATION ASSURANCE LEVEL (LEVEL 4) OF THE NATIONAL SOURCE TRACKING SYSTEM

PURPOSE:

To provide the Commission with the staff's discussion of the advantages and disadvantages associated with changing the authentication assurance level of the National Source Tracking System (NSTS) from a Level 4 to a Level 3 as requested in the Staff Requirements Memorandum (SRM) for SECY-10-0112, "Report Regarding Encouraging States and Licensees to Complete National Source Tracking System Credentialing and to use the System Electronically." Additionally, the staff is requesting Commission approval for the staff to pursue a graduated implementation approach to authentication assurance levels for the NSTS. This paper does not address any new commitments.

SUMMARY:

Since 2006, there have been significant enhancements in the area of source security and protection. Licensees authorized to possess Category 1 and Category 2 quantities of radioactive material, as described in the International Atomic Energy Agency's "Code of Conduct on the Safety and Security of Radioactive Sources," are required to comply with a number of security requirements (i.e., Panoramic and Underwater Irradiators, Manufacturers and Distributors, Shipment of Radioactive Materials Quantities of Concern, Increased Controls and Fingerprinting).

The Energy Policy Act of 2005 directed the U.S. Nuclear Regulatory Commission (NRC) to establish a tracking system for radiation sources in the United States. The NSTS was

CONTACT: Kim Lukes, FSME/MSSA
301-415-6701

developed in response to this direction. In January 2009, licensees began reporting their Category 1 and 2 source information in the NSTS. Licensees have access solely to the information concerning their own material holdings.

The information stored in the NSTS is designated Official Use Only (OUO) - Security-Related Information, a category of Sensitive Unclassified Non-Safeguards Information. The type of information included in the NSTS is the radioactive material (radionuclide) activity at manufacture, licensee contact information, and notification of material transfer or acknowledgment of material receipt. Physical protection information associated with the security requirements is not included in the NSTS. The NRC's publicly available "Implementing Guidance for the Increased Controls"[1] notes that physical protection information is a form of "sensitive information" that should be password protected if stored in non-removable electronic form. However, the sealed source information in the NSTS, a form of OUO information, is currently being protected at a much higher access level than just password protection.

The staff initiated the re-evaluation of the NSTS' security categorization (SecCat) and the Electronic authentication (E-auth) risk assessment to determine the appropriate sensitivity of the source information in the NSTS and to determine if the Level 4 authentication assurance level first established for the system was still appropriate. The SecCat and E-auth risk assessment establish the foundation on which the entire Certification and Accreditation package[2] is normally developed, reviewed, and approved by the Designated Approving Authority (DAA) in order to grant the system's Authority To Operate (ATO). In order to be responsive to the direction in SRM-SECY-10-0112, the staff is going beyond the established process for obtaining DAA approval and submitting this notation vote paper. In this paper, the staff is recommending that the Commission approve changing the sensitivity determination of the NSTS source information and pursue a graduated implementation approach to the authentication assurance level for the NSTS.

BACKGROUND:

To ensure the effectiveness of information security controls over Government information, Congress passed Public Law 107-347, the E-Government Act of 2002. Title III of the Act, known as the Federal Information Security Management Act of 2002 (FISMA), requires agency heads to formally delegate information security program governance, accountability, and oversight to the Chief Information Officer (CIO) and requires the CIO to appoint a senior agency information security officer or Chief Information Security Officer (CISO) to establish and sustain an agency level information security program. In response to the Act's provisions, the NRC's Executive Director for Operations delegated responsibility to the agency's Deputy Executive Directors to serve as the DAA, effective October 2007 (Agencywide Documents Access and Management System (ADAMS) ML072630477), and approved the selection of the agency CISO in March 2008 (ADAMS ML080730491). These executives are responsible for the establishment and implementation of the NRC information security program. In December 2008, the DAA granted the NSTS its ATO. The initial step in achieving a system's ATO is performing a SecCat review. This is the process of categorizing information and information

[1] Increased Controls information is available on the NRC public website at: http://www.nrc.gov/security/byproduct/orders.html#increasedcontrols

[2] A security certification of the system will be conducted in accordance with the Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources;" NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems;" and NRC policy for security accreditation.

systems based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization. Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization from the breach of a computer system.

