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

CMS Security Whitepaper:

SCF/SuperOp Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *SCF/SUPEROP WHITEPAPER,* VERSION 2.0

1) Converted baseline version dated April 4, 2007 to updated CMS style format.
2) Moved Section 1, Introduction, from before Table of Contents to after.
3) Changed "Note" in Section 2, Summary of Results of SCF and SuperOp Review, subsection "SuperOp –FISS/VMS" to footnote.
4) Updated FISCAM footnote reference in Section 3, Components of Effective Change Control, to new FISCAM Exposure Draft version.
5) Added titles to Figure 1, 2, 3, 4, 5, and 6 in Appendix A.
6) Added titles to Figure 7 and Table 1 in Appendix B.
7) Removed former Appendix C CSRs and added pointer to new CMSRs.
8) Added titles to Figures 8 and 9 in Appendix D.
9) Updated the CMSR and FISCAM references in Appendix F.
10) Added a reference in Section 4 to the new SCF Access Controls whitepaper and updated the Appendix C and F CMSR references.

SUMMARY OF CHANGES IN *SCF/SUPEROP WHITEPAPER,* VERSION 1.0

Table 1 Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

(This Page Intentionally Blank)

1 INTRODUCTION

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 paper 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 this agency. 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).

In 2006, a review of change control management procedures and controls for applications using automated program procedures ("scripts") in addition to standard claims systems (FISS, MCS and VMS), to process claims was conducted over Medicare contractors. The review found that Carriers, Fiscal Intermediaries, and Medicare Administrative Contractors (MACs) were using and customizing such applications, although many lacked strong change control management procedures to ensure proper documentation, authorization, and testing prior to implementation into production.

The most pertinent of these applications are the System Control Facility (SCF), processing Part B claims in combination with MCS, and SuperOp, processing Part A and DME claims in combination with FISS and VMS, respectively. Both applications allow for the processing of a substantial amount of claims without human intervention, thus more effectively and consistently. Features allow users to tailor either SCF or SuperOp to be able to meet the specific needs, e.g., policies, mandates, or guidelines, of each contractor's environment. However, customization introduces the possibility of error and processing inaccuracies. Through the implementation of effective change control management procedures the likelihood of unauthorized or erroneous changes to claims can be significantly limited.

To assist Medicare contractors in determining the appropriateness and effectiveness of controls over SCF, SuperOp, and other similar applications, this white paper has been created. Topics presented within this document include the following:

- background of the SCF and SuperOp applications;
- results of the review of change management procedures and controls;
- components of effective change management procedures; and,
- additional controls to consider when such applications are being used.

Having the above information at hand, CMS management and business partners can then ensure that key controls pertaining to the management and customization of applications using

automated scripts to process claims are fully incorporated into CMS' current control environment.

Quick and accurate processing techniques for claims benefits all parties involved. Fewer suspended claims, reduced processing time, and less staff involvement equate to higher productivity, performance, and customer satisfaction. Therefore the business justification behind an application with the ability to use scripts to process claims and the potential to achieve effective results is easy to recognize. However, it is important to understand that strong controls and monitoring are needed to continuously produce expected results.

CMS contractors most notably use the following applications, both provided by CMS maintainers, to assist with automated claims processing:

System Control Facility (SCF)

SCF allows the Carrier to define, modify, and delete policies and procedures, or rules that define Medicare processing. SCF uses system control language, an IF…THEN based language, to script rules associated with a specific edit or audit. MCS then reads and takes specific actions on a claim. Through the use of specific rules, SCF has the ability to modify claim data and/or claim disposition. This is most commonly used in MCS to establish specific edits and audits, although it is also used for other functions, such as defining supplemental insurer crossover rules.

SuperOp

SuperOp is a program within FISS and VMS, which allows the Fiscal Intermediary, MAC and DME to use "smart language" to define environment-specific events. Within the event, rules are attached with guidance on how to take action on claims that have met pre-defined criterion. During claims processing, as an event criterion is met, SuperOp will be invoked and will automatically resolve the audit or edit accordingly.

