Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS Security Whitepapers:

Introduction to CMS Security Whitepapers

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *INTRODUCTION TO CMS SECURITY WHITEPAPERS*, VERSION 2.0

1) Changed Baseline Version with updated CMS style format.
2) Section 1: Changed guidelines to whitepapers.
3) Section 2: Changed guidelines to whitepapers.
    a) Updated the FISCAM reference information.
    b) Changed the date of the NIST SP 800-53 to reflect the current version.
    c) Changed the requirements list from the BPSSM to the CMSRs.
4) Section 3.1: Changed the comparison of the FISCAM and NIST SP 800-53 to the comparison of the controls in the FISCAM and the security requirements of the CMSRs.
5) Section 3.3: Removed the reference to the CAST as it is no longer used.
6) Section 5: Updated the references and reference dates.

SUMMARY OF CHANGES IN INTRODUCTION TO CMS SECURITY WHITEPAPERS, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

This document provides introductory comments for a series of whitepapers issued by the Centers for Medicare and Medicaid Services (CMS) to assist with the proper understanding and implementation of key security requirements around CMS' data and information systems environment. The whitepapers issued consist of many topics which help the business partners with mandatory audits. Here are some of those issued in the following list:

- Logical access controls and segregation of duties
- Development and implementation of an entity-wide security plan
- Application programmers' access to application data and source code and application programmer segregation of duties
- Change management procedures and requirements for maintaining change management documentation
- Testing process for the SANS Top 20 Security Weaknesses
- Implementation of security configuration templates

The intended audience of these guidelines however, extends beyond CMS management and staff to include all CMS business partners. In this context, a CMS business partner is any private or public sector organization which provides services CMS. These business partners include, but are not limited to; Medicare carriers, fiscal intermediaries, Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, claims processing data centers, Medicare Administrative Contractors (MAC), and Enterprise Data Centers (EDC).

Today's highly technology-dependent organization, while benefiting from the increased capabilities offered by continued improvements in Information Technology (IT), is also faced with the challenge of maintaining sufficient security requirements around the increased complexities of new developments in IT. The primary objectives of these security requirements are to maintain confidentiality, integrity, and availability around information critical to the organization's mission.

These whitepapers will provide CMS management and business partners with the information required to ensure that key federal government security requirements pertaining to each of the topics are fully incorporated into CMS' current security management environment.

2 COMPLIANCE CRITERIA

The IT security requirements discussed in the whitepapers are part of the foundation of operating in a secure environment promoting effective security requirements for data confidentiality, integrity, and availability. The importance of these security requirements is evidenced by the direct inclusion or indirect references to these CMS security requirements in numerous federal government Acts, standards, and guidelines, including, but not limited to, the following:

- Chief Financial Officers Act of 1990
- Federal Financial Management Improvement Act (FFMIA) of 1996
- Federal Manager's Financial Integrity Act of 1982
- Federal Information Security Management Act of 2002 (FISMA)
- Various OMB circulars including OMB A-127 (Financial Management Systems) and OMB A-130 (Security of Federal Automated Information Resources)
- Various NIST Special Publications in the 800-series reports, and
- GAO/GAO-08-1029G, *Federal Information System Controls Audit Manual (FISCAM) Exposure Draft*

The whitepapers focus on the identification and description of controls pertaining to each of the security requirement areas as recommended by FISCAM and FISMA (and other federal government or industry standards, as required). Note that CMS has a list of IT security requirements which link to documented controls while other government agencies, such as GAO in the FISCAM, may refer to the audit criteria as the controls. Listed below is a brief discussion of the compliance framework for FISCAM and FISMA:

- A key goal of the Chief Financial Officers Act of 1990 was the development of a consistent approach to financial statement audits of federal government agencies. General Accounting Office' (GAO) Financial Audit Manual (FAM) provides detailed guidance on the performance of financial statement audits. In July of 2008, GAO issued the update to the Federal Information Systems Controls Audit Manual (FISCAM) as a companion to FAM. FISCAM provides the methodology for IT audits review within the framework of a financial statement audit of federal government agencies.
- In December 2007, NIST published Special Publication (SP) 800-53, with updates, to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002. According to the OMB memorandum titled "Memorandum for Heads of Executive Departments and Agencies", dated June 13, 2005, the approach documented in NIST SP 800-53 is to be used by agencies to conduct self assessments in compliance with FISMA. For the purposes of this whitepaper we follow the most recent version of the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSRs) and the latest guidance on FISMA compliance. Note: The CMSRs are the security requirements listed in the appendices of the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements.*

The areas discussed in the whitepapers have manifested themselves within the management practices of CMS through the inclusion of a number of security requirements related to these areas in the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*. CMS has used OMB circulars, NIST Special Publication 800-series reports, and other federal and industry guidelines to compile the IT management practices documented in the CMSRs. As such the content of the CMSRs are not to be viewed as “guidance’. They are, rather, “requirements” for all CMS business partners.

3 ORGANIZATIONAL APPROACH TO CONTROLS IMPLEMENTATION

3.1 YEAR-ROUND CYCLICAL APPROACH

Security requirements which are enforced through a periodic assessment against a static checklist will inevitably fail. Both the operations environment and the IT environment which supports it are fluid as are the security requirements to ensure data confidentiality, integrity, and availability. As such, the implementation of any CMSR at CMS can only be effective if it is an integral part of the management process. This means incorporation of security requirements in the year-round enterprise-wide management lifecycle of the organization.