The SecCat starts with the identification of the information types the system will store, process, and transmit. The sensitivity of these information types is rated in terms of the likely security impacts with the loss of Confidentiality, Integrity, and Availability (C, I, and A)[3] of the information. The SecCat for the NSTS was first performed in 2006 during the developmental phase of the system. At that time, the NSTS was categorized as "high" because it was determined that the loss of C, I, or A could be expected to have a "severe/catastrophic" adverse affect on organizational operations, organizational assets, or individuals.

Another step in achieving a system's ATO is performing an E-auth risk assessment. This is the process of establishing confidence in user identities electronically presented to an information system using the Internet. The Office of Management and Budget Memorandum (OMB) M-04-04, "E-Authentication Guidance for Federal Agencies," provides the criteria for determining the level of E-auth assurance required for specific applications and transactions, based on the risks and the risk likelihood. OMB M-04-04 defines four levels of assurance, Levels 1 to 4. Level 1 is the lowest assurance level and Level 4 is the highest. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, "Electronic Authentication Guideline," provides further detail with respect to the technical requirements for each of the four levels.

In 2006, the authentication assurance level for the NSTS was determined to be a Level 4, which provides the highest confidence in validating the identity of a system user. The NIST SP 800-60, Volume 1, "Guide to Mapping Types of Information and Information Systems to Security Categories," notes that "it is important to routinely revisit the security categorization as the mission/business changes because it is likely the impact levels…may change as well." NIST SP 800-60 further states that "an incorrect information system impact analysis can result in the agency either over protecting the information system thus wasting valuable security resources, or under protecting the information system and placing important operations and assets at risk." Given the experience gained over the last two years of the NSTS being in operation as well as the significant enhancements in the area of radiation source protection and security since 2006, coupled with FSME efforts to improve the alignment of the NSTS companion systems (Web-Based Licensing and License Verification System) as part of the Integrated Source Management Portfolio, the staff determined that a re-evaluation of the SecCat and E-auth was warranted.

DISCUSSION:

Currently, licensees have several options for reporting transaction information to the NSTS. Reporting can be done through the on-line system, by e-mail, by fax, by mail, or by telephone. NRC staff considers on-line access to be the most efficient and accurate method to report source transactions with the least expenditure of NRC and contractor resources for data entry.

[3] A loss of Confidentiality refers to the unauthorized disclosure of information. A loss of Integrity refers to the unauthorized modification or destruction of information. A loss of Availability refers to the disruption of access to or use of information or an information system.

In order to report to the NSTS on-line, an individual must enroll for a digital certificate because the security of the NSTS is based in part on the use of digital certificates. These certificates are currently loaded onto hard tokens or smart cards. A digital certificate is an electronic identifier which establishes a user's credentials when processing transactions on the Internet. The use of digital certificates allows the NSTS to uniquely identify each user. The process of obtaining the digital certificate is called credentialing. The process of verifying that the person applying for a credential is who he or she claims to be is referred to as identity validation or identity proofing.

The credentialing and identity validation requirements to operate the NSTS at Level 4 introduced certificate installation difficulties due to the certificates not being compatible with certain computer operating systems. These difficulties were initial impediments to on-line usage. New and current users continue to encounter similar difficulties that inhibit on-line usage of the NSTS.

As discussed below, there are differences in the certificate collection and identity validation process for a Level 4 and a Level 3 authentication. However, regardless of what authentication assurance level is chosen, all of the remaining security controls will initially be maintained at their current level and the access controls could be tailored (i.e., still require Level 4 identity proofing for Level 3 access) upon DAA approval.

Identity Validation Requirements

For a Level 4 authentication, as part of the identity proofing approval process, an applicant must provide in person to a notary or an NRC Trusted Agent, who manages certificate enrollments by ensuring the information is accurate and valid, two acceptable forms of identification and a recent passport-style photograph. With “in-person” proofing, there is higher assurance that the person applying is the individual requesting access to NSTS, and is the person whose background is being checked in the credentialing process. However, it has been found that paperwork has been returned due to mismatched signature dates (i.e., the applicant and notary and/or NRC Trusted Agent had signed and dated the paperwork on different days) or the seal has not always been affixed on the documents signed by the notary. These types of mistakes, at the inception of the program, may well have been the largest factor for users not being willing to continue with the process of applying for on-line access and choosing alternate means of reporting to NSTS. Today, the credentialing process has reached a level of maturity such that most applicants who choose to pursue on-line access to NSTS are able to successfully navigate through the credentialing process.

