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

CMS Security Whitepaper:

Programmer Access to Data and Source Code

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *PROGRAMMER ACCESS TO DATA AND* SOURCE CODE, VERSION 2.0

1) Updated baseline version with CMS style format.
2) Section 1: Changed the wording of guidelines to whitepapers.
3) Section 3: Changed the BPSSM appendix C to appendix B.
4) Section 4: Modified the wording to include the ARS and use of the CMSRs with the FISCAM controls.
   a) Changed the references to the tables to Table 2.
5) Section 6: Change the BPSSM to the ARS.
6) Table 2: Modified to incorporate the applicable CMSRs with the applicable FISCAM controls.
7) Table 3: Deleted.

SUMMARY OF CHANGES IN *PROGRAMMER ACCESS TO DATA AND* SOURCE CODE, 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 meeting information technology (IT) security requirements is a comprehensive monitoring process by using the FISCAM security controls is to check access for application programmers to application data and source code.

This whitepaper will;

- provide a high level understanding of security requirements around access for application programmers to application data and source code,
- facilitate the identification of IT requirements, in key federal guidelines and standards, which directly concern access for application programmers to application data and source code, and
- provide a sample of prior instances of non-compliance with the CMSRs and the FISCAM controls.

2 INTRODUCTION TO ACCESS CONTROLS FOR APPLICATION PROGRAMMERS TO APPLICATION DATA AND SOURCE CODE

The *Business Partners Systems Security Manual (BPSSM)* defines application software development and change controls as controls that "address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information."

General Accounting Office' (GAO) *Federal Information Systems Controls Audit Manual (FISCAM) Exposure Draft* states that "Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled."

A key component of comprehensive access controls for application programmers is 'Segregation of Duties'. FISCAM defines 'Segregation of duties' as controls that describe how work responsibilities should be segregated so that one person does not have access to or control over all of the critical stages of an information handling process. For instance; while a representative of the user community may initiate requests to changes in system capabilities, computer programmers should not be able to write, test, and approve program changes; and a user who has entered transactions in the system, should not have the capability to also review and approve the processing of all such transactions. Often, proper segregation of duties is achieved by splitting responsibilities between two or more organizational groups to ensure independence and objective checks and balances. These controls can be enforced through automated and/or manual measures.

3 RISKS OF NON-COMPLIANCE

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.

FISCAM states that "inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed." FISCAM provides the following example of potential consequences of inadequate controls around segregation of duties;

> A computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Within appendix B of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. 'Separation of Duties' is listed 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. Additionally, the BPSSM provides further guidance, such as appendix B, *An Approach to Fraud Control*. It should be noted, however, that the 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 controls are deemed applicable, unless other compensatory controls are in place, which satisfy the control 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 CMSRs 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 applicable to the programmer access to data and source code.

Refer to the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) for a description of "Minimum Assurance Requirements" for High Baseline information systems. The High Baseline CMSRs are listed 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* and a detailed listing of all controls 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 the BPSSM (current and future versions) includes the applicable FISCAM controls and CMSRs discussed above in order to facilitate full compliance with guidelines around application programmers' access to application data and source code.

5 SAMPLE INSTANCES OF NON-COMPLIANCE AND RECOMMENDED RESOLUTION

Table 1 provides a listing of sample instances of non-compliance with controls around application programmers' access to application data and source code, based on prior 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 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 in the attachment 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
ACCESS TO DATABASE SECURITY TABLES	PROGRAMMERS AND CONTRACTORS HAVE UPDATE ACCESS TO THE DATABASE SECURITY TABLES OF SELECTED SYSTEMS.	UPDATE ACCESS TO THE APPLICATION DATABASE SECURITY TABLES SHOULD BE REMOVED FOR PROGRAMMERS AND CONTRACTORS. THE ACCESS RIGHTS LIMITATION DOCUMENTATION MUST BE AVAILABLE TO ALL KEY SECURITY POSITIONS INCLUDING, BUT NOT LIMITED TO, SECURITY ADMINISTRATORS, SYSTEM ADMINISTRATORS, AND VARIOUS SECURITY COMPLIANCE MONITORING POSITIONS.
CHANGE CONTROL PROCESS	WHILE REVIEWING THE SOFTWARE QUALITY ASSURANCE (SQA) DOCUMENT, AND COMPLETING OUR DETAILED CHANGE CONTROL TESTING, WE NOTED THAT THE PROCEDURES FOR IMPLEMENTING SQA POLICY DO NOT CONTAIN SPECIFIC	SQA SHOULD BE IMPROVED TO ENSURE THAT IT PROVIDES SPECIFIC RETENTION AND DISPOSAL GUIDELINES FOR ALL ARTIFACTS INCLUDING THE PROJECT INITIATION FORM, TEST CERTIFICATION STATEMENT, PROBLEM REPORT,

	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).	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 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	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.

	INITIATION FORM WAS NOT USED FOR THE CHANGES WE REVIEWED FOR ONE OF THE SYSTEMS. 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,	APPLICATION PROGRAMMERS FOR THE APPLICATION SYSTEM, SHOULD BE REQUIRED TO ATTAIN BUSINESS OWNER APPROVAL FOR MOVEMENT OF CHANGES INTO THE PRODUCTION ENVIRONMENT. FOR THE ONE 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.

