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

CMS Security Whitepaper:

Shared System Security Violation Monitoring Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *SHARED SYSTEM SECURITY VIOLATION MONITORING* WHITEPAPER, VERSION 2.0

1) Converted baseline version dated January 29 2008 to updated CMS style format.
2) Moved Introduction, from before Table of Contents to after into new Section 1.
3) Moved text from Introduction into new Section 1.1, Scope and updated former CSR references to CMSRs.
4) Moved text from former Section 1, Background, into new Section 1.2, Background; and also:
   a) added title to Table 1, and
   b) corrected the footnote formats on footnotes 2 and 3.
5) In Section 3, Instructions for Monitoring Application Security Violations, updated former CSR references to CMSR; and updated subsection numbering.
6) In Section 3.2, Fiscal Intermediaries and Part A/B MACS Using the FISS Shared System, added titles to Figure 1 and Table 2.
7) In Section 3.3, Carriers and Part A/B MACS Using the MCS Shared System, added titles to Figure 2 and Table 3.
8) In Section 3.4, DME MACS Using the VMS Shared System, added titles to Figure 3 and Table 4.
9) In Section 5, Other Controls to Consider, updated subsection numbering.
10) Changed CSR glossary term in Appendix A to CMSR.
11) Removed former Appendix B CSRs and added pointer to new CMSRs.
12) Revised Appendix C, Quick Reference, format.
13) Updated the Appendix B CMSR reference.

SUMMARY OF CHANGES IN *SHARED SYSTEM SECURITY VIOLATION MONITORING* WHITEPAPER, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 SCOPE

This white paper was developed by PricewaterhouseCoopers LLP (PwC) for the Centers for Medicare and Medicaid Services (CMS). This document is one of a number of white papers issued by CMS management to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment.

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

Medicare business partners use standard shared systems to process Medicare claims. The Fiscal Intermediary Shared System (FISS), maintained by Pinnacle Business Solutions, Inc. (PBSI), is used by Fiscal Intermediaries and A/B MACs to process Part A claims. The Multi-Carrier System (MCS), maintained by Electronic Data Services Corporation (EDS), is used by Carriers and A/B MACs to process Part B claims. The ViPS Medicare System (VMS) is used by DME MACs to process Durable Medical Equipment claims. Together these systems process more than 1 billion Medicare claims annually[1]. The systems incorporate features and security controls to meet the standards set in the CMS Minimum Security Requirements (CMSRs). By implementing the CMSRs, CMS and their business partners ensure they are in compliance with key information security requirements for Federal agencies set by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB).

Under the CMSRs, system security administrators are required to regularly monitor activity performed within the CMS shared systems to identify suspicious events. Each of the shared systems has built-in reports to facilitate such a review. While these reports vary by shared system, all include a list of violations committed by users within the system. A violation is recorded whenever a user attempts to perform a function to which they have not been granted access.

In 2007, full-scope applications reviews over the FISS, MCS, and VMS shared systems were conducted at select Medicare contractors. These reviews were conducted in accordance with an application review work program approved by CMS and the Department of Health and Human Services (HHS) Office of Inspector General (OIG). A modified version of these procedures, narrowed to focus on high-risk areas, was performed at high volume claims processing sites. The reviews found that many contractors did not have a process in place to monitor security violations committed within their instances of the shared systems environment. Other contractors had implemented a monitoring process, but did not have sufficient procedures in

[1] *2006 CMS Financial Report* (http://www.cms.hhs.gov/CFOReport/Downloads/2006_CMS_Financial_Report.pdf)

place to ensure that all suspicious events were identified, investigated, and the outcomes of investigations documented.

When performed correctly, application security violation monitoring not only enhances the security of Medicare data by identifying potentially unauthorized attempts to affect claims processing, but also provides value to the Medicare contractor. Through the monitoring of security violations and analyzing trends over time, management can identify potential system problems, inconsistencies in user access levels, and users who may need additional system training to perform their job functions more efficiently.

This white paper has been created to assist CMS business partners implement an effective application security monitoring program. Topics presented within this document include the following:

- background of application security violation monitoring;
- relevant results from the 2007 Chief Financial Officers Act of 1990 Audit (CFO) Full Scope and Desktop Reviews;
- instructions for the monitoring of application security violations using FISS, MCS, and VMS standard system reports;
- documentation requirements; and
- other controls to consider.

Through this guidance, CMS management and business partners will be able to implement an application security violations monitoring program as part of their controls environment.

1.1 BACKGROUND

As CMS becomes more reliant on information systems to automate the claims adjudication process, a growing number of users require access to the claims and the claims processing systems. CMS and its business partners have implemented a set of features within the Medicare shared systems to limit the access of users to only the functions necessary to perform a specific job function. Although each of the shared systems take a different approach to limiting user access, each is able to limit the use of screens, functions, subsystems, and the ability to override edits. Assigning users the least amount of access necessary to perform their job function is a concept referred to as “least privilege”.

Granting access under the concept of least privilege and ensuring users complete security awareness training reduces the risk that a user will misuse an information system. However, on occasion, users will attempt to access functions in the system beyond their authorization, causing security violations to be recorded. Monitoring of violations committed within the shared systems is an essential practice to make certain users are working within the access limits defined by management.

Application Security Violation Monitoring is similar to other forms of security monitoring currently implemented by CMS business partners, such as z/OS system-level security violations. It is important to note however, that application security violation monitoring identifies

violations performed by users within an application, in this case the Medicare Shared Systems. Other forms of system monitoring such as mainframe login violation monitoring, or access control package (e.g. RACF, ACF2, or Top Secret) monitoring, only identify violations committed at the z/OS operating system level. Monitoring at the z/OS system-level identifies users who unsuccessfully attempt to access a resource such as a dataset or Customer Information Control System (CICS) transaction; however, z/OS system-level monitoring may not identify users who commit a violation within an application. For example, an unauthorized user attempting to force a Medicare claim to pass an edit using an override code would not be detected by the mainframe security software (i.e., RACF, ACF2 or Top Secret). Although z/OS system monitoring is an important part of an overall security program, this whitepaper focuses solely on application security violation monitoring.

The following definitions differentiate between the two types of monitoring:

- z/OS system-level monitoring identifies unauthorized attempts to access the mainframe.
- Application security violation monitoring identifies unauthorized attempts to perform a specific action within a shared system.

Each Medicare shared system records a violation when a user attempts to access a screen or perform an activity for which they are not authorized. The shared systems produce a report with violations committed daily. Although reports do vary slightly by system, each contains standard information about each violation including the date and time of occurrence, the user ID that committed the violation, and the nature of the violation. Refer to the table below for report details for each shared system.

Table 1 Report Details for Each Shared System

	FISS – Part A	MCS – Part B	VMS – DME
Report Number	FSSB9311[2]	H99RCRVL	SE5001
Job Number	FSSB9311	D457	VMSSE500
Data captured on report	Date and time of violation Operator ID Operator Signon/ Department File Key identifying record within the file that the operator attempted to access when the violation occurred	Date and time of violation Clerk name and ID Screen mnemonic or transaction the clerk attempted to access/ perform MCS Internal transaction ID for the screen or function Violation message the clerk received	Date and time of violation User ID Terminal ID from where the violation was performed Transaction ID from where the violation was performed Switch number corresponding to the access which the user did not have to perform the requested function Textual name of the switch and action attempted to be performed

[2] This report will only generate in instances of FISS where external security is used. For sites using FISS internal security, report FSSB9310 will list violations generated.

