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

CMS Security Whitepaper:

Implementation of an Entitywide Security Program

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *IMPLEMENTATION OF AN ENTITYWIDE SECURITY* PROGRAM, VERSION 2.0

1) Change Baseline Version with updated CMS style format.
2) Changed the word 'plan' in the title to 'program'.
3) Deleted table three (3).
4) Section 1: Revised from a guide to a whitepaper and where appropriate change controls to CMSRs.
5) Section 2: Deleted paragraphs three (3) and four (4) as these a no longer quotes from the FISCAM.
6) Section 3: Change BPSSM appendix C to appendix B.
7) Section 4: Change the comparison/relationship between the FISCAM and the NIST SP 800-53 to the FISCAM and the CMSRs. Also, added the CMS ARS with CMSRs. Removed the reference to the BPSSM as containing the CSRs.
8) Section 6: Remove references to the NIST 800-53 and change the reference to the ARS.
9) Table 2 Change the table to reflect the FISCAM Critical Element linked to the applicable CMSRs.

SUMMARY OF CHANGES IN *IMPLEMENTATION OF AN ENTITYWIDE SECURITY* PROGRAM, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

One aspect of effective information technology (IT) security requirements validation is based on a foundation of comprehensive *Federal Information Systems Controls Audit Manual (FISCAM)* controls in the development and implementation of an entitywide security program.

This whitepaper will:

- provide a high level understanding of the development and implementation of an entitywide security program,
- facilitate the identification of IT controls, in key federal guidelines and standards, which are directly related to the development and implementation of an entitywide security program, and
- provide a sample of prior instances of non-compliance with the CMSRs and recommended possible corrective measures.

2 INTRODUCTION TO THE DEVELOPMENT AND IMPLEMENTATION OF AN ENTITYWIDE SECURITY PROGRAM

The *Business Partners Systems Security Manual (BPSSM)* defines entity-wide security program as "…the cornerstone of effective security control implementation and maintenance. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by senior management, and staffed by individuals with proper training and knowledge."

According to General Accounting Office' (GAO) *Federal Information Systems Controls Audit Manual (FISCAM)*, key objectives of entitywide security program planning and management are to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer related controls.

3 RISKS OF NON-COMPLIANCE

In discussing security program planning and management, the FISCAM states that "without a well designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources."

Within appendix B of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. Included in these safeguards are a number of security-planning related topics

such as “screening new employees” and “training”. 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 requirements documented in the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) are mandatory and must be in place. Note: The CMSRs are listed in appendices to the document. Additionally, the BPSSM provides further guidance. 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 requirement’s objective.

Table 2 lists all the applicable FISCAM controls to the entitywide security program 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 the entitywide security program.

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.

For business partners within the BPSSM, 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 controls 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* and a detailed listing of all security requirements in the appendices of the document. The CMSRs are organized into seventeen families and three (3) classes, as described in the CMSR 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) include the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with the entitywide security program.

5 SAMPLE INSTANCES OF NON-COMPLIANCE AND RECOMMENDED RESOLUTION

Table 1 below provides a listing of sample instances of non-compliance with development and implementation of an entitywide security plan based on prior and on-going controls reviews and audits. Specifically, the attachment lists 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 current and prior instances of non-compliance at all CMS sites. A sample of prior (and on–going) 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 takes into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the attachment for a specific issue may not apply to all sites.

Table 1 Sample Findings from CMS Controls Reviews and Audits

Finding	Issue	Suggested Remediation
Data classification policy has not been fully implemented	During our review of the data classification policy, we found that the policy has not been fully implemented.	The data classification policy should be fully implemented to ensure that all parties who handle data resources are aware of the security protection required for the resources.
Failed to conduct periodic background reinvestigations of personnel in sensitive positions	This finding is critical not only for employees who currently hold positions categorized as highly sensitive, but also for employees who may transfer from positions requiring minimal background checks to those positions requiring higher-level security checks.	The Business partner should engage in active communication with CMS during the development and implementation of CMS' high-level security policy to become familiar with the required reinvestigation guidelines. CMS should implement its high-level security policy to address the requirements for periodic background reinvestigations. These requirements should ensure that positions are classified by sensitivity level and that reinvestigations are conducted for employees in all sensitive positions defined within the organization, as well as for those employees transferring to sensitive positions.

