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

CMS Security Whitepaper:

Change Management

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *CHANGE MANAGEMENT,* VERSION 2.0

1) Updated baseline version with CMS style format.
2) Section 1: Changed controls to security requirements.
3) Section 2: Updated the FISCAM quotes to match those of the July 2008 FISCAM version.
4) Section 3: Changed the BPSSM appendix C to appendix B.
5) Section 4: Replaced the BPSSM reference with the ARS.
6) Section 6: Changed the reference to the BPSSM to the ARS.
7) Table 2: Combined the applicable FISCAM controls to the applicable CMSRs.
8) Table 3: Deleted.

SUMMARY OF CHANGES IN *CHANGE MANAGEMENT,* VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

A key component of effectively managing information technology (IT) security requirements is the comprehensive FISCAM security controls validating the change management procedures. Included in the FISCAM controls around change management are requirements for maintaining change management documentation.

This whitepaper will:

- provide a high level understanding of change management procedures,
- facilitate the identification of IT security requirements, in key federal guidelines and standards, which are directly related change management procedures, and
- provide a sample of prior instances of non-compliance with the CMSRs and FISCAM controls with recommended corrective measures.

2 INTRODUCTION TO CHANGE MANAGEMENT PROCEDURES

General Accounting Office' (GAO) *Federal Information Systems Controls Audit Manual (FISCAM) Exposure Draft* states that:

> "Establishing controls over the modification of information system components and related documentation helps to ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all hardware, software, and firmware programs and program modifications are properly authorized, tested, and approved, and that access to and distribution of computer assets is carefully controlled."
>
> "Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing systems changes. However, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change."
>
> "The use of standardized change request forms helps ensure that requests are clearly communicated and that all approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected."

3 RISKS OF NON-COMPLIANCE

In discussing change controls, FISCAM states that “Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or ‘turned off’ or that processing irregularities or malicious code could be introduced.” Following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- a knowledgeable programmer could surreptitiously modify program code to provide a means of bypassing controls to gain access to sensitive data;
- the wrong version of a program could be implemented, thereby perpetuating outdated or erroneous processing that is assumed to have been updated; or
- a virus could be introduced, inadvertently or on purpose, that disrupts processing.

Within appendix B of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. Manual controls, such as required maintenance of hardcopy forms/documentation (e.g., change control approvals), are discussed as a key safeguard against employee fraud. For a more detailed look into each of the measures for the prevention and detection of fraudulent activities see appendix B of the BPSSM.

4 SPECIFIC REQUIREMENTS TO BE IMPLEMENTED

All security requirements documented in the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as ‘guidance’ and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all security requirements are deemed applicable, unless other compensatory controls are in place, which satisfy the security requirements’ objective.

Table 2 lists all the applicable to the programmer access to data and source code specific to a FISCAM audit and related CMSRs respectively. Refer to chapters three (3) and four (4) of FISCAM for the “Control Techniques” and “Audit Procedures” for each “Control Activity” listed in Table 2. Refer to the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* for a more detailed discussion of each CMSR in Table 2.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific “Control Enhancements”, within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare claims processing systems and Medicare data center systems be categorized as “high impact” security systems.

As mentioned above, Table 2 contains a listing of all FISCAM controls listed in the FISCAM which are applicable to change management.

Refer to the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) for “supplemental guidance” on each security requirement listed in Table 2 and a description of “Minimum Assurance Requirements” for High Baseline information systems in appendix A.

In order to provide further detailed guidance on specific controls for each FISCAM critical element the reader can then refer to chapters three (3) or four (4) of FISCAM for detailed guidance on “control techniques” and “audit procedures” for each of the corresponding FISCAM controls.

Within the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, CMS has outlined the mandatory CMSRs which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate security requirements to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CMSRs within the body of the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* document. The CMSRs are organized into seventeen families and three (3) classes, as described in the CMSRs of the document.

CMS management is committed to ensuring that each version of the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* and BPSSM (current and future versions) includes the applicable FISCAM and CMSRs discussed above in order to facilitate full compliance with guidelines around change management procedures.