In both instances, processing logic acts as an "automated operator resolving claims" consequently modifying claims without physically being reviewed or worked by a claims operator. Although both applications (SCF and SuperOp) are provided by CMS maintainers, Carriers, Fiscal Intermediaries, and MACs are able to customize processing logic to meet environmental requirements. If an event or rule was not properly controlled during creation or modification a significant number of claims could be incorrectly processed. These functions allow for claims information to be changed without full control over the programs or complete logging and review of the changes made by these two add on systems. Management should ensure an appropriate balance of controls, specifically those in change control management, to make certain there is less than a remote likelihood that a material misstatement of financial statement could arise from improper claims processing because of the use of SCF or SuperOp.

In 2006, a review of change control management procedures and controls for applications using scripts to process claims was conducted over Medicare contractors. The evaluation noted four key areas for which Carriers and Fiscal Intermediaries lacked pervasive controls surrounding the targeted applications (SCF and SuperOp):

- Policies and procedures

- Evidence of formal testing
- Evidence of formal approval
- Proper segregation of duties

Medicare contractors should ensure that applications with the ability to alter claims are subjected to formal change management policies and procedures. Establishing controls over modifications is critical to ensure applications operate as intended and are authorized. Although changes may appear inconsequential, if done improperly, each or a combination of changes can have a significant impact on the reliability of data and programs.

2 SUMMARY OF RESULTS OF SCF AND SUPEROP REVIEW

During the FY 2006 evaluation performed under section 912 of the Medicare Prescription Drug, Improvement and Modernization Act (MMA) of 2003, change control management procedures and controls for applications using automated scripts to process claims were reviewed. The examination consisted of the following procedures for each Carrier, Fiscal Intermediary, and MAC, specific to SCF and SuperOp modifications:

- Inspected evidence supporting formal change control management procedures;
- Identified key change control management elements, including documentation, testing, approval, etc., within procedures;
- Inspected supporting documentation for a sample of SCF and SuperOp modifications; and,
- Inspected evidence of key change control management elements, including testing and approval, for each sampled modification.

The evaluation noted that all Medicare contractors are using either SCF or SuperOp to varying degrees, but without full control over the changes being made using these systems. Specifically, testing revealed the following:

SCF - MCS[*]

Below are the top four deficiencies noted at contractors reviewed:

- Carriers did not have robust policies and procedures to dictate action over changes made to the SCF application;
- Carriers with policies and procedures did not require testing and/or approval of changes made the SCF application;

[*] Testing was not conducted consistently across all contractors during the evaluation for segregation of duties. However, during inquiry with contractors we noted weaknesses in this process.

- Carriers were not able to produce supporting documentation to indicate all changes selected for review were sufficiently tested; and,
- Carriers were not able to produce supporting documentation to indicate all changes selected for review were approved.

SuperOp - FISS/VMS*

Below are the top four deficiencies noted at contractors reviewed:

- Fiscal Intermediaries and MACs did not have robust policies and procedures to dictate action over changes made to the SuperOp application;
- Fiscal Intermediaries and MACs with policies and procedures did not require testing and/or approval of changes made the SuperOp application;
- Fiscal Intermediaries and MACs were not able to produce supporting documentation to indicate all changes selected for review were sufficiently tested; and,
- Fiscal Intermediaries and MACs were not able to produce supporting documentation to indicate all changes selected for review were approved.

The evaluation noted many of the same issues across all Medicare contractors, regardless of the application being used. The following were noted in the evaluation:

Policies and procedures were not robust:

- Formal change management procedures specific to SCF and SuperOp did not exist;
- Policies and procedures were in draft and had not been approved by management and incorporated into the organization;
- High level procedures did not provide sufficient details outlining requirements for approval, testing, and documentation retention for different types of changes (for example, CMS mandated, emergency, minor, major, changes etc.); and
- Medicare contractors did not require SCF or SuperOp changes to go through the formal change management process and therefore require approval and/or testing.

Testing documentation was not sufficient:

- Supporting documentation for changes was not consistently maintained;
- Supporting documentation for changes did not comply with documented policies and procedures; and
- Changes were not consistently tested prior to implementation into production.