Level 3 requires that the applicant provide two acceptable forms of identification, including a Government-issued photograph identification, such as a driver’s license or passport. Level 3 identity proofing requirements are very similar to Level 4, with an option for remote identity validation in lieu of in-person proofing. The remote identity validation can be performed by validating the information with the agency that issued the identification card to the applicant or through credit bureaus or similar authoritative databases that confirm the identity of the individual. However, applicants may be apprehensive of sharing financial information for review.

Certificate Collection Process

For a Level 4 authentication, following the final identity proofing approval, the user is shipped a personalized smart card and reader. Upon receiving the smart card and reader, the user must complete three software component installations in order to collect certificates (equivalent to card activation) for access to the NSTS.

For a Level 3 authentication, there would be fewer steps for users to complete in order to collect certificates for access to the NSTS. The number of software component installations required would decrease from three to one. Additionally, a Level 3 authentication does not require the use of a smart card and reader. With the elimination of a smart card and reader, there would be less Government-issued equipment to track and it would eliminate the possibility of users losing or damaging the equipment.

Another advantage of a Level 3 authentication over a Level 4 authentication is the fact that a user will only need to go to a website to install the digital certificate and obtain a certificate password in order to access the system, as opposed to needing a smart card (with the digital certificate loaded onto it), reader, and pin to access the system. Much staff time has been devoted to assisting users in installing the certificates onto and using the smart cards in order to access the NSTS. Less hardware[4] and easier access to the NSTS would better utilize staff efforts. The enclosure provides more detailed information on the certificate collection requirements for both Level 4 and Level 3 authentications.

Operating Systems and Browsers

Currently, with NRC's solution for meeting the compatibility of a Level 4 authentication, the digital certificates can only be loaded onto smart cards using specific versions of Microsoft Windows operating systems and Microsoft Internet Explorer. Some users may not have these specific versions of products in their infrastructure. Computer compatibility issues will persist as computer technology continues to evolve. However, there would be no user computer compatibility issues with respect to implementing an alternative Level 4 system, as described in more detail in the enclosure.

An advantage of a Level 3 authentication over a Level 4 authentication is that the software certificates could be used on most operating systems (i.e., various versions of Microsoft Windows) as long as the browser being used is Microsoft Internet Explorer or Mozilla Firefox (some other 'mainstream' browsers may work as well).

The staff believes that any of the options discussed below would allow the NRC to adequately monitor sources entered into the NSTS by users. Thus the evaluation of options centers on how best to use NRC's limited resources to achieve the goals of increasing public confidence in the monitoring of sources, increasing the efficiency and effectiveness of the NSTS, and reducing unnecessary regulatory burden on stakeholders. However, as mentioned above, in order to appropriately determine if the current authentication assurance level (Level 4) should be changed, a re-evaluation of the SecCat had to be performed.

[4] A reduction of approximately 8.5 business days (completion time for fulfilling a smart card and reader request) could be achieved by eliminating the need for the smart card and reader, as required under the current Level 4 system. This savings in the number of days is estimated based on observation of the current process and Service Level Agreements with vendors.

The re-evaluation considered all four authentication levels. FSME, the NSTS information system owner, has completed its re-evaluation of the NSTS SecCat and E-auth (ADAMS ML111440309) and CSO has reviewed and approved its recommendation (ADAMS ML11174A219). The results of the SecCat re-evaluation categorize the NSTS as a "moderate" system. The E-auth review process included an objective analysis of the security ramifications of all four authentication assurance levels for processing information in the NSTS and determined the most appropriate access level for NSTS users. The results of the E-auth suggest that a graduated approach to NSTS access authorization, as exemplified in Option 4 below, establishing a Level 3 authentication for users with system-wide access and/or administrative rights and a Level 2 authentication for those with limited access, may be appropriate for implementation. The technological aspects of a Level 4, Level 3, and Level 2 authentication are detailed in the enclosure.