These reports detail all security violations recorded within the shared system. As part of an application security violation monitoring program, reports should be reviewed at a frequency that would allow for the timely follow-up of violations with the appropriate user and management staff. Depending on the number of violations noted on the report, it may be prohibitive to follow-up on every violation. It is therefore important to define and formally document a monitoring strategy that will focus on higher-risk violations that may indicate suspicious activity. Through working with business owners, security management can develop a strategy for monitoring the violation reports and setting criteria for which violations require additional follow-up. This strategy may incorporate one or more of the following approaches:

Setting a Threshold

Some violations recorded by the system may be committed by users who mistakenly used the wrong keystroke or incorrectly entered a command. If the violation was a mistake, it is reasonable to assume that a user would not make the same mistake more than a couple of times before correcting their behavior. Therefore, it may be appropriate to set a quantity of violations that may be committed before follow-up is necessary. Management can apply this threshold to the total number of violations committed by a user on a single day, or the number of times a user commits a specific type of violation. When setting a threshold, be sure that the quantity selected is low enough to identify users who are repeating a violation beyond a reasonable number of tries. The goal is not to detect and follow-up on persons who forgot their passwords, but rather to detect and follow-up on persons who are testing the system and/or exploring the threshold of their access rights.

Targeting higher-risk violations

All violations may not pose the same risk to the organization. For example, management may determine that attempts by an unauthorized user to change a provider mailing address may have a different level of risk than a claims supervisor attempting to view a standard system report. Similarly, a violation committed by a claims processor outside of normal business hours may have a different risk than a violation committed during normal hours. One approach to reducing the number of violations requiring follow-up is to identify the violations that pose a high risk to the organization and specifically target these violations for follow-up.

Trending

In addition to the individual review of daily violation reports, reviewing a series of daily reports may help to identify a trend of violations over time. For example: an organization implements a security violation monitoring program where any user who commits more than five violations per day is contacted for an explanation of their actions. A user who learns of this threshold could commit up to four violations per day without facing any questions from security, trying up to four commands per day to gauge the scope of their access to the system. Although these violations would not necessarily be investigated in daily monitoring because they do not meet the five violation threshold, a trending analysis over a series of days could note the repeated violations performed by the user. Trending can also be used to identify other types of repetitive violations, such as violations that recur on specific days of the week, at certain times of day, or when certain staff are on vacation.

The approach to identifying violations for additional follow-up should be formally documented in policies and procedures. Procedures should also document the frequency at which report monitoring should occur, identify responsibility for reviewing the report, and the process by which violations will be investigated. Individuals should be prohibited from reviewing their own violations. Follow-up on security violations should usually involve users who committed the violation, as well as supervisors and business owners who have responsibility for the areas of the system where the violation occurred. For each violation warranting follow-up, a reason for the violation should be documented; and, if the explanation is not sufficient, a process implemented to escalate violations to the appropriate security group or management. Follow-up activities should be completed timely, with documentation maintained to evidence the review of daily violation reports and follow-up on violations that meet the criteria documented in policies and procedures.

During the fiscal year 2007 CFO Act Audit, a review of application security monitoring procedures and controls was conducted over high-volume Medicare claims processing sites. The evaluation noted that monitoring programs in place have one or more of the following weaknesses, preventing violations from being identified or investigated:

- Medicare shared systems were not configured to produce violation reports.[3]*
- Violation monitoring programs had not been implemented.
- Criteria for identifying violations that require investigation had not been defined.
- Adequate documentation to support the investigation of suspicious violations was not maintained.
- Trending analysis was not performed over violations.

CMS business partners who use one or more of the shared systems should make certain that a shared system security violation monitoring program is developed and implemented, with documentation maintained to evidence the program is operating in accordance with policies and procedures.

2 SUMMARY OF RESULTS OF CFO FULL SCOPE AND DESKTOP REVIEWS

During the fiscal year 2007 CFO Act Audit, a review of application security monitoring procedures and controls was conducted over high-volume Medicare claims processing sites. The following procedures were performed to determine if the monitoring programs implemented at processing sites were sufficient:

- Inspected policies and procedures regarding applications security violation monitoring and determined if procedures included key monitoring concepts;

[3] Instances of the FISS system configured to use internal security did not produce security violation reports at the time of testing. Contractors running the FISS system are now required to use the FISS system's external security option, which does produce violation reports.

- Inspected violation reports produced by shared systems and evidence of review; and
- Inspected evidence supporting the investigation of violations that, according to documented criteria, require follow-up.

The evaluation found that while some application security violation monitoring controls are performed at some sites, these controls were not sufficient. The following issues were noted:

Medicare shared systems were not configured to produce violation reports

Instances of the FISS system configured to use internal security did not produce security violation reports at the time of testing. Contractors running the FISS system are now required to use the FISS system's external security option, which does produce violation reports.

Violation monitoring programs had not been implemented.

The evaluation found that some contractors did not have a program in place to monitor shared system violation reports. Several contractors noted that a program would be implemented after transitioning to the EDCs; however, programs had not been implemented at the time of evaluation.

Criteria for identifying violations that require investigation had not been defined.

Contractors had implemented monitoring programs; however, policies and procedures did not specify the criteria that would be used to identify violations that required follow-up. The lack of formally documented criteria may cause it to be impossible to determine if violations were investigated properly.

Adequate documentation to support the investigation of suspicious violations was not maintained.

Contractors were not able to provide documentation to support actions taken in response to security violations. In some cases, follow-up was not formally documented, in other cases documentation was incomplete or could not be located.

Trend analysis was not performed over violations.

Contractors did not have policies or procedures in place to perform trend analysis as part of their application security violation monitoring program. Some contractors noted that trending is performed informally, with staff reviewing violation reports noticing violations that recur over a period of time. Documentation provided did not however evidence this had occurred.

Together these conditions prevent suspicious violations from consistently being identified and investigated. For events that are investigated, a lack of documentation prevents management from determining if violations were investigated in accordance with policies and procedures. It was noted the cause of many of these conditions was a lack of documented policies and procedures. In other cases, policies and procedures were not followed.

3 INSTRUCTIONS FOR MONITORING APPLICATION SECURITY VIOLATIONS

Based on industry best practice and the results of the 2007 CFO Act Audit, the following instructions for monitoring application security violations have been developed for CMS business partners. These instructions have been designed meet the requirements of the CMSRs and the Federal Information Systems Control and Audit Manual (FISCAM), however business partners may have corporate or other standards which may apply to any new security monitoring programs. Therefore business partners are strongly encouraged to use the instructions below as guidance for the creation of a monitoring program specific to their organization.