5 SAMPLE INSTANCES OF NON-COMPLIANCE AND RECOMMENDED RESOLUTION

Table 1 provides a listing of sample instances of non-compliance with change management controls based on prior controls reviews and audits. Specifically, the findings, issues and recommended course of action for selected cases of non-compliance. The findings and issues in Table 1 are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected instead in order to give the reader a sense of “real world” cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue take into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed for a specific issue may not apply to all sites.

Table 1 Sample Findings from Prior CMS Controls Reviews and Audits

Finding	Issue	Suggested Remediation
Evidence of program staff attendance of SDLC training.	• Management could not produce the sign-in sheets for the SDLC class held in the prior year.	• Document and maintain evidence that the programming staff attended the SDLC class. The SDLC class should include (but not be limited to) the following change management: related topics: • documented authorizations for software modifications • controls around program changes as they progress through testing to final approval • Testing and approval of emergency changes • Controls around distribution and implementation of new or revised software • Program labeling
Change control process requires clarifications	• While reviewing the Software Quality Assurance (SQA) document, and completing our detailed change control testing, we noted that procedures for implementing SQA policy do not contain specific retention and disposal guidelines for the electronic or paper Change Control artifacts (i.e. Project Initiation form, Test Certification Statement, Problem Report, Testing [plan and results], Validation Readiness Review, Implementation Readiness Review, and ENDEVOR Data related to the change).	• SQA should be improved to ensure that it provides specific retention and disposal guidelines for all controls documentation including the Project Initiation form, Test Certification Statement, Problem Report, Testing (plans and results), Validation Readiness Review, Implementation Readiness Review, and ENDEVOR Data related to the change
Compliance with change control procedures	• During the completion of our detailed testing related to the Change Control procedures in use, we noted the following issues: • Of the changes we reviewed for different systems, the standard Change Control procedures were not consistently followed. Specifically, the following was noted: • The application personnel for one system did not use the Project Initiation/Project Release Notice and the Release Notification Package. • The standard change initiation form was not used for the changes we reviewed for one of the systems.	• All changes to applications should consistently follow the official change control policies and procedures outlined in the SQA document. • Management should periodically select a sample of changes for high impact systems to check that procedures are being observed. The entity performing the validation should be organizationally independent of the application being reviewed.

Finding	Issue	Suggested Remediation
	• The Initiation form and the Release Notification Package were not provided to the Software Quality Assurance Point of Contact (SQA POC) for any of the changes reviewed. • Evidence of testing was not available for the changes selected for some of the systems.	
Developer movement of changes into production	• During our review of the ENDEVOR change control software configuration, we noted the following issues: • Application programmers for one application system can cause, through the ENDEVOR approval process, software changes to be placed in the production environment without the knowledge or approval of the application Business Owners. The current ENDEVOR configuration, as it relates to this application system, does not require Business Owner approval for movement of changes into the production environment. • The application programmers for another application system are also the application Business Owners. This results in a lack of separation of duties between the personnel making changes to the application, and the personnel approving those changes for movement into the production environment.	• Application programmers for the application system should be required to attain Business Owner approval for movement of changes into the production environment. For the system discussed under issues, a group other than the programmers should be required to approve all application changes before they are moved into the production environment.
Application change control procedures	• Our testing disclosed the following issues: • Some change control records reviewed had the same individual approve both approval forms at the same time, contradictory to the procedure in place. • The change controls procedures discuss the unit and user testing. However, these procedures do not require the testers, both the unit and/or user, to maintain and approve this testing before it receives the final approval and is entered into production.	• Require change requests to be authorized by unique and appropriate individuals. • A standard for performing unit and user testing, maintaining the results, and approving the completion of this testing should be included within the change control procedures. This standard should be communicated and followed by the appropriate personnel.