Approval documentation was not sufficient

- Supporting documentation for changes was not consistently maintained;

- Supporting documentation for changes did not comply with documented policies and procedures;
- Changes were not consistently approved prior to implementation into production; and
- Changes were reviewed after being moved to production and already processing claims.

Overall, Carriers, Fiscal Intermediaries and MACs do not have strong change management controls over modifications to the SCF or SuperOp applications. In many cases, this stems from not having a strong basis for such controls. A formal, documented policy and procedure that helps to ensure modifications are properly approved, tested, and maintained was not in place. In other cases, policies and procedures were simply not being enforced.

3 COMPONENTS OF EFFECTIVE CHANGE CONTROL

Change control management procedures are adopted to ensure modifications are authorized and allow applications to produce expected results. An effective change control management process includes instituting formal policies and procedures ensuring that all modifications are appropriate and properly authorized, tested, and documented. Procedures may vary depending on the type and significance of the modification, but it is essential that every modification is a part of the process.

For all Medicare Contractors, CMS Change Request 3011, effective August 1, 2004, should be incorporated into each contractor's formal change control management process. This publication defines the testing requirements for Medicare entities and should be used when creating and updating each contractor's policies and procedures.

The following sections discuss some of the key components for incorporating an effective change control management process into an organization.

Documented Policies and Procedures

Contractors should first adopt a high level, organization wide change control management policy. The policy will introduce the change control management process and should set the tone from management that all modifications (whether they be system software, application, CMS mandated, local, etc.) are to be authorized, tested, and approved. Policies may also provide applicable standards, roles and responsibilities, possible consequence for non-compliance, and additional documentation to reference. The parent policy is then put into practice through detailed procedures which provide guidance throughout the entire process. Change control management procedures should be clear and concise and should walk a user step-by-step through the life of the modification. Procedures for modifications may be included in the System Development Life Cycle (SDLC) methodology or may be stand-alone documents. Regardless of the method chosen, procedures must be available to dictate the process for all types of changes the organization may encounter.

Both policies and procedures should be periodically reviewed by appropriate parties to ensure each reflects the current environment. In addition, staff that will be affected by the creation of or any updates made to the policies and procedures should be trained to ensure understanding.

The remainder of the topics in this section will discuss key components of effective change control management. These elements should be documented in the policies and procedures as discussed above. The following sections will discuss the components and provide examples as they relate to SCF and SuperOp modifications.

Authorization Process

The first element of a change control management procedure is to ensure that potential modifications are subject to an authorization process. Documented procedures should provide guidance for:

- Authorization documentation and communication: Standardized change requests should be used to ensure requests are clearly communicated and pertinent information is captured and approved. Change requests can be forms, emails, or memos maintained in either a paper or electronic format. Change requests should include any information that will assist in the approval or rejection of a modification request. They should include, at a minimum, requestor information, description of the modification, priority of modification, expected results, what applications are to be effected, how claims processing will be affected and how many claims will be affected once the modification has occurred. Indication of approval, such as a signature, should also be maintained with the authorization documentation.

- Authorization prioritization: Contractors should have a methodology for assigning a priority level to changes. Rankings suggestions include a) high, medium, or low b) a number scale, or c) standard, urgent, or emergency. Contractors can pick their own classification definitions as long as they are consistently applied. The prioritization will be used to determine when a modification can be implemented.

- Authorization permission: A detailed list of approver positions and the types of modifications each is allowed to authorize should be maintained. Authorizations should be obtained only from those appropriate individuals, for example SCF modifications should be authorized by MCS end users and management as opposed to FISS or VMS management. Other items to consider include the need for a change control board and how many authorizations are needed.

An appropriate retention policy for change requests should be determined within the organization, but throughout the life of the organization is strongly suggested.