1.1 PREPARING FOR A REVIEW

Identifying the appropriate stakeholders

As with any change in security process, it is important to identify and engage all stakeholders who will be affected by an application security violation monitoring program. Based on prior audit experience, the instructions refer to the following stakeholders that are typically involved in a monitoring program:

- Security Management. Team of managers within the organization responsible for overseeing information security. While this level of management is not typically involved in the application security violation monitoring process, the team should be alerted to security incidents that are identified through security violation monitoring.
- Application Security Administrator. Individual responsible for validating that access to the Medicare shared systems is appropriate. This person should not have the ability to grant or modify user access within the shared systems, but should have the ability to review reports generated by the shared system used for monitoring security violations. In most organizations, this person reports to the security management team or to a senior manager with security responsibility. While the instructions below refer to a single application security administrator, often this individual will have a team of staff performing the shared system monitoring responsibilities.
- Business Owner. Individual responsible for the operating effectiveness of the shared system within the organization. This person typically has responsibility for overseeing claims processing or other operations areas.
- Employee's Supervisor. Individual responsible for supervising an employee who has committed a security violation. This person should be notified of security violations by their staff.

Strategies for identifying violations for follow-up

In the Background section on this whitepaper, several strategies for identifying security violations requiring follow-up were discussed. Before performing the instructions below, it is

important to consider and document criteria for identifying security violations requiring follow-up. These strategies include:

- Setting a threshold. A quantity of violations that may be committed before follow-up is necessary.
- Targeting higher-risk violations. Identify the violations that pose a high risk to the organization and specifically target these violations for follow-up.
- Trending. A review of several days of violations to identify other types of repetitive violations, such as violations that recur on specific days of the week, at certain times of day, or when certain staff are on vacation.

For a full description of these strategies refer to the Background section above. These criteria can be revisited and refined over time as the security administration gains additional insight into the nature of violations performed by the organization's users.

1.1 FISCAL INTERMEDIARIES AND PART A/B MACS USING THE FISS SHARED SYSTEM

Step 1: Review security violation reports

On a regular basis, the application security administrator should obtain FISS standard report FSSB9311[4], the FISS Security Violations report, or similar report created for the same purpose. This report is generated daily from the FISS Security Logging file when the site security option is set to 'external'.

Figure 1 Example FSSB9311 Report

```
REPORT: FSSB9311                    INTERMEDIARY NAME - XXXXX              CURRENT DATE: 01/12/2008
                                     FISS SECURITY VIOLATIONS              PAGE NUMBER:  51

    OPERATOR    MENU    SIGNON      TIME        DATE      FILE KEY

    MCPTA088    56 I     CLM      10:14:05    01/12/08    555129876A 50294869502345
    MCPTA088    56 I     CLM      10:14:15    01/12/08    555129876A 50294869502345
    MCPTA012    44 I     CLM      10:14:53    01/12/08    555873258A 50201934856632
    MCPTA088    41 I     CLM      10:15:01    01/12/08
    MCPTA088    42 I     CLM      10:15:15    01/12/08    555129876A 50294869502345
    MCPTA012    57 I     CLM      10:15:26    01/12/08
    MCPTA088    44 I     CLM      10:15:35    01/12/08    555129876A 50294869502345
    MCPTA056    51 U     CLM      15:42:23    01/12/08    555843467A 50279220730626
    MCPTA013    57 I     CLM      21:39:57    01/12/08
```

It is best practice to review the security violation report the day after it is generated, or the day after violations were committed. This will allow security administrators to follow-up on violations in a timely manner while knowledge of any incidents is still fresh in the minds of users and their supervisors. Some organizations may not have the resources to perform a review this frequently. In this case, security administrators are encouraged to perform reviews at a frequency that still allows users and their supervisors to provide timely insight into the intent of the activity performed.

[4] Business partners using FISS 'internal' security will note that FISS report #FSSB9310 contains an extra column: 'Log Type'. Log entries that denote security violations will have a value of 'VIOLATION' in the 'Log Type' column. Other activity appearing on the FSSB9310 report should be ignored for violation monitoring purposes.

In addition to the individual review of the daily security violations reports, all reports for a multiple-day period should be compared as part of trending analysis. The period over which trending should occur will be specific to each organization's situation, refer to examples of violations that can be identified by trending analysis in the Background section of this whitepaper.

Using the strategies and criteria developed to identify suspicious events, review the report and identify the violations requiring follow-up. Consider the following examples that illustrate the strategies discussed in the Background section above:

Table 2 Example Criteria for Identifying Suspicious Events

Strategy	Sample Criteria	Follow-up required?
Setting a threshold	Users who commit more than three violations on a single day will have their violations investigated.	The activity of one user would require follow up. In the example report above, user MCPTA088 committed five violations, greater than the three violation threshold defined.
Targeting higher-risk violations	Any attempts to update a financial transaction that resulted in a violation will be investigated. Any violations committed by claims processing staff outside of normal business hours will be investigated.	The activity of two users would require follow up. In the example report above, user MCPTA056 attempted to update a record using menu 51. User MCPTA013 committed a violation at 9:39pm, after business hours. Based on the targeting criteria specified, both of these attempts would require follow-up.
Trending	Users who commit violations on more than two days per week will be investigated, regardless of the types of violation or the quantity of violations.	The activity on one additional user may require follow-up. In the example report above, user MCPTA012 has committed two violations, however the user does not meet our threshold of three violations or our target criteria of attempting an update. If this user were to commit a violation on another day during the trending period, the violations would require follow-up.

Document the violations that require follow-up. This can be done on a hardcopy of the report itself or in an electronic equivalent. As the security administration staff will need to correspond with other staff regarding these violations, possibly taking several days, a tracking spreadsheet or database should be used. The tracking spreadsheet should include the details of each violation identified for follow-up, the status of the investigation, and the outcome.

The FSSB9311 report for each day should be maintained along with a record of who performed the review and the date on which the review was conducted.

Step 2: Investigate on suspicious events

The security administrator's review of the FSSB9311 report identifies suspicious events that require additional follow-up and explanation. It is important to understand what the user was trying to accomplish when the violations were committed, and to have this explanation validated

by the person responsible for supervising and assigning work to the user. Suspicious events for which an explanation is not sufficient or is not available should be treated as a security incident and escalated to security management for further investigation in accordance with the organization's incident response plan. Security Violation monitoring procedures should document the process used for investigating suspicious events.

The application security administrator should investigate all violations that meet the criteria established in Step 1 above, including violations committed by provider user IDs, system-use IDs, and all other IDs that may not be assigned to a specific employee. If, based on security management discussion or the results of security violation investigations, it becomes apparent that certain violations will occur in the normal course of operations, it may be acceptable to not investigate future instances of the violation. The exception should be well documented in the criteria for identifying security violations, and the exception should be periodically reviewed. For example, if a known system issue were to cause a violation to be recorded each time a user attempts to access a specific system report to which they have been granted access, the resulting violations would not denote a suspicious event and would not need to be investigated on a recurring basis. An explanation of the violation should be noted in the monitoring criteria, along with a date of expected fix by the shared system maintainer. After the expected fix date, the exception should be removed from the criteria for follow-up and future violations of that type investigated.

The security administrator should document events on a standard form detailing the following:

- Date on which the investigation was initiated.
- Details of the violations performed by the user and identified during a review of the security violation reports.
- User id and name of the user who performed the violations. If the activity was performed by a machine or system-use user ID, the name of the person responsible for administering the ID should be noted on the form.
- Position or job responsibility of the employee who performed the violation.
- Supervisor or manager to whom the user who committed the violations reports.
- An area for the user who committed the violations to explain why the violations occurred.
- An area for the user's supervisor to provide any additional information about why the violation occurred or corrective steps taken with the user.
- An area for the security administrator to note any further action taken, such as additional research or escalation to security management.
- Sign-off by the user who committed the violations, their supervisor, the security administrator, and the application business owner.

