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

CMS Security Whitepaper:

Logical Access Controls and Segregation of Duties

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *LOGICAL ACCESS CONTROLS AND SEGREGATION* OF DUTIES, VERSION 2.0

1) Updated baseline version with the CMS style format.
2) Section 1: Changed the wording of controls to IT security requirements.
   a) Change the guidelines wording to whitepaper.
   b) Added the ARS for listing CMSRs and comparison with the FISCAM controls.
3) Section 2: Deleted quotes from the BPSSM that are not in the BPSSM updates.
4) Section 3: Changed BPSSM appendix C to appendix B.
   a) Added another example of possible vulnerability from the July 2008 FISCAM.
5) Section 6: Change NIST SP 800-53 to the CMSR and added the ARS as a go-to reference.
6) Combined applicable FISCAM critical elements with applicable CMSRs in Table 2.
7) Deleted Table 3.

SUMMARY OF CHANGES IN *LOGICAL ACCESS CONTROLS AND SEGREGATION* OF DUTIES, 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 logical access controls and segregation of duties.

This whitepaper will;

- provide a high level understanding of logical access controls and segregation of duties,
- facilitate the identification of IT security requirements, in key federal guidelines and standards, which are directly related to logical access controls and segregation of duties, and
- provide a sample of prior instances of non-compliance with the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) and the FISCAM controls.

2 INTRODUCTION TO LOGICAL ACCESS CONTROLS AND SEGREGATION OF DUTIES

According to the FISCAM, key objectives of logical access controls are to ensure that (1) users have only the access needed to perform their duties, (2) access to very sensitive resources, such as security software programs, is limited to very few individuals, and (3) employees are restricted from performing incompatible functions or functions beyond their responsibility.

FISCAM states that "If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with the practical needs of users. However, establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users."

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (IDs), passwords, or other identifiers that are linked to predetermined access privileges. Controls should be designed to restrict legitimate users to the specific systems, programs, and files needed to perform their duties while inhibiting access by others.

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 representatives of the user community may initiate requests for changes to system capabilities, computer programmers should not be allowed 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. Controls can be enforced through automated and/or manual measures.

3 RISKS OF NON-COMPLIANCE

Per FISCAM, "inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure and modification of data".

Following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- By obtaining direct logical access to data files, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) alter critical data needed to make a strategic policy decision, or (4) obtain confidential personal, commercial, and governmental information.
- By obtaining logical access to business process applications58 used to process transactions, an individual could grant unauthorized access to the application, make unauthorized changes to these programs, or introduce malicious programs, which, in turn, could be used to access data files, resulting in situations similar to those just described, or the processing of unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for him or herself.
- By obtaining access to system-level resources, an individual could circumvent security controls to read, add, delete, or modify critical or sensitive business information or programs. Further, authorized users could gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into the application programs.
- By obtaining physical access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.

FISCAM states that, "Inadequately segregated duties, conversely, 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. For example:

- An individual who is independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection.
- 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, the Centers for Medicare and Medicaid Services (CMS) outlines a number of specific safeguards against employee fraud. Segregation 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 CMS Minimum Security Requirements (CMSR) are documented and explained in either the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* 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 CMSRs are deemed applicable, unless other compensatory controls are in place which satisfy the CMSR objective.

Table 2 lists all the applicable logical access controls and segregation of duties 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 logical access controls and segregation of duties.

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 CMSRs 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 logical access controls and segregation of duties.

5 SAMPLE INSTANCES OF NON-COMPLIANCE AND RECOMMENDED RESOLUTION

Table 1 below provides a listing of sample instances of non-compliance with logical access controls and segregation of duties 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 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 Prior CMS Controls Reviews and Audits

Finding	Issue	Suggested Remediation
Resource owners have not identified or granted access to authorized users.	No user access documentation exists for network devices, including the Cisco router and the Cisco PIX firewall.	Continue efforts in developing a logging and monitoring strategy for Cisco routers and Cisco PIX firewalls. The strategy should be implemented on the Medicare systems and throughout the organization. A policy should also be developed to outline roles and responsibilities in ensuring that the systems are configured correctly and that logs are being generated and reviewed. A formal user access policy should be complied with for granting users access to all network devices including Cisco routers and Cisco PIX firewalls.
	Access to the Cisco routers and the Cisco PIX firewall are not proactively monitored.	
	Logging is disabled on the Cisco PIX firewall.	
Oracle database control deficiencies	A process for establishing the accounts is not defined and documented.	Develop and document procedures for establishing Oracle accounts.
	The defined privileges are not periodically assessed and revalidated.	Develop and document procedures for reviewing Oracle accounts, account privileges, and user roles.
	Procedures for assigning user roles have not been documented.	Develop and document procedures for assigning user roles.
	Oracle logs are not reviewed and automated tools to assist in log reviews do not exist.	Develop and document procedures for reviewing Oracle logs. Research and implement automated tools to assist in log