Testing

A formal process for testing modifications prior to implementation into production is essential to ensure processing is not negatively impacted and expected results are obtained. This is especially important for SCF and SuperOp modifications because they have the potential to process a large amount of claims without human intervention (and therefore, without review.) The testing environment should model that of the production environment and test data should be used. A wide variety of tests exist and the extent of testing can vary depending on the nature of

the modification. As with the authorization process discussed above, contractors should also consider creating a classification scheme for testing. A formal classification will help determine the amount of testing and documentation needed for different types of tests. For the purpose of this paper, three classifications will be used: Major, Minor, and Emergency.

Major modifications: "For new systems being developed or major system enhancements, testing will be extensive, generally progressing through a series of test stages that include (1) testing individual program modules (unit testing), (2) testing groups of modules that must work together (integration testing), and (3) testing an entire system (system testing)."1

For major modifications, tests should be robust and inclusive of all areas and applications affected by the modification. In general, a contractor should perform and document the following during the testing phase:

- Test Plan: Provide a high level guidance on how to perform testing and the components of the testing. This plan may include test cases / scenarios, test conditions, expected test results and success criteria, and the name of the person or department responsible for each test. Test plans must be comprehensive to include cases for each of the needed scenarios, for example unit, integration, system, regression, etc.
- Documentation of the testing steps : In addition to a test plan or an alternative to a test plan, users may need to document what testing steps are performed to provide evidence for the testing. Typically the documentation of these test steps provides the users of the process with enough evidence and information that the testing procedures were performed completely and accurately.
- Testing results: Upon completion of the tests, the actual test results should be documented and compared against expected results. Any discrepancies should be highlighted for further investigation and if necessary, the appropriate program changes should be made and re-tested.
- Screen shots: Where applicable, users should obtain screen shots for relevant testing steps performed. Users should take and retain those screen shots that support their testing results.
- Evidence of Review: Upon completion of the tests, the results and documentation should be evaluated.

If testing cannot be performed by the user, or the testing cannot be evidenced because of system limitations or based on the nature of the change, contractors should consider documenting the reason for not having the test evidence in sufficient detail as to why the testing, or evidence of testing, cannot be maintained or created.

Minor modifications: Minor modifications may be a change that is less risky in terms of the impact or a change that is recurring or very similar to other changes previously implemented. These should still require some testing because if implemented incorrectly the reliability of data and claims processing can be significantly impacted. Minor modifications should still include test plans and/or documentation of the testing steps, testing results, evidence of testing, and evidence of review as described above, albeit completed on a much lower scale. Also, sufficient

[1] *Federal Information System Controls Audit Manual* (FISCAM) Exposure Draft (GAO-08-1029G, July 2008)

testing for minor modifications may be third party verification of a before and after screenshot or third party verification of the code that will be implemented as opposed to running 200 claims through a test facility.

For example, a new SuperOp event has been required to reject lines with reason code 12345. This is a relatively simple SuperOp event to produce as the contractor must use this scenario for many other reason codes throughout the year and even has an example of the code previously written. A sufficient test for this case would be to have a third party verify the programming code intended to be put into production to ensure the logic will in fact reject lines with reason code 12345 (as opposed to 12435).

Emergency Modifications: Sometimes an emergency modification must be implemented in order to keep a critical application processing. Since these types of modifications typically are not able to follow the change control management authorization and testing process, it is important to have additional controls in place to ensure the quick fix does not compromise the integrity of the data or other systems. An emergency modification procedure should be established and documented to reduce the risk of improper modifications. It should specify the following:

- when emergency software changes are warranted;
- who may authorize emergency changes;
- how emergency changes are to be documented; and
- within what period after implementation the change must be tested and approved.2

Based on the period specified in the procedures, normal change control management procedures should be retroactively applied to include authorization and appropriate testing. Management should periodically review logs of emergency modifications to ensure the proper procedures are conducted and documentation is maintained.

Regardless of the amount of testing required, once it has been completed, management should review the adequacy of the test results and documentation. Once satisfied, a final independent approval should be obtained and documented with the original modification request (e.g., change request). This approval will indicate that the change is ready to become fully functional in production.

Implementation

After proper testing and approval, a modification can be moved into production. The movement of the modification between environments should be restricted by access controls (please see section IV) and should be independent of individuals with computer programming roles and responsibilities. A periodic review of post-implementation modifications should be done by management, or an appropriate independent party, to ensure proper segregation of duties was practiced for modifications.

