Audit Standards for Certified PKI Shared Service Providers:
An Analysis of Requirements and Alternatives

Federal PKI Policy Authority
Shared Service Provider Working Group

January 29th, 2007

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

This document represents a subject matter expert (SME) review and determination of a multi-part question considered by the Shared Service Provider Working Group (SSPWG). In this document the SSPWG considers the audit standards that will be mandated for a Certified PKI Shared Service Provider (SSP) candidate, including the compliance audit[1] standard and other requirements, processes, issues and standards such as the Federal requirements for Certification & Accreditation (C&A)[2].

The SSPWG acts under the authority of the Federal PKI Policy Authority, and interacts with the Federal PKI Certificate Policy Working Group. The SSPWG is charged with determining the selection criteria, requirements, processes and oversight provisions for selection of an SSP who will act on the government's behalf under the provisions of the Federal Common Policy[3], Certification Practice Statement (CPS), and a Registration Practice Statement (RPS)[4] that are subject to the approval of the Federal PKI Policy Authority. As such, the SSPWG is responsible for communicating the performance requirements for each SSP, both before and after selection. This includes the relevant capabilities, as well as the performance and audit standards each SSP will be subject to throughout the period of performance with a Contracting Federal Agency[5].

As a result of the subject matter expert determination, the SSPWG has formally reached the determination that both a compliance audit and C&A are required. Further, the SSP compliance audit shall be accomplished in accordance with WebTrust[6], or another standard considered acceptable by the Federal PKI Policy Authority. C&A shall be accomplished in accordance with NIST guidance.

It further recommends that the SSPWG work with the Office of Electronic Government within OMB and the CIO Council to provide funding[7] that addresses compliance audit and C&A requirements for SSP vendors. The balance of this document reviews the process, facts and analysis that culminate in the formal determinations documented in Section 8 – Conclusions and Recommendations.

---

[1] Compliance audits are identified in the IETF RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework in section 4.2.7, Compliance Audit.

[2] Certification and Accreditation is mandated under OMB A 130, Appendix III – Security of Federal Automated Information Resources. The provisions of OMB A-130 have subsequently been codified under various Federal laws, including the Federal Information Security Management Act of 2002.

[3] The Federal Common Policy is more formally known as the X.509 Certificate Policy for the Common Policy Framework.

[4] An RPS, for the purposes of this document, is considered to be the same as a Registration Authority Agreement, which is identified in various PKI references.

[5] A Contracting Federal Agency is any Federal government entity that contracts for services from a SSP, as approved by the SSPWG.

[6] WebTrust Program for Certification Authorities is an established compliance audit format, published by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

[7] Appropriate funding is provided for in the E-Government Act of 2002, as amended.

2.0 ANALYSIS OVERVIEW

This section provides an overview of the analysis. It identifies the authority, roles and responsibility of the SSPWG, and then identifies the purpose of the analysis.

2.1 Shared Service Provider Working Group

The SSPWG acts under the authority of the Federal PKI Policy Authority, and interacts with the Federal PKI Certificate Policy Working Group. The SSPWG is charged with determining the selection criteria, requirements, processes and oversight provisions for selection of an SSP who will act on the government's behalf under the provisions of the Federal Common Policy[8], Certification Practice Statement (CPS) and Registration Practice Statement (RPS)[9] that is subject to the approval of the Federal PKI Policy Authority. As such, the SSPWG is responsible for communicating the performance requirements for each SSP, both before and after selection. This includes the relevant capabilities as well as the performance and audit standards each SSP will be subject to throughout the period of performance with a Contracting Federal Agency[10].

2.2 Purpose

During the deliberations of the SSPWG, a multi-part question was posed concerning the degree to which Shared Service Providers are subject to:

- Federal requirements for Certification and Accreditation (C&A);
- What are the responsibilities related to C&A, if required;
- What are the alternatives related to C&A, if required;
- What is the relevance and requirement for a compliance audit;
- What standard should be adopted for compliance audits, if any, and;
- Does an SSP need to undergo both a compliance audit and C&A?

Based on the multi-part question, the SSPWG identified resources to create a formal analysis, which is represented in this document. The analysis takes into consideration

[8] The Federal Common Policy is more formally known as the X.509 Certificate Policy for the Common Policy Framework.
[9] An RPS, for the purposes of this document, is considered to be the same as a Registration Authority Agreement, which is identified in various PKI references.
[10] A Contracting Federal Agency is any Federal government entity that contracts for services from a SSP, as approved by the SSPWG.

Federal requirements, an analysis of audit standards[11], and a review of the emerging NIST Special Publication series documents that address C&A. The analysis also takes into account the Federal Common Policy, the provisions of a CPS and RPS, as well as other related documents that have a bearing on audit and oversight for each SSP.

[11] The SSPWG requires that a Shared Service Provider candidate must submit a compliance audit as a pre-condition for consideration.

3.0 TERMS AND REFERENCES

This section outlines the terms and references used for the purposes of the analysis in this document. This section is intended to contrast the differences in terms and references that form the basis for vernacular used in this analysis.

3.1 Terms

The term *compliance audit* is defined and contrasted against the two key terms used in Federal C&A, *security certification* and *security accreditation*. It is important to note that compliance audit is not derived from Federal mandates, and is not intended to achieve the same intent, per se, as the Federal C&A requirements.