FISCAM and the CMSRS have each defined specific roles and responsibilities and an approach to planning and management of effective IT systems security. Within sections two (2) and three (3) of the BPSSM, CMS has also documented detailed descriptions of system security roles and responsibilities and an approach to managing IT systems security.

CMS management is committed to ensuring that:

- Sections two (2) and three (3) of the BPSSM are continually evaluated against the IT security management approach and roles and responsibilities listed in the FISCAM. CMS continually assesses the CMSRs to facilitate full compliance; and
- The BPSSM is continually evaluated for compliance with guidance in FISCAM and the CMSRs regarding specific systems to be covered by the security management program.

Table 1 maps the key components of the IT security management approach recommended by FISCAM to those required by the CMSRs, and those applicable discussion sections of the BPSSM.

3.1 MANAGEMENT INVOLVEMENT

As mentioned in the prior section, effective implementation of IT security requirements can only be achieved if it is incorporated in the year-round enterprise-wide management lifecycle at the highest levels of an organization. This requires direct involvement, not only by the IT management structure (e.g., Chief Technology Officer and Chief Information Security Officer) but also by executives at the enterprise-wide level (e.g., program managers and agency leadership). This requirement is not only reflected in the compliance criteria used for the guidelines (e.g., the reporting requirements for FISMA) but also in other IT-related government publications and standards (e.g., the revised OMB Circular A-123, effective FY 2006).

Table 1 Mapping of IT Security Program Management Principles

FISCAM	CMSRs	BPSSM (includes Chapter #)
Assess Risks & Determine Needs	Periodic risk assessments	3.10 Management Security Resources 3.2 Risk Assessment
Implement Policies and Controls	System security plans Policies and procedures based (on the risk assessments) and subordinate plans for providing adequate system security Plans and Procedures to Ensure Continuity of Operations for IT Systems	3.1 System Security Plan 3.4 IT Systems Contingency Plan 3.8 Fraud Control 3.9 Patch Management
Promote Awareness	Security awareness training	*See the CMS Minimum Security Requirements*
Monitor & Evaluate Policy and Control Effectiveness	Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including: • Network assessments • Penetration activities • Change management procedures • Other Remedial activities, processes and reporting for deficiencies Incident detection, reporting and response	3.3 Certification 3.5.1 Annual Compliance Audit 3.5.2 Plan of Action and Milestones 3.6 Incident Reporting and Response 3.7 System Security Profile

3.1 REPORTING REQUIREMENTS

Given the fact that FISCAM's intended audience is financial statement auditors (i.e., Inspector Generals and independent auditors) it contains no reporting requirements directed specifically at agency management. FISMA however contains specific reporting requirements for agency management as well as the Inspector General.

According to the OMB Memorandum for Heads of Executive Departments and Agencies, published on June 13, 2005, regarding FISMA reporting instructions, "all agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget and Congress on the effectiveness of their security programs". According to the memorandum, each agency head's annual report should be submitted to the Director of OMB and should comprise:

- A transmittal letter from the agency head, including a discussion of any differences between the findings of the agency CIO and IG
- Results of annual IT security reviews of systems and programs [completed by the CIO]
- Results of the IG's independent evaluation [completed by the IG]
- Status of agency compliance with OMB privacy policies [completed by the senior agency official for privacy]

The memorandum states that, prior to submission of the report, the CIO and IG assessment results need to be reconciled to resolve discrepancies, if any, between the two sections. It is also expected that a Plan of Action and Milestones (POA&M) will be developed by each agency to correct weaknesses identified in the above reporting process. Reports documenting FISMA compliance updates must be sent by the agency to OMB on a quarterly basis.

The memorandum emphasizes the fact that FISMA applies to information systems used or operated by an agency or by a contractor of the agency or other organization on behalf of the agency. It also states that agencies should report both at an agency-wide level as well as by individual component. Clearly, the FISMA requirements apply to CMS Business Partners listed in the introduction section of the whitepaper.

In the CMS security requirement environment, the BPSSM discusses a tool to help CMS business partners conduct systems security self-assessments. It is known as the CMS Integrated Security Suite (CISS) tool. This tool assists business partners to prepare for periodic audits. Upon completion of a self assessment, the business partner is required to submit the database to the CMS Central Office, the Consortium Contractor Management Officer and/or CMS Project Officer (CCMO/PO) for review [along with other required security documentation which is described in section three (3) of the BPSSM]. For CMS business partners, Joint Signature Memorandum JSM-05352, dated 05-17-05, specifies that POA&M reporting is to be performed on a monthly basis.

It is critical that the security review and reporting cycle prescribed by the BPSSM follow a time table that allows for timely input to the FISMA reporting process and deadlines mentioned above.

4 CONCULSION

The primary objectives of effective IT security requirements and audits are to maintain confidentiality, integrity, and availability around information critical to the organization’s mission. Through the implementation of effective IT security requirements, vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud. The implementation of the security requirements discussed in the whitepapers, however, should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated into the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS’ operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS’ security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

5 REFERENCES

- GAO/GAO-08-1029G, *Federal Information System Controls Audit Manual (FISCAM) Exposure Draft,* July 2008.
- *OMB Guidance on FISMA Reporting Instructions*, Memorandum for Heads of Executive Departments and Agencies, June 13, 2005.
- *Federal Information Security Management Act (FISMA)* of 2002.
- NIST Special Publication 800-53*, Recommended Security Controls for Federal Information Systems*, December 2007.
- *CMS Business Partners Systems Security Manual (BPSSM)*, as amended and CMS approved.