[2] *Federal Information System Controls Audit Manual (FISCAM)* Exposure Draft (GAO-08-1029G, July 2008)

4 OTHER CONTROLS TO CONSIDER

In addition to change control management, Medicare contractors must also ensure that they have proper access controls in place and are continuously monitoring changes to the application. It is important for the contractors to know who has the ability to create and modify events and rules, ensure privileges are appropriate for roles and responsibilities, and to continuously monitor such individuals. Each contractor is responsible for establishing and documenting security controls for their respective application's maintenance functions.

SCF - MCS

SCF security is controlled through the CLERK file, via the SCF security field. An individual must have the SCF security field set to "Y" (Yes, has authorization to update) on the CLERK file in order to have access to SCF Maintenance/Utilities functions; allowing for the creation, modification, and deletion of rules. "N" (No authorization to update) is the default. (Refer to the *SCF Access Controls* whitepaper published in February 2009 for additional guidance on restricting access.)

One of the first steps to controlling access to SCF is to identify users with "Y" in the SCF security field. There are at least two ways of doing this:

- Review the "Clerk Record Update" screen for individual users and determine if a "Y" is in the SCF security field under "File Maintenance Authorization."
- Run the "Clerk File Security Report (H99PCSEC)," a daily report that details out each clerk on the clerk file and their associated security levels.

Once those individuals have been identified it is important to review each person to determine if they have a business need for such privileges and ensure that it does not cause a segregation of duties concern. Note that the MCS application is set up such that direct access (above inquiry) is required for GDX datasets because access to these datasets is required to allow users to update SCF tables. Although required for production, whenever individuals have direct access to data, logging and audit trails must be enabled through the contractor's security package (e.g., RACF, ACF2 or TopSecret). Documented policies and procedures for logging and reviewing transaction logs should be established and implemented. For more information regarding direct data access, refer to Joint Signature Memorandum 07002 and the Direct Access to Data Whitepaper presented 02/07/07 at the CMS Security Conference.

SuperOp - FISS

FISS SuperOp security is controlled through the Operator Control File, via switches that control the authorization level to different SuperOp components. Authorization levels to the SuperOp application are based on the value found in the "SuperOp" field on the "Operator Control System" screen. The following are potential values and a description of each:

- 1 - Inquire only
- 2 - Level 1 plus Add/Update/Inactivate/Activate/Copy/Restore events

- 3 - Level 2 plus Delete events
- 4 - Level 3 plus the ability to move an event into production

The "Operator Security List" screen can be used to identify those users with one of the authorization assignments above. This screen will list all users (using "L/ ") with SuperOp access. For each user, the screen will display the authorization switches respective to the user and the values for each switch field. Refer to Appendix B for a listing of those values.

Note: Once the list has been produced, it may be easier to understand the values listed under the "Authorization Switches" section by using the "Operator Control System" screen to look up each user individually.

Using those users identified in the "Operator Security List" it is important to review each to determine if they have a business need for such privileges and ensure that it does not cause a segregation of duties concern.

SuperOp - VMS

VMS SuperOp security is controlled through the VMS Security System (VSEC), via switches specific to "SUPR" transactions. When a user (referred to as an operator) attempts to add, delete, or update an event, the program will review the VSEC switch values to determine if the UserID has appropriate authority. In VMS the program allows separate security for different types of SuperOp transactions (e.g., express adjustment events (XADJ) and on-line quality control (VOQC)). A list of SuperOp Security Switch Values can be found in Appendix B. Of those listed, only switch 086 allows inquiry. All other listed switches allow an operator to update or delete events, move an event to production, and/or archive an event.