- ***Compliance Audits –*** In the context of a public key infrastructure (PKI), compliance audits are defined in the Internet Engineering Task Force (IETF) RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.* Compliance audits concentrate on a determination of whether the PKI system is being operated in accordance with the published Certificate Policy (CP) and Certificate Practice Statement (CPS). There is a general presumption that the organization that operates the PKI system has reached determinations related to the nature of the system, including risk management and minimum standards and controls.

- ***Security accreditation*** – is the official management decision to authorize operation of an information system. This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, remaining after the implementation of an agreed upon set of security controls. By accrediting an information system, the agency official is not only responsible for the security of the system but is also accountable for adverse impacts to the agency if a breach of security occurs.

- ***Security certification*** – is the comprehensive evaluation of the management, operational, and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls.

3.2 References

While conducting the analysis for this document, a series of documents were considered. This includes references from the Federal government, industry, international organizations, and audit standards, which are categorized in each section below.

3.2.1 Federal References

There are a number of federal references related to this issue. The listing below identifies the federal references that were considered in the development of this document.

- E-Government Act of 2002 (Public Law 107-347)
- Federal Information Security Management Act of 2002, Title III, (Public Law 107-347)
- OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*
- United States General Accounting Office *Federal Information System Controls Audit Manual* (FISCAM)
- E-Authentication Policy for Federal Agencies (DRAFT)
- X.509 Certificate Policy for the Common Policy Framework (DRAFT)
- Federal Smart Card Policy (DRAFT)
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (DRAFT)
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- NIST Special Publication 800-26, *Security Self -Assessment Guide for Information Technology Systems*
- NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (DRAFT)
- NIST Special Publication 800-53, *Security Controls for Federal Information Systems* (DRAFT)
- NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems* (DRAFT)
- NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*

- NIST Special Publication 800-60, *Guide for Mapping Information and Information Types to Security Objectives and Risk Levels* (DRAFT)

3.2.2 International and Industry References

The following international and industry references were consulting during the analysis:

- International Standard, ISO/IEC 17799, *Code of Practice for Information Security Management*
- International Standard, ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation*
- Information Security Audit and Control Association, *Control Objectives for IT and Related Technologies* (COBIT)
- American Bar Association, *PKI Assessment Guidelines*
- AICPA/CICA, *WebTrust Program for Certification Authorities*

4.0 ROLES AND RESPONSIBILITIES

This section illuminates the roles and responsibilities that are assessed during a compliance audit and the roles and responsibilities that are intended under the pending C&A processes defined by NIST. The roles and responsibilities are different, reflecting the dissimilar basis for a compliance audit versus Federal C&A.

4.1 Compliance Audit Specific

There are three principal roles considered in this analysis[12] – the Policy Authority (PA), the Certification Authority (CA) and the Registration Authority (RA). An explanation of the roles and responsibilities, and the alternatives are presented in this section. The compliance audit assessor is required to review the roles and responsibilities to ensure that, in all regards, this is defined and assigned properly.

4.1.1 Policy Authority

The Policy Authority (PA) role is assigned to the Federal PKI Policy Authority, a group of U.S. Federal Government Agencies (including cabinet-level Departments) established pursuant to the Federal CIO Council. The Federal PKI Policy Authority is responsible for the maintenance of the Federal Common Policy, and approves the CPS and the RPS for each PKI system implemented under the Federal Common Policy. The PA is also responsible for the approval of the compliance audit report for each CA issuing certificates under the Federal Common Policy.

4.1.2 Certification Authority

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The CP, CPS and other appropriate documents define the role of the CA in more detail.

4.1.3 Registration Authority

The registration authority (RA) is the entity that collects and verifies each subscriber's identity and information that are to be entered into the subscriber's public key certificate. The CP, RPS and other appropriate documents define the role of the RA in more detail.

4.1.4 Functional Role Alternatives

Potential RA functions are a subset of CA functions. There are nine CA functions, of which five can be accomplished in whole or in part by the RA[13]. Assignment of these functional areas to an RA must be accomplished in writing.

[12] The roles and definitions are taken from the Federal Common Policy, and are consistent with generally accepted definitions, roles and responsibilities contained in authoritative references.
[13] The functional roles and alternatives are adopted from the American Bar Association PKI Assessment Guidelines. The assignment of functional roles is defined by the CP, CPS, or RPS documents.

Table 4-1: CA and RA Functional Role Alternatives

Functional Area	Certification Authority	Registration Authority
Key management functions, such as the generation of CA key pairs, the secure management of CA private keys, and the distribution of CA public keys	YES	NO
Establishing an environment and procedure for certificate applicants to submit their certificate applications (e.g., creating a web-based enrollment page)	YES	YES
The identification and authentication of individuals or entities applying for a certificate	YES	YES
The approval or rejection of certificate applications	YES	YES
The signing and issuance of certificates in a repository, where certificates are made available for potential relying parties	YES	NO
The publication of certificates in a repository, where certificates are made available for potential relying parties	YES	NO
The initiation of certificate revocations, either at the subscriber's request or upon the entity's own initiative	YES	YES
The revocation of certificates, including by such means as issuing and publishing Certificate Revocation Lists (CRL) or providing revocation information via Online Certificate Status Protocol (OCSP) or other online methods	YES	NO
The identification and authentication of individuals or entities submitting requests to renew certificates or seeking a new certificate following a re-keying process, and processes set forth above for certificates issues in response to approved renewal or re-keying requests	YES	YES

According to the ABA PKI Assessment Guidelines, assessors should read the PKI's policy and practice documents to see how the functions are identified and allocated among various entities. Assessors should determine if the relevant entities are identified and if their respective roles are clear. Assessors should also review agreements to determine if all functions are accounted for and if they clearly state the respective roles of the entities performing the functions.