Finding	Issue	Suggested Remediation
Mainframe systems software controls	• The "LNKAUTH=LNKLST" setting (instead of "LNKAUTH=APFTAB") was inappropriately in effect as defined within the IEASYS00 member of 'SYS1.PARMLIB'. • In addition to all libraries defined in the Authorized Program Facility (APF) List, this setting inappropriately grants APF-authorization to all libraries defined in the Link List. • APF authorized libraries contain programs that are allowed to bypass the security software (RACF) on the mainframe. Programs executed from such libraries could gain update access to all programs and data on the system and should therefore be limited to only those programs requiring this ability to execute and perform their intended function. • Through analysis of the Link List and the APF List libraries, we noted the following: • Many libraries were defined to both the Link List and to the APF List. • Some libraries were defined to the Link List, but not to the APF List, thereby attaining APF-authorization via the LNKAUTH=LNKLST setting. • Numerous libraries were defined to the APF List, but not the Link List.	• With the next operating system upgrade (i.e., rollout of the next operating system shell), • change the LNKAUTH parameter to "LNKAUTH=APFTAB", making the PROGxx members of 'SYS1.PARMLIB' the single-source of APF-authorized datasets (explicitly defined in the APF List) and using the LNKLSTxx member of 'SYS1.PARMLIB' (or • DYNAMIC LNKLST) only for its primary purpose of being the default search path for executed programs and not as a secondary APF List.
Application change management	• Change management procedures were outdated. Policies for local code procedures including emergency changes, written and published by the contractor, do not reflect the current implementation processes for emergency changes. • All of the changes sampled did not have documented authorization forms.	• Emergency change procedures, documented in the local code procedures, should • be updated to reflect the current process for implementation of emergency changes, • Management should ensure that request forms are completed and authorized before promoting a change into production. The request forms should be maintained for audit trail purposes.

6 PERIODIC REVIEW AND TESTING OF CONTROLS

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security requirements documented in the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* must be reviewed and modified on an on-going basis to ensure compliance with updates to federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

7 CONCLUSION

Change management procedures are controls that help to ensure that only authorized programs and authorized modifications are implemented. Documentation of these processes are critical in that they allow CMS management to identify who requested a change to the system, why the change was requested (business/operational justification), what the exact change was who made the change and who approved the change. Through the implementation of effective change management procedures, security 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 these security requirements should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in 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.

Table 2 depicts the applicable FISCAM controls linked to the applicable CMSRs for Change Management.

Table 2 Applicable FISCAM Controls

FISCAM Critical Elements	CMSR Description
AC-3 Implement effective authorization controls	• AC-13 Supervision and Review - Access Control • AC-14 Permitted Actions without Identification or Authentication • AC-2 Account Management • AC-3 Access Enforcement • AC-6 Least Privilege • AU-2 Auditable Events • AU-6 Audit Monitoring, Analysis, and Reporting • CM-6 Configuration Settings • CM-7 Least Functionality • IA-4 Identifier Management • SC-14 Public Access Protections • SC-15 Collaborative Computing • SC-6 Resource Priority
AC-4 Adequately protect sensitive system resources	• AC-1 Access Control Policy and Procedures • AC-15 Automated Marking • AC-16 Automated Labeling • AC-17 Remote Access • AC-18 Wireless Access Restrictions • AC-2 Account Management • AC-3 Access Enforcement • AC-6 Least Privilege • AU-2 Auditable Events • AU-6 Audit Monitoring, Analysis, and Reporting • CM-5 Access Restrictions for Change • IA-4 Identifier Management • IA-7 Cryptographic Module Authentication • MA-3 Maintenance Tools • MA-4 Remote Maintenance