Forms used for documenting investigations may be paper-based, electronic, or part of a database/workflow solution. Whichever method is used to complete the form, the completed investigation form must contain the above information and be maintained for subsequent review.

Once a suspicious event has been documented on the standard investigation form, the form should be distributed to the user who committed the violation, the user's supervisor or manager, and the FISS system business owner. If the volume of investigations makes it impractical for the FISS system business owner to review all investigations at the time of the investigation, a report of investigations conducted over a period of time may be prepared by the security administrator and reviewed by the business owner on a periodic basis.

A standard deadline for reviewing and completing the form should be set. This deadline gives sufficient time to review and complete the form, however it should be short enough to allow for further investigation in a timely manner while log and other tracking data is still available. For example, if a user is given 10 calendar days to respond to an investigation of a suspicious event performed seven days ago, the security administrator could expect to receive the user's explanation of the event 17 days after the violation occurred, assuming the form is received on time. If application system logs are only maintained for 14 days, the security administrator would not have sufficient data available to further investigate the event should the user's explanation be insufficient.

An escalation process should be put into place for users who fail to respond to investigations by the deadline specified. The consequences of non-compliance and timetable for escalating through each step of the process will vary based on organizational needs, however the process should recognize the urgency of security monitoring and the need to understand why suspicious events are taking place. Following are some suggested actions to take for users or supervisors who fail to complete their investigation forms:

- Resend the investigation form to the user, their supervisor, and the next senior level of management. In the explanation accompanying the form, stress that this is the second request for the form's completion and provide a quicker return deadline.
- Revoke or suspend the account of the user who committed the access violation. Before reactivating the account, require the completed investigation form be returned to the security administrator. Alert the user's supervisor of the user account's suspension.
- Take action in accordance with organizational policy for progressive employee discipline commensurate with an Information Technology Rules of Behavior violation.

Completed investigation forms should be reviewed by the FISS system business owner and security administrator for appropriateness. The business owner should evaluate the business need for the user to have attempted the action described in the explanation, while the security administrator should note any system concerns or any recurring violation trends. If either the business owner or the security administrator is not satisfied with the responses provided, the form should either be returned to the user's supervisor for additional information, or escalated to security management for further investigation as a security incident. These reviews should be documented on the tracking spreadsheet discussed in Step 1 or on the form itself.

Step 3: Document the steps taken

As noted above, all aspects of the violation monitoring review should be documented on either standardized paper-based or electronic forms. One complete review cycle should generate the following documentation:

- Daily FSSB9311 report
- Evidence that the FSSB9311 report has been reviewed, including who reviewed it and the date on which it was reviewed.
- A list of suspicious events requiring follow-up identified on the FSSB9311 report or reports and an explanation of how each was resolved.
- Completed investigation forms for each suspicious event showing the violations identified for follow-up, explanations from the user who performed the violation and their supervisor.
- Evidence that the security administrator and FISS system business owner have reviewed the investigation forms and taken any other necessary action.
- Any other documentation presented to or generated by security management in support of the security violation monitoring process.

A good security violation monitoring program can generate a sizeable amount of documentation. To verify all documentation is properly received and completed, a Quality Assurance (QA) review should be integrated into the security violation monitoring process. This process should be completed by someone other than the security administrator who reviewed the FSSB9311 report and sent out the investigation forms.

As part of the QA review, the reviewer should verify that all necessary types of documentation have been maintained to provide auditors or law enforcement officials evidence of a review of the security violation report and that suspicious events have been correctly identified in accordance with the organization's criteria. The reviewer should also verify that all suspicious events have been investigated and supported with a completed investigation form. If any documentation is found to be missing or insufficient, the QA reviewer or security administrator should complete these aspects of the review and note why the documentation was not initially completed. The completion of the QA review should be documented with the other documentation maintained to evidence the security violation review.

1.2 CARRIERS AND PART A/B MACS USING THE MCS SHARED SYSTEM

Step 1: Review security violation reports

On a regular basis, the application security administrator should obtain MCS standard report H99RCRVL[5], the MCS System Violation Violations report. This report is generated daily and contains every instance where a clerk received a security violation message. The report is sorted by department, then by clerk last name, clerk first name, clerk ID, and the screen mnemonic or transaction where the violation occurred.

[5] Business partners using FISS 'internal' security will note that FISS report #FSSB9310 contains an extra column: 'Log Type'. Log entries that denote security violations will have a value of 'VIOLATION' in the 'Log Type' column. Other activity appearing on the FSSB9310 report should be ignored.

Figure 2 Example H99RCRVL Report

```
REPORT ID: H99RCRVL                MCS QUALITY ASSURANCE         JANUARY 07, 2008        PAGE:   1
                                   SYSTEM VIOLATION REPORT
                                      DEPARTMENT 111
LAST NAME       FIRST NAME     CLERK ID  SCREEN/FUNC TRAN ID  DATE/TIME      MESSAGE
ADKINS          SALLY           PTB001     FT         MT7M    01/07/08 16:41 M218  H99X7TK0  NOT
AUTHORIZED
                                                                          TOTAL VIOLATIONS  =
JEFFERSON       FRED            PTB038     CLAM       SB4M    01/07/08 11:56 USER NOT AUTHORIZED
JEFFERSON       FRED            PTB038     CLAM       SB4M    01/07/08 12:01 USER NOT AUTHORIZED
                                                                        TOTAL VIOLATIONS  =
SMITH           JOHN            PTB014     PSUP       SB4M    01/07/08 09:21 USER NOT AUTHORIZED
SMITH           JOHN            PTB014     VE         SB4M    01/07/08 09:22 USER NOT AUTHORIZED
SMITH           JOHN            PTB014     V1         SB4N    01/07/08 09:21 USER NOT AUTHORIZED
SMITH           JOHN            PTB014     V2         SB4M    01/07/08 09:22 USER NOT AUTHORIZED
SMITH           JOHN            PTB014     V3         SB4M    01/07/08 09:22 USER NOT AUTHORIZED
                                                                        TOTAL VIOLATIONS  =   5
WILLIAMS        BOB             PTB083     FMM        SB4M    01/07/08 03:04 USER NOT AUTHORIZED
                                                                        TOTAL VIOLATIONS  =    1
```

It is best practice to review the security violation report on the day that it is generated, or the day after violations were committed. This will allow security administrators to follow-up on violations in a timely manner while knowledge of any incidents is still fresh in the minds of users and their supervisors. Some organizations may not have the resources to perform a review this frequently. In this case, security administrators are encouraged to perform reviews at a frequency that still allows users and their supervisors to provide timely insight into the intent of the activity performed.

In addition to the individual review of the daily security violations reports, all reports for a multiple-day period should be compared as part of trending analysis. The period over which trending should occur will be specific to each organization's situation, refer to examples of violations that can be identified by trending analysis in the Background section of this whitepaper.