4.2 C&A Specific

The roles and responsibilities listed in this section are adopted from the NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; however, only those roles that are relevant to the analysis are incorporated into this section. The key participants in the security certification and accreditation process are listed below.

Recognizing that agencies have widely varying missions and organizational structures, there may be differences in naming conventions for security certification and accreditation-related roles and how the associated responsibilities are allocated among agency personnel. At the discretion of senior agency officials, certain security certification and accreditation roles may be delegated. Agency officials may appoint appropriately qualified individuals, to include contractors, to perform the activities associated with a particular security certification and accreditation role. However, the signatory authority to authorize operation of a Federal information system cannot be delegated, and the authorizing official must be a Federal official.

4.2.1 Authorizing Official

The *authorizing official,* sometimes referred to as a designated approving or accrediting authority, is the senior management official or executive with the authority to approve the operation of the information system at an acceptable level of risk to agency operations, agency assets, or individuals. The role of this individual fulfills a specific requirement in OMB A-130.

4.2.2 Information System Owner

The *information system owner (system owner)* represents the interests of the user community throughout the life cycle of the information system. The information system owner is responsible for the development of the security plan and ensures the system is deployed and operated according to the security requirements documented in the plan. The system owner is also responsible for deciding who has access to the information system and ensures that system users and support personnel receive the requisite security training. The system owner informs key agency officials of the need to conduct a security certification and accreditation of the information system, ensures appropriate resources are available for the effort, and provides the necessary system-related documentation to the certification agent.

After taking appropriate steps to reduce or eliminate vulnerabilities, the system owner assembles the final security certification package with inputs from the certification agent, information system security officer, and other interested parties and submits the package to the authorizing official or the authorizing official's designated representative.

4.2.3 Information System Security Officer

The *information system security officer* is the principal staff advisor to the system owner on all matters (technical and otherwise) involving the security of the information system. The information system security officer typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many agencies, is assigned responsibility for the day-to-day security operations of the system. In close coordination with the information system owner, the information system security officer

often plays an active role in developing and updating the security plan for the information system as well as in managing and controlling changes to the system and assessing the security impact of those changes.

4.2.4 Certification Agent

The *certification agent* is the individual responsible for conducting the comprehensive evaluation of the management, operational, and technical security controls in the information system. The certification agent also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security test and evaluation activities, the certification agent provides an independent assessment of the security plan to ensure the plan provides a complete and consistent security specification for the information system.

To preserve the impartial and unbiased nature of the security certification, the certification agent should be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system. The certification agent should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification. The independence of the certification agent is an important factor in assessing the credibility of the security test and evaluation results and ensuring the authorizing official receives the most objective information possible in order to make an informed, risk-based security accreditation decision.

4.2.5 User Representative

The *user representative* represents the operational interests and mission needs of the user community within the agency and serves as the liaison for that community throughout the life cycle of the information system. The user representative assists in the security certification and accreditation process, when needed, to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls for the information system defined in the security plan.

5.0 ANALYSIS OF FEDERAL REQUIREMENTS

This section reviews various Federal requirements related to the work of the Subcommittee. This includes recent federal legislation, current OMB circulars, NIST publications, and the National Archives and Records Administration (NARA).

5.1 E-Government Act of 2002

In support of the President's Management Agenda (PMA), Congress passed into law the E-Government Act of 2002. The E-Government Act of 2002 provisions are relevant to this analysis in two separate areas: (1) legislative language that provides direction and funding to support Federal agency efforts, such as establishing a PKI common trust anchor, as provided for by the Federal Common Policy, and (2) the provisions of FISMA which are addressed in section 5.2 below.

The Act identifies specific actions, responsibilities, and funding intended for the government to improve service to citizens, and improve internal efficiency within the government. The Act specifically directs and funds certain PKI related activities, including the Federal Bridge Certification Authority, and directs the government to identify innovations that merit funding[14]. This includes enabling Federal agencies to take advantage of information technology in sharing information and conducting transactions with each other and with State and local governments.

Section 3604 of the Act provides for the E-Government Fund, which is overseen by the General Services Administration, assisted by the Administrator of the Office of Electronic Government. The criteria identified in the Act can be applied by the Federal government to this issue. In particular, to the benefit of every participating agency, the E-Government fund can be used to accomplish either compliance audits or C&A, and the results of the compliance audit and C&A can be utilized by the Federal PKI Policy Authority, FICC, and each Contracting Federal Agency to consolidate costs.