Option 1 - NSTS remains a Level 4 authentication. Option 1 implements the current approach to obtaining access to the NSTS. The current approach has certain limitations with respect to the identity proofing and certificate collection processes. It may be a severe impediment to greater use of the on-line system if the NSTS were expanded to track lower activity sources, such as Category 3 sources. Currently, there are approximately 60,000 annual transactions of Category 1 and 2 sources in the NSTS. That number would be expected to nearly double with the inclusion of Category 3 sources and approximately 1,000 new licensee users added to the approximately 1,400 licensees currently using the system. However, as noted in more detail in the enclosure, the staff conducted research on the feasibility of an alternative Level 4 authentication assurance method. This method does not employ use of a hard token, such as the smart card and reader, currently used for NSTS that has posed a difficulty for new users of the system. Therefore, there is another method that can be employed to meet the Level 4 requirements that avoids the burdens of downloading certificates on smart cards and alleviates the computer compatibility issues that are experienced with the current Level 4 authentication.

Option 2 - NSTS becomes a Level 3 authentication. Option 2 significantly reduces some of the certificate collection challenges on users that currently access or could access the system. Alleviating some of these challenges could encourage new users to use the system on-line. Although Option 2 would be an improvement over the status quo, it would be better to employ a graduated approach as exemplified in Option 3 or Option 4.

Option 3 - NSTS applies a graduated approach by which NSTS remains a Level 4 authentication for users having system-wide access and/or administrative rights to the system and a Level 3 authentication for users granted only limited access. NIST SP 800-60, Volume 1, indicates that "some information may have little or no sensitivity in isolation but may be highly sensitive in aggregation." Specifically, Option 3 includes no change in the current approach for those users with system-wide access (NRC and Agreement State regulators) and/or administrative rights to the system. However, Option 3 lessens the certification challenges and resource burdens for those users with limited access capabilities (licensees that have access to only their source inventory). It would be advantageous to change the system for a subset of users based on their roles and associated access rights to encourage more on-line use of the system; however, there would be transition burdens such as maintaining a schedule and process for collecting the smart cards and readers and assisting users in installing software certificates to their browsers and obtaining new certificate passwords.

Option 4 - NSTS applies a graduated approach by which NSTS employs Level 3 authentication for users having system-wide access and/or administrative rights to the system and a Level 2 authentication for users granted only limited access. This option applies a graduated approach similar to Option 3; however, the authentication assurance levels chosen in this option are based on the results of the E-auth risk assessment. Therefore, it would be preferable to consider the feasibility of implementation of this option.

RECOMMENDATION:

The staff recommends that the Commission approve the request to consider the feasibility of implementing a graduated authentication approach concept, as discussed in Option 4, with an overall system security impact level of "moderate" for NSTS.

RESOURCES:

Since the inception of NSTS, there have been many improvements made regarding the identity validation and credentialing processes. Most users who find it practical to report on-line are now doing so; however, simplifying the credentialing process could persuade more users to report on-line. A simplified process would likely reduce some of the obstacles and frustrations that in the past have caused some licensees to lapse into reporting via e-mail, fax, telephone, or mail instead of the on-line method. However, there would be an increase in short-term costs with the implementation of any of the four options[5]. The start-up costs could include: Help Desk support; credentialing support; and workflow development of new kinds/types of credentials. There may be longer term costs avoided if users' credentialing application and authentication access burdens are simplified. Avoided costs could include: reduced need in processing data that is received via other alternate methods (i.e., e-mail, fax, telephone, or mail) due to greater user accessibility of the on-line method; more flexibility in computer credential compatibility as computer technology evolves (i.e., change to a new operating systems which is not compatible with the software certificate). Implementation of any of the options would not require that additional funds be requested by the staff.

[5]With respect to Option 1, the consideration of increased short-term costs are being considered with respect to transitioning users from smart cards to an alternative Level 4 authentication method, as described in the enclosure. There would be no additional resource impacts in maintaining the current smart card approach for users.