These multiple levels of security make it even more important to ensure only appropriate operators have access to modify SuperOp events. VMS Contractors can identify those operators by using two main reports:

- "Operator Security Detail (SE5501)" report: Using the "Operator Print System Report Parm" screen in the VSEC system (VSEC/R), a specific switch number can be entered for applicable SuperOp transactions (those listed in Appendix B). The report will then print all or a range of the operators' information for which the switch number is set to "Y" depending on the values set in the parameters. The SE5501 report will print one operator ID per page. To produce the "Detail" (as opposed to the "List" report) a "D" should be entered in the "Type" field of the VSEC/R screen.
- "Operator Security List (SE5502)" report: Using the "Operator Print System Report Parm" screen in the VSEC system (VSEC/R) the instructions above can be applied to produce a less detailed list of all or a range of operators for which a specific switch has been set to "Y." The SE5502 will produce a list of only the operator ID information and will produce seven at a time on the screen. To produce the "List" (as opposed to the "Detail" report) a "L" should be entered in the "Type" field of the VSEC/R screen.

It should be noted that only operators deemed in the system as the Corporate Security Officer and the Department Security Officer can produce this report.

Once those operators have been identified it is important to review each to determine if they have a business need for such privileges and ensure that it does not cause a segregation of duties concern.

Monitoring

As individuals' roles and responsibilities change within the organization, it is important to ensure access to modify SCF rules and SuperOp events is only granted to those who warrant such access. Therefore, it is important to periodically review individuals' access authorization, using those instructions above, to ensure each is still appropriate. Evidence of such reviews as well as justifications for those individuals with access levels discussed above should be maintained. In addition, management should also review a sample of modifications being made by individuals to ensure they are appropriate and proper supporting documentation has been maintained.

5 CONCLUSION

As previously noted, using SCF, SuperOp, and other similar applications can be quite beneficial to the contractors and their claims processing businesses. The use of customized scripts to simulate the actions of a claims operator can produce more efficient and effective processes, but once in production these scripts can literally impact thousands or more claims and could, unless properly controlled, adversely impact financial statements. Because of this concept, it is extremely important to ensure that strong security controls with a concentration in change and access management and segregation of duties must exist to ensure expected results are obtained. Using the instructions identified in this white paper, Carriers, Fiscal Intermediaries, and MACs should be able to build reliable controls around applications such as SCF and SuperOp.

(This Page Intentionally Blank)

APPENDIX A - REPORT EXAMPLES

SCF - MCS

Example of the Clerk Record Update Screen (page 1 of the screen). The SCF security field is field number 64 with valid values being either a “Y” or “N”.

Figure 1 Clerk Record Update Screen

```
TASK 1...                  CLERK RECORD UPDATE
KEY 2...............                                          3............

ACTION CODE  4           A = ADD     CLERK RECORD              PF3=MENU
                         C = CHANGE  CLERK RECORD              PF8=PAGE2
                         D = DELETE  CLERK RECORD
                         I = INQUIRY CLERK RECORD

CLERK   5...             NEXT CLERK  6...

NAME  FIRST              LAST              DEPT DIV  UNIT   LAST UPDATED   BY
      7...........       8..............   9..   10   11      12......   .13.

      NICKNAME           B-DATE     HOLD    STATE INDICATORS
      14........          15..       16     17 18 .. . .. . .. .


    ONLINE SCREEN ACCESS                FILE MAINTENANCE AUTHORIZATION


AGE      19      ACIS 1   36         ADS              50    MM              65
AUDIT    20      ACIS 2   37         CENSUS UPDATES   51    NU              66
CLERK    21      ACIS 3   38         CRITERIA         52    SU              67
DEOL     22      ACIS 4   39         CWF ERROR        53    CO              68
GT       23      ACIS 5   40         DIAGNOSIS        54
HELP     24      ACIS 6   41         EDIT             55    2590 REPORT
IS       25      E1       42         EDIT/AUDIT       56    AUTHORIZATION   69
LCEF     26      E2       43         EOMB             57
MSG      27      E3       44         HARDCODED E/A    58
MSPR     28      C1       45         MODIFIER         59    PSUP            70
SMRT     29      C2       46         NARRATIVE        60
SS       30      C3       47         PCF              61    SAFE
TRNG     31      C4       48         PROCEDURE        62    S1  71
CLRK CA  32      HR       49         TACS             63    S2  72
VH       33                          SCF              64    S3  73
LC       34
HIMR SS  35


MSG 74.............................................
```

(This Page Intentionally Blank)

Example of the Clerk File Security Report (H99PCSEC). The SCF security field is field number 8 with valid values being either a "Y" or "N".