5.2 FISMA

The Federal requirements for C&A are derived from OMB A-130, Appendix III – *Security of Federal Automated Information Resources*. This was substantially codified in the E-Government Act (Public Law 107-347), Title III – *Federal Information Security Management Act of 2002* (FISMA). Under the FISMA statutes, the following federal requirements must be met[15]:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or

[14] The Act provides clear evaluation criteria used to determine eligibility for funding under the Act. An analysis of the criteria supports a conclusion that the SSPWG can request funding for compliance audits and C&A of Shared Service Providers.
[15] The text provided is contained in NIST Special Publication 800.37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (DRAFT).

destruction of information and information systems that support the operations and assets of the agency;

- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;

- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;

- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;

- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;

- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices, of the agency;

- Procedures for detecting, reporting, and responding to security incidents; and

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

5.3 OMB Circular A 130

The Federal requirements for C&A are derived from OMB A-130, Appendix III – *Security of Federal Automated Information Resources*. This requires executive agencies within the federal government to:

- Plan for security;

- Ensure that appropriate officials are assigned security responsibility;

- Periodically review the security controls in their information systems; and

- Authorize system processing prior to operations and, periodically, thereafter.

Systems must be reassessed every three years, as a minimum; however, system owners may determine a more frequent schedule. Also, systems must be re-evaluated under certain conditions, such as a new system interconnection, a change in the risk exposure to the

system, or a security event, as examples. Compliance audits, in contrast, are generally conducted annually and do not have provisions that would require an aperiodic review[16].

5.4 NIST Guidance

As mandated in various federal information security laws, including FISMA, NIST is required to provide standards and guidance for government agencies in the area of information security. Recently, NIST has taken substantial steps to enhance the guidance related to C&A. This includes identification of criteria, process and methodology for areas considered during formal C&A of a federal information system. Most of the documents are currently in public draft[17], and include:

- NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (DRAFT)
- NIST Special Publication 800-53, Security Controls for Federal Information Systems (DRAFT)
- NIST Special Publication 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems (DRAFT)
- NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk Levels (DRAFT)
- NIST Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (DRAFT)

Security accreditation is the official management decision to authorize operation of an information system. This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, remaining after the implementation of an agreed upon set of security controls. By accrediting an information system, the agency official is not only responsible for the security of the system but is also accountable for adverse impacts to the agency if a breach of security occurs. Security accreditation, which is required under OMB Circular A-130, provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical constraints, operational constraints, cost and schedule constraints, and mission requirements.

[16] Aperiodic reviews are conducted outside of the schedule. The Federal Common Policy identifies that the Federal PKI Policy Authority may elect to have an aperiodic compliance audit conducted at any time.
[17] NIST Federal Information Processing Standard (FIPS) 102, *Guidelines for Computer Security Certification and Accreditation*, dated September 1983, is not considered in this analysis. This FIPS publication is expected to be revoked when the new Special Publication documents are finalized.

The assessment of risk and the development of security plans are two important activities in an agency's information security program that directly support the security accreditation process and are required under FISMA and OMB Circular A-130. Risk assessments, whether done formally or informally, influence the development of the security requirements and the security controls for information systems and generate much of the information needed for the associated security plans for those systems. Security plans document the security requirements and security controls for information systems and provide essential information for security accreditations. Security plans typically include as references or attachments, other important security-related documents (e.g., contingency plans, configuration management plans, risk assessments, information system interconnection agreements) that are produced as part of an agency information security program.

In addition to risk assessments and security plans, security evaluation also plays an important role in the security accreditation process. It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make credible, risk-based decisions on whether to authorize operation of those systems. This information and supporting evidence for system authorization is often developed during a detailed security review of the information system, typically referred to as *security certification*. Security certification is the comprehensive evaluation of the management, operational, and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls.

The results of the security certification are used to reassess the risks and update the security plan for the information system—thus, providing the factual basis for the authorizing official to render the security accreditation decision. By accrediting the information system, the agency official accepts the risk associated with it and the implications on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Formalization of the security accreditation process ensures that information systems will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically and whenever there is a significant change to the system or its environment. Security certification and accreditation of agency information systems support the legislative requirements of FISMA by ensuring that agencies periodically: (i) assess the risk resulting from the operation of those systems; (ii) test and evaluate the security controls in those systems to determine control effectiveness and system vulnerabilities; and (iii) assess the information security programs supporting those systems (e.g., security awareness and training, incident response, and contingency planning).

5.5 NARA Guidance

On March 14, 2003, the National Archives and Records Administration (NARA) finalized guidance related to the application of PKI technology within the Federal government. Entitled *Records Management Guidance for PKI-Unique Administrative*

Records, this document was produced for the CIO Council and the records management community.

The target audience for this guidance includes federal agency information technology, records management and operations personnel responsible for planning, implementing, operating or otherwise documenting and managing records produced by PKI administrative activities. Other entities, such as state and local government agencies, as well as commercial entities interacting with government agencies may find this guidance document useful and may adopt and or modify it to suit their specific needs. However, a compliance audit would generally overlook this reference.

6.0 COMPLIANCE AUDIT ANALYSIS

This section reviews the various requirements for a compliance audit, including the sources that establish compliance audit criteria. The sources include standards bodies such as the Internet Engineering Task Force (IETF), as well as, Federal requirements.