Using the strategies and criteria developed to identify suspicious events, review the report and identify the violations requiring follow-up. Consider the following examples that illustrate the strategies discussed in the Background section above:

Table 3 Example Criteria for Identifying Suspicious Events

Strategy	Sample Criteria	Follow-up required?
Setting a threshold	Users who commit more than three violations on a single day will have their violations investigated.	The activity of one user would require follow up. In the example report above, user PTB014 committed five violations, greater than the three violation threshold defined.
Targeting higher-risk violations	Any attempts to update a financial transaction that resulted in a violation will be investigated. Any violations committed by claims processing staff outside of normal business hours will be investigated	The activity of two users would require follow up. In the example report above, user PTB001 attempted to update a transaction on the Financial Transaction Screen. User PTB083 committed a violation at 03:04am, after business hours. Based on the targeting criteria specified, both of these attempts would require follow-up.

Strategy	Sample Criteria	Follow-up required?
Trending	Users who commit violations on more than two days per week will be investigated, regardless of the types of violation or the quantity of violations.	The activity on one additional user may require follow-up. In the example report above, user PTB038 has committed two violations, however the user does not meet our threshold of three violations or our target criteria of attempting an update. If this user were to commit a violation on another day during the trending period, the violations would require follow-up.

Document the violations that require follow-up. This can be done on a hardcopy of the report itself or in an electronic equivalent. As the security administration staff will need to correspond with other staff regarding these violations, possibly taking several days, a tracking spreadsheet or database should be used. The tracking spreadsheet should include the details of each violation identified for follow-up, the status of the investigation, and the outcome.

The H99RCRVL report for each day should be maintained along with a record of who performed the review and the date on which the review was conducted.

Step 2: Investigate on suspicious events

The security administrator's review of the H99RCRVL report identifies suspicious events that require additional follow-up and explanation. It is important to understand what the user was trying to accomplish when the violations were committed, and to have this explanation validated by the person responsible for supervising and assigning work to the user. Suspicious events for which an explanation is not sufficient or is not available should be treated as a security incident and escalated to security management for further investigation in accordance with the organization's incident response plan. Security Violation monitoring procedures should document the process used for investigating suspicious events.

The application security administrator should investigate all violations that meet the criteria established in Step 1 above, including violations committed by provider user IDs, system-use IDs, and all other IDs that may not be assigned to a specific employee. If, based on security management discussion or the results of security violation investigations, it becomes apparent that certain violations will occur in the normal course of operations, it may be acceptable to not investigate future instances of the violation. The exception should be well documented in the criteria for identifying security violations, and the exception should be periodically reviewed. For example, if a known system issue were to cause a violation to be recorded each time a user attempts to access a specific system report to which they have been granted access, the resulting violations would not denote a suspicious event and would not need to be investigated on a recurring basis. An explanation of the violation should be noted in the monitoring criteria, along with a date of expected fix by the shared system maintainer. After the expected fix date, the exception should be removed from the criteria for follow-up and future violations of that type investigated.

The security administrator should document events on a standard form detailing the following:

- Date on which the investigation was initiated.

- Details of the violations performed by the user and identified during a review of the security violation reports.
- User id and name of the user who performed the violations. If the activity was performed by a machine or system-use user ID, the name of the person responsible for administering the ID should be noted on the form.
- Position or job responsibility of the employee who performed the violation.
- Supervisor or manager to whom the user who committed the violations reports.
- An area for the user who committed the violations to explain why the violations occurred.
- An area for the user's supervisor to provide any additional information about why the violation occurred or corrective steps taken with the user.
- An area for the security administrator to note any further action taken, such as additional research or escalation to security management.
- Sign-off by the user who committed the violations, their supervisor, the security administrator, and the application business owner.

Forms used for documenting investigations may be paper-based, electronic, or part of a database/workflow solution. Whichever method is used to complete the form, the completed investigation form must contain the above information and be maintained for subsequent review.

Once a suspicious event has been documented on the standard investigation form, the form should be distributed to the user who committed the violation, the user's supervisor or manager, and the MCS system business owner. If the volume of investigations makes it impractical for the MCS system business owner to review all investigations at the time of the investigation, a report of investigations conducted over a period of time may be prepared by the security administrator and reviewed by the business owner on a periodic basis.

A standard deadline for reviewing and completing the form should be set. This deadline gives sufficient time to review and complete the form, however it should be short enough to allow for further investigation in a timely manner while log and other tracking data is still available. For example, if a user is given 10 calendar days to respond to an investigation of a suspicious event performed seven days ago, the security administrator could expect to receive the user's explanation of the event 17 days after the violation occurred, assuming the form is received on time. If application system logs are only maintained for 14 days, the security administrator would not have sufficient data available to further investigate the event should the user's explanation be insufficient.

An escalation process should be put into place for users who fail to respond to investigations by the deadline specified. The consequences of non-compliance and timetable for escalating through each step of the process will vary based on organizational needs, however the process should recognize the urgency of security monitoring and the need to understand why suspicious events are taking place. Following are some suggested actions to take for users or supervisors who fail to complete their investigation forms:

- Resend the investigation form to the user, their supervisor, and the next senior level of management. In the explanation accompanying the form, stress that this is the second request for the form's completion and provide a quicker return deadline.
- Revoke or suspend the account of the user who committed the access violation. Before reactivating the account, require the completed investigation form be returned to the security administrator. Alert the user's supervisor of the user account's suspension.
- Take action in accordance with organizational policy for progressive employee discipline commensurate with an Information Technology Rules of Behavior violation.

Completed investigation forms should be reviewed by the MCS system business owner and security administrator for appropriateness. The business owner should evaluate the business need for the user to have attempted the action described in the explanation, while the security administrator should note any system concerns or any recurring violation trends. If either the business owner or the security administrator is not satisfied with the responses provided, the form should either be returned to the user's supervisor for additional information, or escalated to security management for further investigation as a security incident. These reviews should be documented on the tracking spreadsheet discussed in Step 1 or on the form itself.

Step 3: Document the steps taken

As noted above, all aspects of the violation monitoring review should be documented on either standardized paper-based or electronic forms. One complete review cycle should generate the following documentation:

- Daily H99RCRVL report.
- Evidence that the H99RCRVL report has been reviewed, including who reviewed it and the date on which it was reviewed.
- A list of suspicious events requiring follow-up identified on the H99RCRVL report or reports and an explanation of how each was resolved.
- Completed investigation forms for each suspicious event showing the violations identified for follow-up, explanations from the user who performed the violation and their supervisor.
- Evidence that the security administrator and MCS system business owner have reviewed the investigation forms and taken any other necessary action.
- Any other documentation presented to or generated by security management in support of the security violation monitoring process.

A good security violation monitoring program can generate a sizeable amount of documentation. To verify all documentation is properly received and completed, a Quality Assurance (QA) review should be integrated into the security violation monitoring process. This process should be completed by someone other than the security administrator who reviewed the H99RCRVL report and sent out the investigation forms.

As part of the QA review, the reviewer should verify that all necessary types of documentation have been maintained to provide auditors or law enforcement officials evidence of a review of

the security violation report and that suspicious events have been correctly identified in accordance with the organization's criteria. The reviewer should also verify that all suspicious events have been investigated and supported with a completed investigation form. If any documentation is found to be missing or insufficient, the QA reviewer or security administrator should complete these aspects of the review and note why the documentation was not initially completed. The completion of the QA review should be documented with the other documentation maintained to evidence the security violation review.

1.3 DME MACS USING THE VMS SHARED SYSTEM

Step 1: Review security violation reports

On a regular basis, the application security administrator should obtain VMS standard report SE5001[6], the VMS Security Violation Report. This report is generated daily lists all the information that was written to the security violation transaction file. It is sorted by User ID.