COORDINATION:

This action has been coordinated with the Office of the Chief Financial Officer. The Office of the General Counsel has reviewed this paper and has no legal objection.

/RA Michael Weber for/

R. W. Borchardt
Executive Director
for Operations

Enclosure:
Technological Differences Between
Level 4, Level 3, and Level 2

Technological Differences Between Level 4, Level 3, and Level 2

For a Level 4, the smart card form factor is the only current option offered by Authentication and Credentialing Services (ACS). Transitioning to an alternative Level 4 or to a Level 3 authentication technology would require ACS to be modified to include the new approach in order to support the National Source Tracking System (NSTS) user community. The National Institute of Standards and Technology (NIST) guidelines for Level 4 require the use of Public Key Infrastructure (PKI) that complies with Federal Bridge PKI policies, and a cryptographic hardware token that meets NIST standards.

Under the ACS service, following final identity proofing approval, the applicant is shipped a smart card and reader. Upon receiving the smart card and reader, the applicant must complete the following computer installations and configurations in order to prepare his/her computer for certificate collection (card activation) and subsequent usage of the smart card to access the NSTS:

- Install MyID Client Components – Used for the collection of certificates
- Install Card Reader Driver – Allows the computer to recognize the card reader
- Install Smart Card Middleware – Allows the computer to access and interpret the contents of the smart card
- Configure browser settings – Allows the collection of certificates

Each time a user attempts to access the NSTS, he/she must insert their smart card into the reader and must supply a PIN he/she created during the card activation step.

The process described above limits the number of security control alternatives at Level 4; however, the staff recently initiated research in determining the feasibility of an alternative Level 4 authentication assurance method, which does not employ use of a hard token, such as a smart card and reader, as currently employed for use of the NSTS.

A proposal was developed in which Multi-factor One-Time-Password (MF OTP) tokens can be combined with a Transport Layer Security (TLS) based mutual authentication protocol to meet the Level 4 authentication requirements. A MF OTP hardware token will display the user's OTP which will change every 60 seconds, and can only be used once to authenticate to the system, like the NSTS. After the OTP has been used it cannot be reused. The system, like the NSTS, could also lock out accounts per NIST and NRC guidance after a set number of login failures for a period that is compliant with NRC and NIST guidance. The authentication session will be negotiated using Hypertext Transfer Protocol Secure over TLS, with full mutual authentication on both ends. This will require the user to install client certificates to authenticate the session to the system.

Analysis of the requirements indicates that the proposed method meets the current NIST Special Publication (SP) 800-63, "Electronic Authentication Guideline," requirements for Level 4 authentication assurance. It also appears to be a method that NIST intended to support. In the most recent draft of NIST SP 800-63 (SP 800-63-1 dated December 2008), the publication explicitly states that this method is acceptable.

For a Level 3, browser-installed software certificates are currently the only option offered by ACS. This is similar to the process NRC employees' use for Citrix remote access. NIST guidelines allow for a wider range of technology options at Level 3 than at Level 4. However, if PKI is used, it must comply with Federal Bridge PKI policies, and if an OTP device is used it must be validated to NIST standards. Under the ACS-defined service, following final identity proofing approval, the applicant would be sent an e-mail with a link to the certificate collection website. Generating and installing the software certificate requires no special applicant computer access, computer knowledge, computer configuration, or computer privileges. The applicant would be expected to create a password to secure the use of the certificate. During the installation process, a first-time certificate user may be prompted to allow the automatic installation of:

- VeriSign Personal Trust Agent (VSPTA) Browser Plug-in – Used during generation and installation of certificates

Each time a user attempts to access the NSTS, he/she must supply the password that he/she created during the certificate installation step.

Due to certain security configurations that are becoming increasingly popular, it is possible that applicants would require one-time computer administrative privileges in order to successfully install the VSPTA Browser Plug-in.[1]

For a Level 2, similar to a MF OTP, a Single-factor (SF) OTP hardware token will display the user's OTP which will change every 60 seconds and can only be used once to authenticate to the system. The user will gain access to the NSTS by entering the user name and the generated SF OTP into the provided browser application to gain access.

[1]Such administrative privileges are not routinely available to the general user, meaning, even in this scenario there may have to be intervention by the user's local computer support group.