6.1 Compliance Audit Origin

The provisions for a compliance audit are originally derived from the IETF RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* in section 4.2.7, Compliance Audit. There are no Federal requirements[18] for a compliance audit, aside from those derived by business requirements through Relying Party agreements, or similar considerations. The business and legal community has taken action to further define compliance audit standards to take full advantage of the integrity and assurance value offered. A compliance audit indicates that the Certification Authority (CA) has undergone an independent review[19]. A compliance audit may identify deficiencies that require remediation. The areas identified for consideration in a compliance audit include:

- Frequency of compliance audit for each entity;
- Identity/qualifications of the auditor;
- Auditor's relationship to the entity being audited;
- List of topics covered under the compliance audit: sample check on the various I&A policies, comprehensive checks on key management policies, comprehensive checks on system security controls, comprehensive checks on operations policy, and comprehensive checks on certificate profiles;
- Actions taken as a result of a deficiency found during compliance audit, the examples include:, temporary suspension of operations until deficiencies are corrected, revocation of entity certificate, change in personnel, invocation of liability policy, more frequent compliance audit, etc.;
- Compliance audit results: who they are shared with (e.g., subject CA, RA, and/or end entities), who provides them (e.g., entity being audited or auditor), how they are communicated.

Compliance audits are principally focused on whether the Certification Authority is operating in a manner that is consistent with the CP, the CPS, and other related

[18] The Federal Common Policy requires a compliance audit in section 2.7; however, this provision in the Federal Common Policy is not derived from a Federal requirement, but rather from the general outline and structure provisions of IETF RFC 2527.

[19] A compliance audit is generally contracted for by the Certification Authority, and as such does not meet the definition of independence, as considered by the Federal government in OMB A-130, Appendix III - Security of Federal Automated Information Resources.

documents. As a result, compliance audits do not focus on risk management, or whether the system controls are appropriate, or whether the controls meet specific industry or Federal requirements.

6.2 WebTrust Program for Certification Authorities

WebTrust was developed by the AICPA and CICA[20] to address the security assurance and compliance issues of the e-commerce business community. The WebTrust compliance audit process results in a WebTrust Seal that may be used by the organization as a method of conferring confidence to a potential customer or business partner. The WebTrust audit periods are generally annual; however audits may be scheduled more frequently. The references used in the development of the WebTrust standard are contained in Appendix A – WebTrust Reference Documents.

The WebTrust process is generally commissioned by the candidate Shared Service Provider, and therefore does not set the level of independence required by the Federal government; however, the Federal PKI Policy Authority may contract for and compensate the WebTrust compliance audit firm to achieve an independent audit.

At the time an SSP candidate is applying for consideration, it is important to note that any existing WebTrust compliance audit is predicated on the then current nature of the SSP candidate. The nature of the Federal Common Policy SSP roles and duties may be different, and this may create different compliance audit outcomes. Therefore, a revised compliance audit should be considered shortly after a SSP is approved and initiates services for a Contracting Federal Agency.

6.3 SAS 70 Audit Standard

There are separate professional standards for auditors to report on controls for third-party service providers (a service auditor's engagement). The SSPWG considered the relevance of SAS 70, both Type 1 and Type 2 audits, to the review of a SSP candidate. A SAS 70 audit may be required in the financial community by a business partner.

The guidance for these engagements is set out in the AICPA's Statement on Auditing Standard (SAS) No. 70, Service Organizations (AICPA, Professional Standards, vol. 1, AU sec. 324), as amended. However, AICPA identifies that SAS 70 audits are not intended for the review of PKI Certification Authority engagements, and the more appropriate standard is the WebTrust Program for Certification Authorities. The differences between WebTrust and SAS 70 are contained in Appendix E of the WebTrust Program for Certification Authorities document.

[20] The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accounts (CICA) jointly developed the WebTrust standard.

6.4 ISO 17799 Audit Standard

Formally entitled International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, this standard is a broad based best practices standard derived from BS 7799[21], a standard developed by the British government to address information security management.

ISO 17799 is not normally considered to be a compliance audit standard, and is not tailored to auditing PKI Certification Authorities. The Federal government does not support the use of ISO 17799 as a mandatory standards reference[22].

6.5 COBIT

Control Objectives for IT and Related Technologies (COBIT) is published by the Information Security Audit and Control Association (www.isaca.org), and forms the basis for various audit standards. For example, the GAO publication *Federal Information System Controls Audit Manual* (FISCAM) is principally derived from COBIT, and a number for public and private sector audit programs utilize the COBIT approach. However, COBIT is not specifically tailored for PKI assessments or audits.

6.6 Professional Compliance Audit Firm Standards

The analysis considered that certain independent, commercial entities may offer professional audit services that include PKI compliance audit standards, methodologies and approaches that are not represented in the this section. The Federal PKI Policy Authority may find, upon evaluation, that such compliance audit standards may be acceptable; however, such professional audit service standards were not reviewed.

Principally, such audit standards are generally not available[23] and an analysis cannot reasonably conclude that a reference being reviewed is current, or that it represents the current audit approach for an independent firm. Additionally, it would not be reasonable to draw a broad conclusion about professional compliance audit firms and their suitability based on a limited review of select professional audit firms.

[21] ISO 17799 incorporates Part 1 of BS 7799, but Part 2 of BS 7799 has not been adopted by ISO.
[22] The United States government, represented by NIST, has taken the formal position that ISO 17799 does not provide detailed conformance specifications necessary for an organizational information security management program. It does not provide enough information to support an in-depth organizational information security review, or to support a certification program like the ISO 9000 process quality certification program. (csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf)
[23] Professional compliance audit firms may regard internally developed standards as intellectual property, or documents that may have competitive value. As such, release of the audit standard is controlled.