Figure 2 Clerk File Security Report (H99PCSEC)

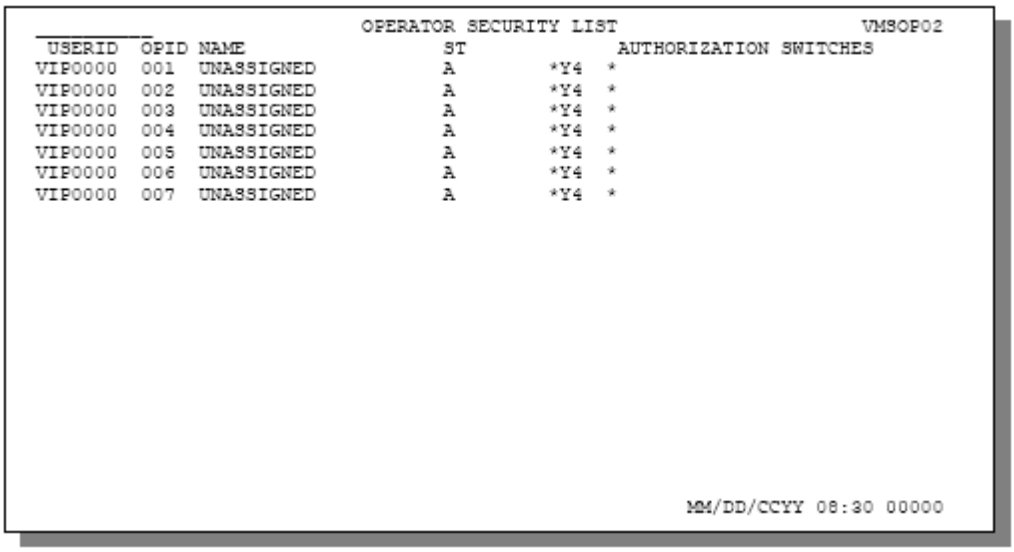
```
 REPORT ID: H99RCRCF                        MCS QUALITY ASSURANCE                          FEBRUARY 07, 2005          PAGE:   1
                                            CLERK FILE SECURITY REPORT
                                                                                1 1 1 1 1  1    1111222222222233 3 33333334444444444555555
 1      2                                    3   4  5     6          7    8 9    0 1 2 3 4  5    6789012345678901 2 34567890123456789012345
 CLRK CLERK NAME                           DEPT D  U LAST UPDATED NICKNAM S B-D  H S S S S LIMIT AACDGHILMMSSTCVL H AAAAAAEEECCCCHACCCDEEHE
 ID   FIRST/LAST                               I  N   DATE/BY           C   A  O T T T T       GULETESCSSMSRAHC M CCCCCC1231234RDERWIDDDO
                                               V  I                     F   T  L 1 2 3 4       EDRO L EGPR N    R SSSSSS        SNIFAIAEM
                                                  T                         E  D                IKL P F RT G    S 123456         ST GTUAB

                                           55556 666666 666      77777777778888888889 99999999 9  1  1  1 1 1 1 1 1 1 1 1 11 1
                                           67890 123456 789      01234567890123456789 12345678 9  0  0  0 0 0 0 0 0 0 0 11 1
                                                                                                  0  1  2 3 4 5 6 7 8 9 01 2
-                                          MNPPT MNSC2P SSS      IRNAIXXXAAAAFIBITTNRV MMSSSMAC * *2 *4 *9 J # W I R X O VP PSWD
                                           OACRA MUUO5S 123      AECFGABOASIPIRSPXCGGQ FTPTTDRT                          IR UPDT
                                           DRFOC     9U                              US                                OO
                                           IR CS     0P                              PP                                LD


AC0    ACLERK          AAAAACLERK          000 00 0 000000      AAAAA     N 0000 N X X X X 00000 NUNUUNINNNNIUNNI I UIIIIUUUUUUUUNNNNNNNNN
                                          NNNNN UUUUNN NNN      NUNUNNNNUIIIIIIUUUNUU NNNNNNN  Y Y  Y  Y  Y Y Y Y Y Y   NY 010140

BC0    BCLERK          BBBBBCLERK          000 00 0 000000      BBBBB     N 0000 N X X X X 00000 NUNUUNINNNNIUNNI I UIIIIUUUUUUUUNNNNNNNNN
                                          NNNNN UUUUNN NNN      NUNUNNNNUIIIIIIUUUNUU NNNNNNN  Y Y  Y  Y  Y Y Y Y Y Y   NY 010140

CC0    CCLERK          CCCCCCLERK          000 00 0 000000      CCCCC     N 0000 N X X X X 00000 NUNUUNINNNNIUNNI I UIIIIUUUUUUUUNNNNNNNNN
                                          NNNNN UUUUNN NNN      NUNUNNNNUIIIIIIUUUNUU NNNNNNN  Y Y  Y  Y  Y Y Y Y Y Y   NY 010140

                                                    TOTAL NUMBER OF CLERKS =  113..
```