Figure 3 Example SE5001 Report

```
CARRIER: 12345                                  CARRIER NAME                  RUN DATE: 01/08/08
PROGRAM: VMSSE500                              MEDICARE DMERC                 RUN TIME: 21:49:48
REPORT:  SE5001                          SECURITY VIOLATION REPORT            PAGE:        1
USER ID  NAME           DATE     TIME     TERM TRAN ID  Q#  QUESTION TEXT
MDME052  SALLY ADKINS   01/07/08 03:24:55 TERM VSAF     549 VIEW SECURITY FILE CHANGES?
MDME021  FRED JEFFERSON 01/07/08 09:15:41 TERM ICOR     009 AUTHORITY FOR THIS TRANSACTION?
                        01/07/08 09:15:54 TERM ICOR     009 AUTHORITY FOR THIS TRANSACTION?
MDME048  JOHN SMITH     01/07/08 HH:MM:SS TERM APPL1    442 UPDATE PAYEE RECORDS
MDME041  ROB WILLIAMS   01/07/08 HH:MM:SS TERM APPL1    193 UPDATE PROVIDER HEADER EXCEPT NAME AND ADDRESS?
                        01/07/08 HH:MM:SS TERM APPL1    193 UPDATE PROVIDER HEADER EXCEPT NAME AND ADDRESS?
                        01/07/08 HH:MM:SS TERM APPL1    193 UPDATE PROVIDER HEADER EXCEPT NAME AND ADDRESS?
                        01/07/08 HH:MM:SS TERM APPL1    193 UPDATE PROVIDER HEADER EXCEPT NAME AND ADDRESS?
                        01/07/08 HH:MM:SS TERM APPL1    193 UPDATE PROVIDER HEADER EXCEPT NAME AND ADDRESS?
```

It is best practice to review the security violation report on the day that it is generated, or the day after violations were committed. This will allow security administrators to follow-up on violations in a timely manner while knowledge of any incidents is still fresh in the minds of users and their supervisors. Some organizations may not have the resources to perform a review this frequently. In this case, security administrators are encouraged to perform reviews at a frequency that still allows users and their supervisors to provide timely insight into the intent of the activity performed.

In addition to the individual review of the daily security violations reports, all reports for a multiple-day period should be compared as part of trending analysis. The period over which trending should occur will be specific to each organization's situation, refer to examples of violations that can be identified by trending analysis in the Background section of this whitepaper.

Using the strategies and criteria developed to identify suspicious events, review the report and identify the violations requiring follow-up. Consider the following examples that illustrate the strategies discussed in the Background section above:

[6] Business partners using FISS 'internal' security will note that FISS report #FSSB9310 contains an extra column: 'Log Type'. Log entries that denote security violations will have a value of 'VIOLATION' in the 'Log Type' column. Other activity appearing on the FSSB9310 report should be ignored.

Table 4 Example Criteria for Identifying Suspicious Events

Strategy	Sample Criteria	Follow-up required?
Setting a threshold	Users who commit more than three violations on a single day will have their violations investigated.	The activity of one user would require follow up. In the example report above, user MDME041 committed five violations, greater than the three violation threshold defined.
Targeting higher-risk violations	Any attempts to update a financial transaction that resulted in a violation will be investigated. Any violations committed by claims processing staff outside of normal business hours will be investigated	The activity of two users would require follow up. In the example report above, user MDME048 attempted to update a financial screen. User MDME052 committed a violation at 03:24am, after business hours. Based on the targeting criteria specified, both of these attempts would require follow-up.
Trending	Users who commit violations on more than two days per week will be investigated, regardless of the types of violation or the quantity of violations.	The activity on one additional user may require follow-up. In the example report above, user MDME021 has committed two violations, however the user does not meet our threshold of three violations or our target criteria of attempting an update. If this user were to commit a violation on another day during the trending period, the violations would require follow-up.

Document the violations that require follow-up. This can be done on a hardcopy of the report itself or in an electronic equivalent. As the security administration staff will need to correspond with other staff regarding these violations, possibly taking several days, a tracking spreadsheet or database should be used. The tracking spreadsheet should include the details of each violation identified for follow-up, the status of the investigation, and the outcome.

The SE5001 report for each day should be maintained along with a record of who performed the review and the date on which the review was conducted.

Step 2: Investigate on suspicious events

The security administrator's review of the SE5001 report identifies suspicious events that require additional follow-up and explanation. It is important to understand what the user was trying to accomplish when the violations were committed, and to have this explanation validated by the person responsible for supervising and assigning work to the user. Suspicious events for which an explanation is not sufficient or is not available should be treated as a security incident and escalated to security management for further investigation in accordance with the organization's incident response plan. Security Violation monitoring procedures should document the process used for investigating suspicious events.

The application security administrator should investigate all violations that meet the criteria established in Step 1 above, including violations committed by provider user IDs, system-use IDs, and all other IDs that may not be assigned to a specific employee. If, based on security management discussion or the results of security violation investigations, it becomes apparent

that certain violations will occur in the normal course of operations, it may be acceptable to not investigate future instances of the violation. The exception should be well documented in the criteria for identifying security violations, and the exception should be periodically reviewed. For example, if a known system issue were to cause a violation to be recorded each time a user attempts to access a specific system report to which they have been granted access, the resulting violations would not denote a suspicious event and would not need to be investigated on a recurring basis. An explanation of the violation should be noted in the monitoring criteria, along with a date of expected fix by the shared system maintainer. After the expected fix date, the exception should be removed from the criteria for follow-up and future violations of that type investigated.

The security administrator should document events on a standard form detailing the following:

- Date on which the investigation was initiated.
- Details of the violations performed by the user and identified during a review of the security violation reports.
- User id and name of the user who performed the violations. If the activity was performed by a machine or system-use user ID, the name of the person responsible for administering the ID should be noted on the form.
- Position or job responsibility of the employee who performed the violation.
- Supervisor or manager to whom the user who committed the violations reports.
- An area for the user who committed the violations to explain why the violations occurred.
- An area for the user's supervisor to provide any additional information about why the violation occurred or corrective steps taken with the user.
- An area for the security administrator to note any further action taken, such as additional research or escalation to security management.
- Sign-off by the user who committed the violations, their supervisor, the security administrator, and the application business owner.

Forms used for documenting investigations may be paper-based, electronic, or part of a database/workflow solution. Whichever method is used to complete the form, the completed investigation form must contain the above information and be maintained for subsequent review.

Once a suspicious event has been documented on the standard investigation form, the form should be distributed to the user who committed the violation, the user's supervisor or manager, and the VMS system business owner. If the volume of investigations makes it impractical for the VMS system business owner to review all investigations at the time of the investigation, a report of investigations conducted over a period of time may be prepared by the security administrator and reviewed by the business owner on a periodic basis.

A standard deadline for reviewing and completing the form should be set. This deadline gives sufficient time to review and complete the form, however it should be short enough to allow for further investigation in a timely manner while log and other tracking data is still available. For

example, if a user is given 10 calendar days to respond to an investigation of a suspicious event performed seven days ago, the security administrator could expect to receive the user's explanation of the event 17 days after the violation occurred, assuming the form is received on time. If application system logs are only maintained for 14 days, the security administrator would not have sufficient data available to further investigate the event should the user's explanation be insufficient.