6.7 Recommended Compliance Audit Standard

Based on industry standards and acceptance, the WebTrust Program for Certification Authorities should be considered, as well as other standards that are independently reviewed and accepted by the Federal PKI Policy Authority. Most, if not all SSP candidates[24] will already have a compliance audit, and submission of a compliance audit should be a pre-condition for consideration of a SSP candidate. The audit standard used should be specifically intended to assess a PKI system.

[24] The SSPWG takes into consideration that Federal agencies may elect to provide SSP services to other Federal agencies, but may not have elected to have an independent compliance audit conducted. This analysis does not attempt to make a recommendation in this area, and the SSPWG will have to determine the policy, requirements and processes in such cases.

7.0 WEBTRUST VERSUS FEDERAL CRITERIA

This section considers to what degree a compliance audit, based on WebTrust, addresses all of the Federal C&A criteria stipulated in laws and policy. The intent of this section is to facilitate analysis of whether a compliance audit can be used in lieu of C&A.

7.1 OMB A-130 Analysis

OMB Circular A-130, Appendix III – *Security of Federal Automated Information Resources* is published by The Office of Management and Budget, part of the Executive Office of the President. This circular has been progressively codified in federal laws, including under the provisions of FISMA. For the purposes of this assessment, it is assumed that a PKI solution would be construed as a General Support System (GSS)[25]. This circular requires the following, which should be considered relevant to this analysis:

- Under the General Support Systems section, the "system owner" shall have an independent review conducted of the System Security Plan. The System Security Plan will not exist at the time the candidate Shared Service Provider is under consideration. However, a System Security Plan will be required in order to complete the C&A process.

  A compliance audit presented by a Shared Service Provider will, generally, not consider the intent of OMB A-130, and the degree to which it is truly independent is not clear. In most scenarios, the compliance audit is conducted at the direction of the Shared Service Provider, who also provides the compensation to the compliance audit entity. As such, the compliance audit is not intended to consider federal requirements, and it not conducted at the direction of the "system owner."

- The "system owner" must reach a determination of whether adequate security exists, defined as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.

  The auditor, under WebTrust, is not required to consider the risk analysis, and can not reach such a determination prior to selection. For instance, the intended Registration Authority processes and controls may not exist at the time of a compliance audit. In a post implementation audit, the auditor may be required to consider risk and mitigation of risk; however, this would be supplemental to the normal audit criteria.

- The auditor will not be able to conduct a review of security training or personnel controls, as it applies to the Federal agency contracting services. As it pertains to

[25] OMB A-130 defines two types of systems. Major Applications (MA) and General Support Systems (GSS). A Major Application is principally a data management solution, where a General Support System is technology based, such as infrastructure solutions.

training, OMB A-130 specifically incorporates contractors as entities that must comply with the training requirement. Post implementation, this can be taken into consideration.

- The auditor will not be able to assess the provisions of the *Incident Response Capability* section, as such provisions will not exist, and therefore the processes and controls cannot be properly determined. As part of the C&A process, this must be incorporated into the analysis by the Certification Agent.

- The *Continuity of Support* section cannot be properly assessed, and the modern considerations for government continuity of operations are not part of the WebTrust audit criteria. Federal systems have continuity of operation (COOP) risk factors that a compliance audit would not normally consider.

- The *Technical Security* considerations are not uniform between NIST publications and WebTrust, or other potential audit standards. As NIST publications are incrementally released, there are no provisions under compliance audit standards to consult and update the considerations contained in NIST publications.

- *System Interconnection* cannot be properly assessed because, in most cases, the system interconnections do not exist. For example, connectivity to an authoritative data source used to populate digital certificate fields will not be present, and new system interconnects require re-assessment by the system owner. Post selection, this would have to be reviewed by the Certification Agent.

7.2 FISMA Analysis

As mandated under the E-Government Act of 2002, Title III - Federal Information Security Management Act of 2002 (FISMA), there are several provisions that may not be assessed through the WebTrust or similar audit process. A representation for analysis is incorporated into NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, currently in the second public draft. Topical areas of consideration include:

- Roles and responsibilities (section 2.2), which will not be assessed against federal standards, nor will those roles technically exist prior to consideration of a candidate Shared Service Provider. For instance, there is no Authorizing Official, Authorizing Official Designated Representative, Information System Owner, Information System Security Officer, Certification Agent, or User Representative.

- A compliance audit may be considered by the "system owner" but this does not address the requirements identified under Section 2.6 – Security Accreditation Decisions.

- Section 2.7 – Supporting Documentation identifies the information and processes that must exist, as well as a risk management processes outlined in NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*

or the analysis required in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* and in NIST Special Publication 800-53, *Security Controls for Federal Information Systems*. These will not exist as part of an existing compliance audit, and is not required to be considered in any post implementation analysis processes.

7.3 NIST Publications

The WebTrust process does not conduct assessments related to compliance with FIPS[26] or Special Publication series documents published by NIST. It does not imply compliance with relevant PKI technical standards and guidance used by the Federal government, such as NIST Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, or NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*. Federal agencies have contingency planning considerations that most PKI compliance audits would not normally consider.