Finding	Issue	Suggested Remediation
		reviews and monitoring.
	The configuration setting to provide log actions performed by privileged accounts was not set.	Configure the Oracle initialization file to generate audit logs of actions performed by privileged users.
Improvements in Password controls over network devices that allow Dial-in access	Noted poor password controls for devices that allow access to the network. As a result, passwords could be easily guessed.	Management should establish, implement, and enforce formal policies and procedures for remote access password-use ensuring that "hard-to-guess" passwords are required for authentication of remote users.
Password Parameters did not meet CMS Core Security Requirements	For the mainframe, the following ACF2 password settings were used:	ACF2 policies should be improved to meet the minimum requirements outlined in the CMS Core Security Requirements. Correct and resubmit CMS CAST worksheets to reflect the current environment.
	PSWD HISTORY = NO - Activates default history of one generation. Old passwords may be used after one generation	
	MIN PSWD LENGTH = 5 - Allowed five characters for a minimum.	
	LOGON RETRY COUNT = 3 - Does not deactivate the user ID after three failed passwords, but rather logs the terminal session off. The user can immediately restart the session and conduct additional logon attempts.	
	MAX PSWD ATTEMPTS = 6 - Allows a user ID to have six invalid password attempts during a password change period, at which time the account is locked out.	
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 order to reduce potential security risks.

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 security requirements 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 CMSRs 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 requirements 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 requirements and proper testing of existing security requirements.

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

Logical access controls are controls that provide reasonable assurance that information handling resources are protected against unauthorized loss, modification, disclosure, and damage. Segregation of duties controls are controls that 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 logical access controls and segregation of duties, 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 and validated by the FISCAM 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 security requirements' 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 lists all the applicable logical access controls and segregation of duties specific to a FISCAM audit and related CMSRs respectively.

Table 2 Applicable FISCAM Controls

FISCAM Critical Elements	CMSR Description
AC-1 Adequately protect information system boundaries	• AC-11 Session Lock • AC-12 Session Termination • AC-17 Remote Access • AC-18 Wireless Access Restrictions • AC-19 Access Control for Portable and Mobile Devices • AC-4 Information Flow Enforcement • AC-8 System Use Notification • AC-9 Previous Logon Notification • CA-3 Information System Connections • IA-3 Device Identification and Authentication • SC-10 Network Disconnect • SC-7 Boundary Protection • SC-CMS-6
AC-2 Implement effective identification and authentication mechanisms	• AC-10 Concurrent Session Control • AC-14 Permitted Actions without Identification or Authentication • AC-2 Account Management • AC-7 Unsuccessful Login Attempts • AU-10 Non-repudiation • IA-2 User Identification and Authentication • IA-3 Device Identification and Authentication • IA-4 Identifier Management • IA-5 Authenticator Management • IA-6 Authenticator Feedback • SA-3 Life Cycle Support • SC-14 Public Access Protections • SC-17 Public Key Infrastructure Certificates • SC-20 Secure Name / Address Resolution Service (Authoritative Source) • SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) • SC-22 Architecture and Provisioning for Name / Address Resolution Service • SC-23 Session Authenticity
AC-3 Implement effective authorization controls	• AC-13 Supervision and Review - Access Control • AC-14 Permitted Actions without Identification or Authentication

FISCAM Critical Elements	CMSR Description
	• 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 • 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

FISCAM Critical Elements	CMSR Description
	• SC-9 Transmission Confidentiality • SC-CMS-3 • SC-CMS-4 • SI-7 Software and Information Integrity
AC-5 Implement an effective audit and monitoring capability	• AC-13 Supervision and Review - Access Control • AT-5 Contacts with Security Groups and Associations • AU-11 Audit Record Retention • AU-2 Auditable Events • AU-3 Content of Audit Records • AU-4 Audit Storage Capacity • AU-5 Response to Audit Processing Failures • AU-6 Audit Monitoring, Analysis, and Reporting • AU-7 Audit Reduction and Report Generation • AU-8 Time Stamps • AU-9 Protection of Audit Information • IR-1 Incident Response Policy and Procedures • IR-2 Incident Response Training • IR-3 Incident Response Testing and Exercises • IR-4 Incident Handling • IR-5 Incident Monitoring • IR-6 Incident Reporting • IR-7 Incident Response Assistance • PE-6 Monitoring Physical Access • PS-8 Personnel Sanctions • SC-5 Denial of Service Protection • SI-4 Information System Monitoring Tools and Techniques • SI-5 Security Alerts and Advisories • SI-6 Security Functionality Verification
AS-1 Implement effective application security management	• AC-1 Access Control Policy and Procedures • AC-3 Access Enforcement • AC-5 Separation of Duties • AT-1 Security Awareness and Training Policy and Procedures • AT-3 Security Training • AT-4 Security Training Records • AU-1 Audit and Accountability Policy and Procedures • CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures • CA-2 Security Assessments • CA-4 Security Certification • CA-5 Plan of Action and Milestones • CA-7 Continuous Monitoring