Finding	Issue	Suggested Remediation
Security awareness and safety training for employees needs strengthening	Several employees were identified who had not completed the required prior year security awareness refresher-training course. Also, data center staff had not received periodic safety training in emergency, fire, water and alarm incident procedures since 2 years prior.	Management should ensure that all employees complete their annual training requirements. Further, officials should ensure that training in emergency, fire, water, and alarm incident procedures is conducted annually for new and existing data center employees.
New hires did not receive new employee orientation	A significant number of a sample of new hires did not receive New Employee Orientation, which consists of policy training, data training on the Data Classification and Handling System, and training on the acceptable use of the internet and communication systems.	Management should fully implement mandatory new hire training for all employees to ensure that employees are aware of their security responsibilities. Additionally, we recommend more stringent monitoring of new hire training for all employees, including penalties for those employees who do not attend. Monitoring should include periodic sampling of compliance by management.
Annual security awareness training refresher course is not mandatory	Our review of the annual security awareness training refresher course noted that there has not been an establishment of a mandatory requirement for all employees/contractors to participate in the refresher course.	We recommend that management establish a mandatory requirement for 100% participation of the annual security awareness refresher training course for all associates and contractors relative to their job functions and their access to sensitive information. Additionally, we recommend monitoring and tracking compliance of this requirement for all associates and contractors. Like the audit team, management should periodically select a sample of employees during the year to check ongoing compliance.
The incident response capability needs strengthening	During our review of the Computer Incident Response Capability we noted that an understanding of the constituency being served is unavailable, as well as evidence of the Incidence Response Team qualifications and training.	We recommend that management review their incident response capability and ensure that an Incidence Response Team is established with the necessary qualifications, skills, knowledge and abilities to respond to security incidents. Additionally, the Incidence Response Team should be trained, at a minimum, annually on emergency/incidence response and procedures. That training should be monitored and tracked for 100% participation of all IRT members.
Job rotation and vacation policy does not exist	A formal policy mandating periodic job rotations and vacation for personnel does not exist.	We recommend that management incorporate a formal job rotation and vacation policy so that responsibilities can be re-assigned to different individuals. Should neither of the above two measures exist, we recommend the monitoring of employee activities who are exposed to sensitive data over extended periods in

Finding	Issue	Suggested Remediation
		order to reduce potential security risks.
Weaknesses identified in termination process	During our review of Exit Interview checklists for a sample of terminations, we noted that checklists were not completed for a large percentage of terminations.	We recommend that the enforcement of the termination policy/procedures be strengthened. Management should be held accountable for completion of termination checklist.

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 the *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 controls documented in the BPSSM 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

The development and implementation of an entitywide security plan is the foundation for building a secure information processing environment. The objective of development and implementation of an entitywide security program is to provide a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an entity's computer related controls.

Through the development and implementation of an effective entitywide security plan, 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 effective IT controls 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 Applicable FISCAM Controls

FISCAM Critical Elements	CMSR Description
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 • 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-2 Periodically assess and validate risks	• CA-4 Security Certification • CA-6 Security Accreditation • RA-1 Risk Assessment Policy and Procedures • RA-2 Security Categorization • RA-3 Risk Assessment • RA-4 Risk Assessment Update

FISCAM Critical Elements	CMSR Description
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-4 Implement effective security awareness of other security-related personnel policies	• AC-2 Account Management • AT-2 Security Awareness • AT-3 Security Training • AT-4 Security Training Records • PE-3 Physical Access Control • PL-4 Rules of Behavior • PS-1 Personnel Security Policy and Procedures • PS-2 Position Categorization • PS-3 Personnel Screening • PS-4 Personnel Termination • PS-5 Personnel Transfer • PS-6 Access Agreements • PS-7 Third-Party Personnel Security • PS-8 Personnel Sanctions

FISCAM Critical Elements	CMSR Description
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 • SI-4 Information System Monitoring Tools and Techniques • SI-5 Security Alerts and Advisories
SM-6 Effectively remediate information security weaknesses	• CA-5 Plan of Action and Milestones
SM-7 Ensure that activities performed by external third parties are adequately secure	• AC-20 Use of External Information Systems • AT-1 Security Awareness and Training Policy and Procedures • MA-4 Remote Maintenance • MA-5 Maintenance Personnel • PS-3 Personnel Screening • PS-7 Third-Party Personnel Security • SA-4 Acquisitions • SA-9 External Information System Services

(This Page Intentionally Blank)