FISCAM Critical Elements	CMSR Description
	- MP-2 Media Access - MP-3 Media Labeling - MP-4 Media Storage - MP-5 Media Transport - MP-6 Media Sanitization and Disposal - PE-19 Information Leakage - SC-11 Trusted Path - SC-12 Cryptographic Key Establishment and Management - SC-13 Use of Cryptography - SC-16 Transmission of Security Parameters - SC-18 Mobile Code - SC-2 Application Partitioning - SC-3 Security Function Isolation - SC-4 Information Remnance - SC-8 Transmission Integrity - SC-9 Transmission Confidentiality - SC-CMS-3 - SC-CMS-4 - SI-7 Software and Information Integrity
AS-3 Implement effective application configuration management	- AC-3 Access Enforcement - AC-5 Separation of Duties - AC-6 Least Privilege - CA-2 Security Assessments - CM-3 Configuration Change Control - CM-4 Monitoring Configuration Changes - CM-5 Access Restrictions for Change - CM-6 Configuration Settings - SA-10 Developer Configuration Management - SA-11 Developer Security Testing - SA-3 Life Cycle Support - SA-5 Information System Documentation - SI-2 Flaw Remediation - SI-5 Security Alerts and Advisories
CM-1 Develop and document CM policies, plans, and procedures	- CM-1 Configuration Management Policy and Procedures - SA-3 Life Cycle Support
CM-2 Maintain current configuration identification information	- CM-2 Baseline Configuration - CM-6 Configuration Settings - CM-8 Information System Component Inventory - SA-5 Information System Documentation
CM-3 Properly authorize, test, approve, and track all	- AC-3 Access Enforcement

FISCAM Critical Elements	CMSR Description
configuration changes	• CM-2 Baseline Configuration • CM-3 Configuration Change Control • CM-4 Monitoring Configuration Changes • CM-5 Access Restrictions for Change • CM-6 Configuration Settings • CM-7 Least Functionality • SA-10 Developer Configuration Management • SA-11 Developer Security Testing • SA-2 Allocation of Resources • SA-3 Life Cycle Support • SA-4 Acquisitions • SA-5 Information System Documentation • SA-7 User Installed Software • SA-8 Security Engineering Principles
CM-4 Routinely monitor the configuration	• CM-4 Monitoring Configuration Changes • CM-5 Access Restrictions for Change • SA-10 Developer Configuration Management • SI-6 Security Functionality Verification • SI-7 Software and Information Integrity
CM-5 Update software on a timely basis to protect against known vulnerabilities	• CM-2 Baseline Configuration • CM-3 Configuration Change Control • MA-1 System Maintenance Policy and Procedures • PL-3 System Security Plan Update • RA-4 Risk Assessment Update • RA-5 Vulnerability Scanning • SA-6 Software Usage Restrictions • SA-7 User Installed Software • SC-1 System and Communications Protection Policy and Procedures • SC-19 Voice Over Internet Protocol • SI-2 Flaw Remediation • SI-3 Malicious Code Protection • SI-5 Security Alerts and Advisories • SI-8 Spam Protection
CM-6 Appropriately document and approve emergency changes to the configuration	• CM-3 Configuration Change Control • SA-10 Developer Configuration Management
CP-2 Take steps to prevent and minimize potential damage and interruption	• CM-1 Configuration Management Policy and Procedures • CM-3 Configuration Change Control • CP-10 Information System Recovery and Reconstitution • CP-2 Contingency Plan

FISCAM Critical Elements	CMSR Description
	• CP-3 Contingency Training • CP-4 Contingency Plan Testing and Exercises • CP-6 Alternate Storage Site • CP-7 Alternate Processing Site • CP-8 Telecommunications Services • CP-9 Information System Backup • IR-1 Incident Response Policy and Procedures • MA-1 System Maintenance Policy and Procedures • MA-2 Controlled Maintenance • MA-3 Maintenance Tools • MA-5 Maintenance Personnel • MA-6 Timely Maintenance • PE-1 Physical and Environmental Protection Policy and Procedures • PE-10 Emergency Shutoff • PE-11 Emergency Power • PE-12 Emergency Lighting • PE-13 Fire Protection • PE-14 Temperature and Humidity Controls • PE-15 Water Damage Protection • PE-16 Delivery and Removal • PE-17 Alternate Work Site • PE-18 Location of Information System Components • PE-9 Power Equipment and Power Cabling • PL-2 System Security Plan • PL-4 Rules of Behavior • RA-3 Risk Assessment • SA-10 Developer Configuration Management • SA-5 Information System Documentation • SI-1 System and Information Integrity Policy and Procedures
CP-3 Develop and document a comprehensive contingency plan	• CP-1 Contingency Planning Policy and Procedures • CP-10 Information System Recovery and Reconstitution • CP-2 Contingency Plan • CP-5 Contingency Plan Update • CP-6 Alternate Storage Site • CP-7 Alternate Processing Site • CP-8 Telecommunications Services • SA-3 Life Cycle Support
DA-1 Implement an effective data management system strategy and design	• AC-4 Information Flow Enforcement • AU-2 Auditable Events • AU-3 Content of Audit Records