An escalation process should be put into place for users who fail to respond to investigations by the deadline specified. The consequences of non-compliance and timetable for escalating through each step of the process will vary based on organizational needs, however the process should recognize the urgency of security monitoring and the need to understand why suspicious events are taking place. Following are some suggested actions to take for users or supervisors who fail to complete their investigation forms:

- Resend the investigation form to the user, their supervisor, and the next senior level of management. In the explanation accompanying the form, stress that this is the second request for the form's completion and provide a quicker return deadline.
- Revoke or suspend the account of the user who committed the access violation. Before reactivating the account, require the completed investigation form be returned to the security administrator. Alert the user's supervisor of the user account's suspension.
- Take action in accordance with organizational policy for progressive employee discipline commensurate with an Information Technology Rules of Behavior violation.

Completed investigation forms should be reviewed by the VMS system business owner and security administrator for appropriateness. The business owner should evaluate the business need for the user to have attempted the action described in the explanation, while the security administrator should note any system concerns or any recurring violation trends. If either the business owner or the security administrator is not satisfied with the responses provided, the form should either be returned to the user's supervisor for additional information, or escalated to security management for further investigation as a security incident. These reviews should be documented on the tracking spreadsheet discussed in Step 1 or on the form itself.

Step 3: Document the steps taken

As noted above, all aspects of the violation monitoring review should be documented on either standardized paper-based or electronic forms. One complete review cycle should generate the following documentation:

- Daily SE5001 report.
- Evidence that the SE5001 report has been reviewed, including who reviewed it and the date on which it was reviewed.
- A list of suspicious events requiring follow-up identified on the SE5001 report or reports and an explanation of how each was resolved.
- Completed investigation forms for each suspicious event showing the violations identified for follow-up, explanations from the user who performed the violation and their supervisor.

- Evidence that the security administrator and VMS system business owner have reviewed the investigation forms and taken any other necessary action.
- Any other documentation presented to or generated by security management in support of the security violation monitoring process.

A good security violation monitoring program can generate a sizeable amount of documentation. To verify all documentation is properly received and completed, a Quality Assurance (QA) review should be integrated into the security violation monitoring process. This process should be completed by someone other than the security administrator who reviewed the SE5001 report and sent out the investigation forms.

As part of the QA review, the reviewer should verify that all necessary types of documentation have been maintained to provide auditors or law enforcement officials evidence of a review of the security violation report and that suspicious events have been correctly identified in accordance with the organization's criteria. The reviewer should also verify that all suspicious events have been investigated and supported with a completed investigation form. If any documentation is found to be missing or insufficient, the QA reviewer or security administrator should complete these aspects of the review and note why the documentation was not initially completed. The completion of the QA review should be documented with the other documentation maintained to evidence the security violation review.

4 DOCUMENTATION REQUIREMENTS

Each step of the violation monitoring process should be sufficiently documented to allow an individual outside of security organization to reasonably reperform the review of the security violation report and reach the same conclusions as the person who administered the review.

Step 3 of the Instructions section above lists the documentation that must be maintained to support a successful application security violation monitoring program. This documentation can be maintained in print form or electronically, however it should be readily available for CMS or external reviewers. Documentation should be retained for at least one year.

When planning a security violation monitoring review, consider the following documentation best practices:

- Reviews of violation reports and investigation forms must be documented. This could be as simple as the reviewer initialling and dating the report reviewed, or completing a tracking spread sheet that notes the report reviewed with any notes about the outcome of the review. Documentation maintained to evidence a review should include the name (or initials) of the person who performed the review, the date the review was performed, and any items noted by the reviewer requiring follow-up. If documentation is not maintained to evidence reviews, CMS and other external parties cannot conclude that a review has been completed.
- System-generated reports used during reviews to identify suspicious events must be maintained. These reports, such as the FISS FSSB9311, MCS H99RCRVL, and VMS SE5001, or similar reports, contain detail that may be used by CMS and external parties to

determine if all suspicious, as defined by policies and procedures, have been correctly identified and investigated.

Any suspicious events identified on violation reports should result in the creation of supporting documentation. In most cases, the supporting documentation will be a completed investigation form, reviewed by a user's supervisor and the security administrator. If certain suspicious events can be explained by exceptions, documented in policies and procedures, such as known system issues, the rationale for not investigating these events must still be documented along with the documentation maintained to support the daily violation review. This will prevent subsequent reviewers from questioning why documentation to support certain suspicious events appears to be missing.

After implementing a violation monitoring program, conducting a review over a selection of days will determine if adequate documentation is being maintained. For each day selected, reperform the security violation monitoring process according to documented policies and procedures. While performing this test, ask the following questions:

- Has the system-generated violation report been maintained?
- Did the reviewer correctly identify the suspicious events requiring follow-up? Are there any additional events that should have been identified according to our policies and procedures?
- Is there a completed investigation form for each suspicious event identified? If not, has some an explanation been provided as to why investigation was not performed?
- Does the explanation provided on each investigation form make sense? If any questions or requests have been made on the investigation form (e.g. a supervisor asking security to further investigate the suspicious event), have responses to these questions been documented?
- Has the shared system business owner reviewed the investigation forms or a summary of events for the time period that covers the day selected?
- Are there any incomplete aspects of the documentation that might cause an external reviewer to consider the documentation incomplete?

If this test reveals any missing, incomplete, or unclear documentation, consider revising the procedures for conducting the violation monitoring review to prevent issues in future reviews.

5 OTHER CONTROLS TO CONSIDER

1.1 SYSTEM-SPECIFIC ISSUES THAT COULD IMPACT REPORT GENERATION

FISS, MCS, and VMS are complex systems that are continually being updated. A change to a shared system may impact the ability of the system to produce violation monitoring reports or the content of reports. For example, an issue with a shared system may cause a violation to be

noted each time a user performs a set of actions, even if the user has the correct access levels for each transaction performed.

In cases such as the example above, security administrators may be able to explain why certain violations are occurring on a systemic basis and not perform additional follow-up with users and their supervisors. System issue exceptions to security violation monitoring criteria should be clearly documented with the expected date of resolution. When violations occur that can be attributed to the issue, the reason for not investigating the violations should be documented on the violation report or tracking spreadsheet. For additional information, refer to the Instructions section, Step 2 - Investigate on suspicious events.

1.1 OTHER CONTROLS THAT SUPPORT SECURITY VIOLATION MONITORING

The implementation of an Application Security Violation Monitoring program should be considered in the context of an organization's overall control environment. As a detective control, violation monitoring helps security administrators investigate violations after they have been committed. There are several preventative controls which, if implemented properly, can preclude users from committing violations and thereby reducing the number of suspicious events that administrators need to investigate. Additional controls include:

- Implementation of role-based access: When determining the levels of system access to Medicare shared systems, create a standard level of access for specific job positions or roles, not individual users. Standardizing access by role allows the organization to consistently grant user access to multiple staff performing the same job functions, minimizing the risk that an individual user will have a key level of access omitted from their user account.
- Recertification of user access: A regular review and recertification of user access to the Medicare shared systems allows supervisors to assess the appropriateness of the levels of access granted to individual users. A recertification identifies users who have changed job responsibilities and require additional changes to their access and inconsistencies between a user's access levels and their respective role-based profile. For more information about recertification of user access, refer to the CMS Whitepaper, "Fee For Service Application Access Recertification".
- Security awareness training: Prior to receiving access to the system, users should be notified that their activity is monitored and that use of the Medicare shared systems should be limited to required work-related activities. A security awareness training should discourage users from "exploring" the system, or attempting to access screens or functionality not needed to perform job duties.
- Proper systems training: Users should receive training for screens and scenarios they are expected to work within a Medicare shared system. Providing users with training reduces the number of mistakes made within the system, which can result in violations.