7.4 Common Criteria

The United States government is a participant in Common Criteria, and generally holds that Common Criteria affords the government with a framework to evaluate information technology solutions. The Federal government expects that the use of Common Criteria certified products and the associated Protection Profiles can reduce the amount of effort expended in evaluating a system, and can reduce the cost associated with risk mitigation.

The compliance audit process does not take into account Common Criteria, and the selection of components is generally not a consideration by the compliance auditor.

7.5 Federal Common Policy

The Federal Common Policy, more formally known as the X.509 Certificate Policy for the Common Policy Framework was reviewed[27]. This document specifically requires an annual compliance audit. However, a specific compliance audit standard is not identified, nor do Certificate Policy documents normally specify a specific audit standard.

Consideration for C&A is not addressed in the Federal Common Policy, and is not required to be identified. This does not negate the requirement found in other references.

7.6 Analysis of Auditor Qualifications

The Federal Common Policy does identify expectations of competency for the compliance auditor, and requires the compliance auditor to be an independent private firm. The Federal PKI Policy Authority is responsible for approving a compliance auditor, and all aspects of a PKI solution are subject to compliance audit inspections.

[26] WebTrust does incorporate consideration of FIPS 140; however, this is the sole FIPS document cited.
[27] The Federal Common Policy reviewed was in "Final Draft" form, and dated December 10th, 2003.

Recently the Federal PKI Policy Authority adopted a new competency standard as referenced in Federal Bridge CA Certificate Policy Change Proposal Change Number 2003-05, and adopted by the Federal PKI Certificate Policy Working Group. The change stipulates that *the auditor must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.*

8.0 CONCLUSIONS AND RECOMMENDATIONS

As identified in section 2.0, Analysis Overview, the multi-part question posed by the Subcommittee concerned the degree to which Shared Service Providers are subject to:

- Federal requirements for Certification and Accreditation (C&A);
- What are the responsibilities related to C&A, if required;
- What are the alternatives related to C&A, if required;
- What is the relevance and requirement for a compliance audit;
- What standard should be adopted for compliance audits, if any, and;
- Does an SSP need to undergo both a compliance audit and C&A?

The following conclusions and recommendations provided in this section address these questions, and provide additional guidance that extends the original multi-part question.

8.1 Conclusions

Based on the requirements, facts, processes and objectives considered by the SSPWG, the following conclusions are adopted in the analysis:

- The structure of roles and responsibilities under the Federal Common Policy is highly unusual, and as such compliance auditors and Certification Agents will require guidance from the Federal PKI Policy Authority and the Contracting Federal Agency. While it is not unusual to have the CA and RA functions separated in a managed service contract, the additional separation of the Policy Authority function will create oversight and control questions.
- The objectives of a compliance audit do not address the requirements of C&A identified by the Federal government.
- There are potentially different compliance audit standards, and approaches. This may create challenges when assessing a SSP candidate.
- The objectives of a compliance audit have a more specification orientation towards evaluation of PKI systems, and therefore offers value to the "system owner," and as such, the Federal government. Further, a compliance audit is required by the Federal Common Policy.
- A Relying Party may require a compliance audit as part of a due diligence review, and therefore this offers value to the government. This is particularly applicable

to Contracting Federal Agencies that have Relying Party agreements in the healthcare and financial sectors.

- Compliance audit standards do not establish minimum criteria for personnel conducting compliance audits, which is not desirable, and inconsistent with recent determinations by the Federal Bridge Certification Authority (FBCA) and the Federal Common Policy.

- Compliance audits are conducted annually, as a minimum. Federal C&A requirements mandate re-assessment at least once every three years, although more frequent assessments may be required by the "system owner."

- The "system owner" should make specific determinations related to control and release of specific audit documents, in particular C&A documents. As an example, Security Test and Evaluation reports that include penetration test results may not be appropriate for release, and may be withheld from the personnel performing the compliance audit if deemed necessary by the system owner.

- Contracting Federal Agencies have information and business process management obligations that may be defined by agency specific legislation, which must be taken into consideration.

- The Federal PKI Policy Authority is the "system owner" for the root CA implemented by the Federal government. As such, compliance audits and C&A are the responsibility of the Federal PKI Policy Authority for this CA. However, the subordinate PKI implementations have different "system owners" who must ensure that compliance audits, C&A and controls are conducted in accordance with the legal mandates that govern each agency[28].

- The C&A processes do not take into account defined roles and responsibilities in a PKI system, which are essential to proper assessment. Most Federal agency C&A contractors do not have expertise in this area.

- Compliance audits and C&A have similar evaluation areas, which creates the opportunity to consolidate effort. However, the evaluation criteria for such areas have significant differences.

- The Federal PKI Policy Authority does not have the authority to waive the requirement for C&A, and a GAO audit of a system would result in a challenge to the Contracting Federal Agency.

[28] In accordance with the Federal Common Policy, the Federal PKI Policy Authority may at any time suspend or revoke the CA or RA authorization if an agency is found to be non-compliant, and the Policy Authority deems this to be the most appropriate action.

- Combined compliance audit and C&A activities could be combined; however, this would require participation and representation by the various parties.