FISCAM Critical Elements	CMSR Description
	• AU-5 Response to Audit Processing Failures • AU-6 Audit Monitoring, Analysis, and Reporting • SA-10 Developer Configuration Management • SA-3 Life Cycle Support • SA-5 Information System Documentation • SC-2 Application Partitioning • SI-4 Information System Monitoring Tools and Techniques • SI-5 Security Alerts and Advisories
IN-1 Implement an effective interface strategy and design	• SA-3 Life Cycle Support • SA-5 Information System Documentation • SI-10 Information Accuracy, Completeness, Validity, and Authenticity • SI-11 Error Handling • SI-9 Information Input Restrictions
SD-2 Control personnel activities through formal operating procedures, supervision, and review	• AC-13 Supervision and Review - Access Control • AC-2 Account Management • AC-5 Separation of Duties • CM-2 Baseline Configuration • PS-1 Personnel Security Policy and Procedures • PS-2 Position Categorization • PS-6 Access Agreements • PS-8 Personnel Sanctions • PS-CMS-1 • RA-4 Risk Assessment Update • SA-5 Information System Documentation
SM-1 Establish a security management program	• AC-1 Access Control Policy and Procedures • AT-1 Security Awareness and Training Policy and Procedures • AU-1 Audit and Accountability Policy and Procedures • CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures • CA-3 Information System Connections • CM-1 Configuration Management Policy and Procedures • CM-8 Information System Component Inventory • CP-1 Contingency Planning Policy and Procedures • IA-1 Identification and Authentication Policy and Procedures • IR-1 Incident Response Policy and Procedures • MA-1 System Maintenance Policy and Procedures • MP-1 Media Protection Policy and Procedures • PE-1 Physical and Environmental Protection Policy and Procedures • PL-1 Security Planning Policy and Procedures • PL-2 System Security Plan

FISCAM Critical Elements	CMSR Description
	• PL-3 System Security Plan Update • PL-6 Security-Related Activity Planning • PS-1 Personnel Security Policy and Procedures • PS-CMS-2 • RA-1 Risk Assessment Policy and Procedures • SA-1 System and Services Acquisition Policy and Procedures • SA-2 Allocation of Resources • SC-1 System and Communications Protection Policy and Procedures • SI-1 System and Information Integrity Policy and Procedures
SM-3 Document security control policies and procedures	• AC-1 Access Control Policy and Procedures • AT-1 Security Awareness and Training Policy and Procedures • AU-1 Audit and Accountability Policy and Procedures • CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures • CM-1 Configuration Management Policy and Procedures • CP-1 Contingency Planning Policy and Procedures • IA-1 Identification and Authentication Policy and Procedures • IR-1 Incident Response Policy and Procedures • MA-1 System Maintenance Policy and Procedures • MP-1 Media Protection Policy and Procedures • PE-1 Physical and Environmental Protection Policy and Procedures • PL-1 Security Planning Policy and Procedures • PS-1 Personnel Security Policy and Procedures • RA-1 Risk Assessment Policy and Procedures • SA-1 System and Services Acquisition Policy and Procedures • SC-1 System and Communications Protection Policy and Procedures • SI-1 System and Information Integrity Policy and Procedures
SM-5 Monitor the effectiveness of the security program	• AU-6 Audit Monitoring, Analysis, and Reporting • CA-2 Security Assessments • CA-4 Security Certification • CA-5 Plan of Action and Milestones • CA-6 Security Accreditation • CA-7 Continuous Monitoring • CM-4 Monitoring Configuration Changes • IR-5 Incident Monitoring • PE-6 Monitoring Physical Access • PL-5 Privacy Impact Assessment • RA-5 Vulnerability Scanning • SA-11 Developer Security Testing

FISCAM Critical Elements	CMSR Description
	• SI-4 Information System Monitoring Tools and Techniques • SI-5 Security Alerts and Advisories