1.4 CUSTOM BUILT REPORTS AND MONITORING TOOLS

While each shared system produces a standard violations report, some CMS business partners may elect to create their own reporting solutions from the source data captured by the shared systems. Custom solutions allow business partners to tailor the violation information generated to match their organization's structure, policies, and procedures.

Any in-house developed solutions must be developed in accordance with an organization's Systems Development Life Cycle (SDLC), with all changes made through an effective change control process that prevents systems and security staff from making unauthorized changes. Custom solutions should be tested prior to implementation and subsequently tested with each new release of the shared systems.

A customized solution can be used to filter violations recorded by the shared system, presenting to a security administrator only the suspicious events that require follow-up according to a business partner's monitoring criteria. While this is an acceptable approach to monitoring, it is absolutely necessary to retain the underlying log data or report parsed by the custom solution as part of the documentation maintained to support the review process. The log data must be available to CMS or external reviews for use determining if the custom solution is properly identifying violations for follow-up.

1.5 SHARED SYSTEM LOGGING TOOLS

Each of the shared systems logs activity performed by users within the system. These logs can be a source of information for typical transactions performed by a user and an indication of a user's intent when a violation occurs. Additionally, the MCS and VMS systems utilize the ViPS System Auditing Function Expert (SAFE) system to capture before and after record images along with user-provided explanations for changes to many types of sensitive records and data. Refer to shared system users manuals and the SAFE User Guide for more information on these tools.

6 CONCLUSION

Monitoring security violations that are committed within the CMS shared systems provides security administrators with additional comfort over the activity performed by end users. The FISS, MCS, and VMS shared systems currently capture violations to a log file, and produce a daily report of these violations. Although prior attempts by CMS Business Partners have not always yielded successful monitoring programs, background provided in this white paper identifies common problems in approach and solutions.

An enhanced understanding of security violation monitoring processes, objectives, and concepts involved will help business partners successfully implement a manageable monitoring program. By developing a monitoring strategy that includes criteria specific to the business partner's organization, business partners will spend less time investigating low risk and explainable violations. By involving all stakeholders involved in securing the application, from end users

and their supervisors to security administrators and business owners, incorrect or inappropriate end user behaviors can be quickly identified and corrected. By implementing a Quality Assurance process, business partners can validate the effectiveness of their monitoring program prior to reviews conducted by CMS and external reviewers.

With the guidance provided in this whitepaper, CMS management and business partners will be able to implement an application security violations monitoring program as part of their controls environment, reinforcing the security and integrity of their claims processing environment.

(This Page Intentionally Blank)

APPENDIX A - GLOSSARY

ACF2	eTrust CA-ACF2 mainframe security package
CFO	Chief Financial Officers Act of 1990
CICS	IBM Customer Information Control System
CMS	Centers for Medicare & Medicaid Services
CMSR	CMS Minimum Security Requirement
CWF	Common Working File
DME	Durable Medical Equipment
EDC	CMS Enterprise Data Center
EDS	Electronic Data Systems Corporation
FI	Fiscal Intermediaries
FISCAM	Federal Information Systems Audit and Control Manual
FISS	Fiscal Intermediary Shared System
HHS	U.S. Department of Health and Human Services
ID	User Identification code
MAC	Medicare Administrative Contractors
MCS	Multi Carrier System
MMA	Medicare Prescription Drug, Improvement and Modernization Act
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PBSI	Pinnacle Business Solutions, Inc.
PwC	PricewaterhouseCoopers LLP
QA	Quality Assurance
RACF	IBM Resource Access Control Facility mainframe security package
SAFE	System Auditing Function Expert
SDLC	System Development Life Cycle
VIPS	ViPS, Inc., formerly Viable Information Processing Systems
VMS	ViPS Medicare System

z/OS	IBM z/OS Mainframe Operating System

APPENDIX B - CMS Minimum Security Requirements (CMSRs)

Refer to *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, Appendix A, *CMS Minimum Security Requirements for High Impact Level Data*, for the applicable CMSRs.

Appendix C - Quick Reference: Application Security Violation Monitoring

SECURITY VIOLATIONS REPORTS

Reports vary slightly by system, however each contains standard information about each violation including the date and time of occurrence, the user ID that committed the violation, and the nature of the violation.

- **FISS:** FSSB9311
- **MCS:** H99RCRVL
- **VMS:** SE5001

STRATEGIES FOR REVIEWING REPORTS

Set a Threshold: Set a quantity of violations that may be committed before follow-up is necessary. Management can apply this threshold to the total number of violations committed by a user on a single day, or the number of times a user commits a specific type of violation. When setting a threshold, be sure that the quantity selected is low enough to identify users who are repeating a violation beyond a reasonable number of tries.

Target Higher Risk Violations: Identify the violations that pose a high risk to the organization and specifically target these violations for follow-up.

Perform Trending Analysis: Reviewing a series of daily reports may help to identify a trend of violations over time. A trending analysis over a series of days could note the repeated violations performed by the user. Trending can also be used to identify other types of repetitive violations, such as violations that recur on specific days of the week, at certain times of day, or when certain staff are on vacation.

PREPARING FOR A REVIEW

Identify Stakeholders: Engage all stakeholders who will be affected by an application security violation monitoring program, for example: security management team, application security administrator, business owner, employee's supervisor, etc.

Identify a Strategy for Identifying Violations for Follow Up: Consider and document criteria for identifying security violations requiring follow-up: set a threshold, target higher risk violations, and trending analysis.

INSTRUCTION

Step 1: Review Security Violations Reports

Application security administration should regularly receive the applicable application security violations reports (Recommended frequency: daily). Using strategies and criteria for identifying suspicious events, review report and identify those violations requiring follow up. In addition, reports for a multiple day period should be compared as part of trending analysis.

Step 2: Investigate Suspicious Events

Understand what the user was trying to accomplish when the violations were committed, and have the explanation validated by the person responsible for supervising and assigning work to the user. Suspicious events for which an explanation is not sufficient or is not available should be treated as a security incident and escalated to security management for further investigation in accordance with the organization's incident response plan. The security administrator should document events requiring on a standard form.

Step 3: Document the Steps Taken

One complete review cycle should generate the following documentation:

- Security violations report.
- Evidence that the report was reviewed, who reviewed it, and the date it was reviewed
- A list of suspicious events requiring follow-up identified in the report or reports and an explanation of how each was resolved.
- Completed investigation forms for each suspicious event showing the violations identified for follow-up, explanations from the user who performed the violation and their supervisor.
- Evidence that the security administrator and application business owner have reviewed the investigation forms and taken any other necessary action.
- Any other documentation presented to or generated by security management in support of the security violation monitoring process.

(This Page Intentionally Blank)