- The Federal Common Policy specifically addresses user certificates. Agencies will require device certificates, and may elect to contract for these through the same SSP vendor. This will require a separate CP, CPS and related documents. A separate determination of audit requirements will be required on the part of the Contracting Federal Agency[29], as negotiated with the SSP vendor. This will also create questions by the compliance auditor and the Certification Agent.

- The Federal PKI Policy Authority is charged with review and acceptance of a compliance audit, as stipulated in the Federal Common Policy. However, the *information system owner* is responsible for submitting a system to an agency *authorizing official*, as required by OMB A-130. This creates a distinct difference in required approval processes. Therefore, Contracting Federal Agencies operating under the Federal Common Policy will require approval by both the Federal PKI Policy Authority and the agency *authorizing official* in order to operate.

8.2 Recommendations

Based on an analysis of the references, facts and requirements, the following recommendations are adopted:

- The Federal PKI Policy Authority should require each SSP to have and maintain compliance audits. This is already provided or in the Federal Common Policy. The compliance audits conducted on a SSP vendor should be contracted for by the Federal PKI Policy Authority, and not by the SSP vendor operating the CA. This is intended to ensure the independence of the compliance auditor.

- The Federal PKI Policy Authority should standardize on a specific compliance audit standard that creates uniform expectations, and enhances the ability to assess the SSP vendor community in a uniform manner. If necessary, this should be developed to ensure consistency.

- Each SSP candidate should be required to submit a current compliance audit and a proposed CPS as a pre-condition for consideration by the SSPWG.

- The Federal PKI Policy Authority should evaluate and approve independent entities that have the expertise to conduct both compliance audits and act as Certification Agents. ***Compliance audits and C&A should be combined, where possible.***

- The SSPWG should require each SSP candidate who has successfully completed the Operational Capabilities Demonstration (OCD) to undergo a compliance audit

[29] This assumes that the Contracting Federal Agency is also the Policy Authority in this scenario.

and C&A, which the SSPWG should pay for through the use of E-Government Act funds. The C&A should be conducted once, on behalf of all Contracting Government Agencies.

- A single certification process[30] for a SSP vendor will control costs, reduce timelines, but will need to be supplemented. As a new Contracting Federal Agency engages a SSP vendor, there will be areas that will require supplemental analysis. In particular, the RA function will require a compliance and C&A analysis. However, this is substantially more cost effective than conducting both a comprehensive compliance audit and C&A separately for each agency, where no benefit to the government can be discerned.

- If the alternative identified immediately above is not chosen, each Contracting Federal Agency is responsible for conducting a compliance audit and C&A separately.

- Professional standards for auditors recommend that all prior audit reports should be reviewed while conducting any new audits. The compliance auditors and the Certification Agent should avail themselves of all audit reports, both compliance audits and C&A, to the extent permitted by the "system owner."

- The Federal PKI Policy Authority should establish timelines for compliance audits, and C&A, and maintain a schedule that tracks audit and C&A time tables for the various agencies. This includes a determination of how soon a compliance audit and C&A is required after the Federal PKI Policy Authority approves commencement of services.

[30] C&A considers different approaches, which include facility based approaches, system based approaches, and type certifications.

Appendix A – WebTrust Reference Documents

The following documents and references are cited in the WebTrust Program for Certification Authorities document. The references represent a broad spectrum of audit related documents, but are not necessarily representative of Federal audit standards.

1. Suitable Trust Services Criteria and Illustrations for Certification Authorities www.aicpa.org/download/trust_services/final-Trust-Services.pdf

2. ANSI X9.79 PKI Practices and Policy Framework, including the provisions of Annex B (Normative) Certification Authority Control Objectives. The references used to form the listing of Control Objectives includes:
    a. IETF RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
    b. IETF RFC 2560, Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
    c. British Standard BS 7799, Information Security Management
    d. ISO 9594, Information Technology – Open Systems Interconnection – The Directory
    e. ISO 10202, Financial Transaction Cards – Security architecture of financial transaction systems using integrated circuit cards
    f. ISO 11568, Banking – Key Management (retail)
    g. ISO 13491, Banking – Secure cryptographic devices (retail)
    h. ISO 15782, Certificate management for financial services
    i. ANSI X9.30, Digital Signatures
    j. ANSI X9.31, Certificate Management for RSA
    k. ANSI X9.57, Public Key Cryptography for the Financial Services Industry: Certificate Management
    l. ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)
    m. ANSI X9.80, Prime Number Generation, Primality Testing, and Primality Certificates
    n. FIPS 140-1, Security Requirements for Cryptographic Modules

3. The ABA PKI Assessment Guidelines – The American Bar Association Information Security Committee (ABA-ISC) PKI Assessment Guidelines (PAG), which addresses the legal and technical requirements for certification authorities. The PAG makes reference to the Certification Authority Control Objectives that are detailed in the ANSI X9.79 (PKI Practices and Policy Framework) standard and reflected in the WebTrust Principles and Criteria for Certification Authorities.

The WebTrust process does not incorporate the Information Systems Audit and Control Association (www.isaca.org) control objectives contained in the Control Objectives for

Information and Related Technology (COBIT), as overseen by the IT Governance Institute (www.itgi.org). COBIT is the principal reference used by GAO in the Federal Information System Controls Audit Manual (FISCAM).