Logical Access Controls and Segregation of Duties

FISCAM Critical Elements	CMSR Description
	• 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 • PL-2 System Security Plan • PL-3 System Security Plan Update • PS-1 Personnel Security Policy and Procedures • PS-6 Access Agreements • PS-7 Third-Party Personnel Security • RA-1 Risk Assessment Policy and Procedures • RA-3 Risk Assessment • RA-4 Risk Assessment Update • SA-1 System and Services Acquisition Policy and Procedures • SA-10 Developer Configuration Management • SA-11 Developer Security Testing • SA-4 Acquisitions • SA-5 Information System Documentation • SA-9 External Information System Services • SC-1 System and Communications Protection Policy and Procedures • SI-1 System and Information Integrity Policy and Procedures
AS-2 Implement effective application access controls	• AC-10 Concurrent Session Control • AC-11 Session Lock • AC-12 Session Termination • AC-14 Permitted Actions without Identification or Authentication • AC-2 Account Management • AC-3 Access Enforcement • AC-5 Separation of Duties • AC-6 Least Privilege • AU-1 Audit and Accountability Policy and Procedures • AU-2 Auditable Events • AU-3 Content of Audit Records • AU-6 Audit Monitoring, Analysis, and Reporting • IA-2 User Identification and Authentication • IA-4 Identifier Management • IA-5 Authenticator Management • PE-1 Physical and Environmental Protection Policy and

FISCAM Critical Elements	CMSR Description
	Procedures • PL-2 System Security Plan • SA-5 Information System Documentation • SC-10 Network Disconnect • SC-17 Public Key Infrastructure Certificates • SC-2 Application Partitioning • SC-7 Boundary Protection
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
AS-4 Segregate application user access to conflicting transactions and activities and monitor segregation	• AC-13 Supervision and Review - Access Control • AC-2 Account Management • AC-3 Access Enforcement • AC-5 Separation of Duties • SA-5 Information System Documentation
BP-2 Transaction Data Processing is complete, accurate, valid, and confidential (Transaction data processing controls)	• AC-3 Access Enforcement • AC-4 Information Flow Enforcement • CM-3 Configuration Change Control • SA-10 Developer Configuration Management • SA-3 Life Cycle Support • SA-5 Information System Documentation • SA-8 Security Engineering Principles • SC-9 Transmission Confidentiality • SI-1 System and Information Integrity Policy and Procedures • SI-10 Information Accuracy, Completeness, Validity, and Authenticity • SI-11 Error Handling • SI-12 Information Output Handling and Retention • SI-9 Information Input Restrictions
BP-3 Transaction Data Output is complete, accurate, valid, and	• AC-2 Account Management

FISCAM Critical Elements	CMSR Description
confidential (Transaction data output controls)	• MP-2 Media Access • SA-3 Life Cycle Support • SA-5 Information System Documentation • SI-1 System and Information Integrity Policy and Procedures • SI-10 Information Accuracy, Completeness, Validity, and Authenticity • SI-11 Error Handling • SI-12 Information Output Handling and Retention • SI-9 Information Input Restrictions
• BP-4 Master data setup and maintenance is adequately controlled	• AC-3 Access Enforcement • AC-4 Information Flow Enforcement • AC-5 Separation of Duties • SA-10 Developer Configuration Management • SA-3 Life Cycle Support • SA-5 Information System Documentation • SA-8 Security Engineering Principles • SC-9 Transmission Confidentiality • SI-1 System and Information Integrity Policy and Procedures • SI-10 Information Accuracy, Completeness, Validity, and Authenticity • SI-11 Error Handling • SI-9 Information Input Restrictions
IN-2 Implement effective interface processing procedures	• AC-3 Access Enforcement • SA-2 Allocation of Resources • SA-5 Information System Documentation • SI-10 Information Accuracy, Completeness, Validity, and Authenticity • SI-11 Error Handling • SI-9 Information Input Restrictions
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

FISCAM Critical Elements	CMSR Description
	• 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

(This Page Intentionally Blank)