MEMORANDUM

To: Agency Chief Information Officers and Senior Agency Information Security Officers

From: Chair, Federal Public Key Infrastructure (PKI) Policy Authority (PA)

Subject: Reuse of PKI Compliance Audit Results in Federal IT Systems Security Reviews and Certification and Accreditation Reviews

Date: August 31, 2007

Background

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidance to Federal agencies on security controls that must be applied to their information systems in order to establish a security posture that is commensurate with the sensitivity of the data processed by the information systems. When a Certification and Accreditation (C&A) is conducted on a Federal agency IT system, the implementation of the required security controls are assessed in accordance with the criteria contained in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems.* NIST SP 800-53A defines the purpose of an assessment as *"...to determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system).*"

Draft NIST SP 800-53A dated April 21, 2006, encourages the use of security control assessments performed by outside sources in accordance with recognized criteria. The guidance encourages the use of previous assessments subject to conditions in Section 1.5, "REUSE OF ASSESSMENT RESULTS:"

> *The reuse of applicable security assessment results from previously accepted/approved assessments of the information system can also be considered in developing the necessary evidence for determining overall security control*

effectiveness. Applying previous assessment results to a current assessment requires a thorough analysis of the security controls and state of the information system to determine if any changes have occurred since the previous assessment and if the previous assessment results are applicable to the current assessment.

Economies are gained for the C&A process when the results of separate assessments are used in lieu of locally conducted test procedures.

PKI Audit Requirements and Security Assessments

Certification Authorities (CA) that are cross-certified with the Federal Public Key Infrastructure (FPKI) operate in accordance with certificate policies (CPs) that include a substantial number of IT system security requirements. During cross-certification, the Federal PKI Policy Authority (FPKI PA) performs a mapping process to establish equivalence between the applicant PKI's certificate policies and one or more of the Federal Bridge Certification Authority's (FBCA) certificate policies. Subsequently, cross-certified PKIs are required to conduct compliance audits to prove their systems meet and operate in accordance with the Policy(ies) associated with that PKI.

Trusted Third Party PKI services vendors that have been qualified as Shared Service Providers (SSPs) under the HSPD-12 program operate CAs in accordance with the Common Policy Framework CP. The Common Policy CP is tightly aligned with the FBCA CP and a mapping of these policies was performed such that certain levels of assurance in the Common Policy map to the Medium and above assurance levels in the FBCA CP. The SSP CAs are required by the Federal Common Policy to undergo annual compliance audits to demonstrate that their CA systems are operating in compliance with the Common Policy.

The compliance audit processes described above establish a basis for Federal agencies to trust each others' digital certificates, and for Federal agencies and cross-certified non-Federal PKIs to trust digital certificates issued by each others' PKIs at known and verified levels of assurance.

The PKI compliance audit process presents an opportunity for the reuse of security assessment results, since the required compliance audits assess PKIs to a level of detail that in most cases meets or exceeds the procedures and compliance requirements defined by NIST SP 800-53A. Further, to maintain certification of a CA, the FPKI PA requires compliance audits on the same frequency as required for the C&A of Federal IT systems: every three years; or whenever significant changes are made to the system. The depth and conditions for recurrence of compliance audits meet the criteria for the re-use of assessment results advocated by NIST SP 800-53A.

The FPKI Policy Authority, in consultation with NIST, has reviewed the security requirements imposed by the FBCA CP and compared them to the security controls defined in SP 800-53. Based on this review, the FPKI PA has determined that a successful compliance audit by a cross-certified PKI or an SSP CA verifies that a

significant subset of the SP 800-53 security controls are in place (additional controls may be in place to satisfy the entity CP). The precise set of security controls that must be in place depends upon the individual CP. An extensive table mapping these equivalences has been posted to the Federal PKI Policy Authority website at http://www.cio.gov/fpkipa/documents/CPto800-53MappingTables.doc

To avoid duplication of effort and to gain savings, agencies are encouraged to accept the results of Federal PKI (FPKI)-mandated compliance audits as partial assessment results for Certification and Accreditation of the entity CA system required under FISMA and as part of the triennial A-130 mandated Certification and Accreditation of IT systems. To complete the Certification and Accreditation process, agencies should use the results from the FPKI PA compliance audit and assess any additional security controls required for the specified system that are not covered by the mapped FBCA certificate policy.

For more information, please feel free to contact me at 301-252-8846 or altermap@mail.nih.gov.

Peter Alterman, Ph.D.