	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.	
PRODUCTION SYSTEMS LOGICAL ACCESS	THE OPERATIONS ATTRIBUTE, WHICH ALLOWS SPECIAL PRIVILEGES UNDER THE SECURITY SOFTWARE ON THE MAINFRAME, INCLUDING THE ABILITY TO BYPASS SECURITY AND/OR CHANGE ACCESS FOR SOME OTHER USERS, WAS ASSIGNED TO A PERSON WHO NO LONGER NEEDS THE ATTRIBUTE TO PERFORM JOB RESPONSIBILITIES. THIS PERSON WAS A MAINFRAME SYSTEMS PROGRAMMER, BUT NOW SUPPORTS MID-	MANAGEMENT SHOULD ENSURE THAT: USER ACCESS ASSIGNED IS PERIODICALLY REVIEWED AND ADJUSTED AS NECESSARY, INCLUDING REVIEW OF ACCESS TO SYSTEMS SOFTWARE FILES. ACCESS IS ONLY ASSIGNED ON THE BASIS OF LEAST PRIVILEGE TO PERFORM JOB RESPONSIBILITIES. ACCESS ASSIGNED ENSURES SEGREGATION OF DUTIES IS ENFORCED. ACCESS ASSIGNMENT

	RANGE SYSTEMS.	PROCESSES ARE CONSISTENTLY PERFORMED THROUGH THE USE OF FORMAL WRITTEN STANDARD PROCEDURES THAT DEFINE THE PROCESSES TO ASSIGN, REVIEW OR MODIFY THE ACCESS OF ALL SYSTEM USERS.
	ALTER ACCESS TO PRODUCTION DATA HAS BEEN GRANTED TO NUMEROUS USERS, INCLUDING SYSTEMS ANALYSTS AND APPLICATION PROGRAMMERS. ALTER ACCESS BY SYSTEMS ANALYSTS AND APPLICATION PROGRAMMERS REPRESENTS A SEGREGATION OF DUTIES ISSUE FOR THESE USERS WHO COULD USE THIS ACCESS TO CHANGE DATA OUTSIDE OF THE APPLICATION PROCESSES.	ONGOING REVIEW AND MONITORING OF USER ACTIVITIES IS PERFORMED FOR THE USE OF SENSITIVE UTILITY PROGRAMS OR ACCESS TO SYSTEM DATASETS.
	ACCESS TO BYPASS TAPE DATASET SECURITY CHECKING HAD BEEN ASSIGNED TO A NUMBER OF USERS, INCLUDING NUMEROUS SYSTEMS ANALYSTS AND APPLICATION PROGRAMMERS. SUCH ACCESS VIOLATES THE CONCEPT OF SEGREGATION OF DUTIES AND ALLOWS ALL OF THESE USERS TO ACCESS AND UPDATE ANY TAPE DATASET.	
PRODUCTION SYSTEMS LOGICAL ACCESS	SOME OF THE INDIVIDUALS AUTHORIZED TO MOVE APPLICATION CHANGES INTO PRODUCTION WERE APPLICATION PROGRAMMERS.	APPLICATION PROGRAMMER ACCESS TO THE PRODUCTION ENVIRONMENT SHOULD BE REMOVED,

		FURTHERMORE, ACCESS PROVIDED TO THE PROGRAMMERS SHOULD BE LIMITED TO THEIR JOB RESPONSIBILITY.
APPLICATIONS PROGRAMMERS ACCESS TO PRODUCTION CODE AND DATA	DURING OUR AUDIT WE NOTED THE FOLLOWING DEFICIENCIES: PROGRAMMERS HAVE ACCESS TO NETWORK-BASED APPLICATIONS INCLUDING PRODUCTION CODE AND PRODUCTION DATA. PROGRAMMER ACCESS TO BOTH OLDER AND NEW NETWORK-BASED APPLICATION PRODUCTION CODE AND DATA INCLUDES READ, WRITE, AND DELETE ACCESS RIGHTS.	CREATE AND MAINTAIN A CHANGE MANAGEMENT PROCESS THAT CONTROLS ALL NETWORK-BASED APPLICATION ENVIRONMENTS. CREATE SEPARATE TEST/DEVELOPMENT ENVIRONMENT FOR NETWORK-BASED APPLICATIONS. BUILD APPLICATION ACCESS CONTROLS INTO NETWORK-BASED APPLICATIONS. ALTER PROGRAMMER ACCESS RIGHTS TO PRODUCTION CODE AND DATA FOR NETWORK-BASED APPLICATIONS.

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 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

Controls around application programmers' access to application data and source code help to ensure that only authorized programs and authorized modifications are implemented. Segregation of duties, a key component of these controls, facilitate the separation of work responsibilities such that one person does not have access to or control over all of the critical stages of an information handling process such that unauthorized data access and modification is not prevented or detected.

Through the implementation of effective controls around application programmers' access to application data and source code 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 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 depicts all the FISCAM critical elements with related CMSRs that should be included in the on-going compliance process.

Table 2 Applicable FISCAM Controls

FISCAM CRITICAL ELEMENTS	CMSR DESCRIPTION
SD-1 SEGREGATE INCOMPATIBLE DUTIES AND ESTABLISH RELATED POLICIES	• **AC-13 SUPERVISION AND REVIEW - ACCESS CONTROL** • **AC-5 SEPARATION OF DUTIES** • **PE-3 PHYSICAL ACCESS CONTROL** • **PS-2 POSITION CATEGORIZATION** • **PS-6 ACCESS AGREEMENTS** • **PS-7 THIRD-PARTY PERSONNEL SECURITY** • **SA-2 ALLOCATION OF RESOURCES** • **SA-5 INFORMATION SYSTEM DOCUMENTATION**
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**