(This Page Intentionally Blank)

SuperOp - FISS

Example of the Operator Security List. The "Authorization Switches" section details the security assignments for each individual. Security assignment descriptions can be found in Appendix B.

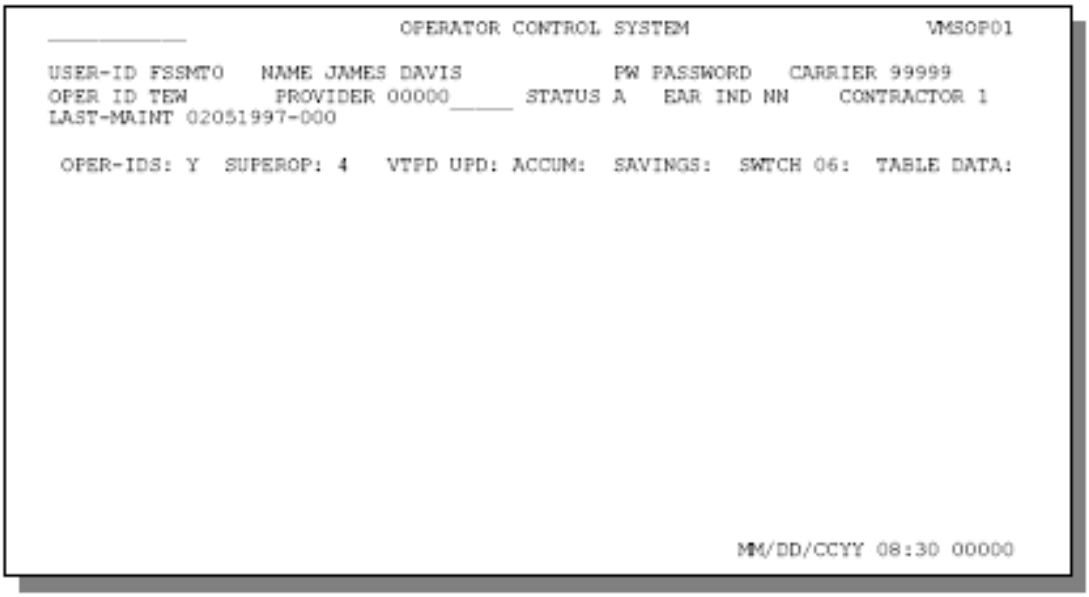
Figure 3 Operator Security List



```
_________                    OPERATOR SECURITY LIST                    VMSOP02
 USERID  OPID NAME               ST          AUTHORIZATION SWITCHES
VIP0000  001  UNASSIGNED         A        *Y4  *
VIP0000  002  UNASSIGNED         A        *Y4  *
VIP0000  003  UNASSIGNED         A        *Y4  *
VIP0000  004  UNASSIGNED         A        *Y4  *
VIP0000  005  UNASSIGNED         A        *Y4  *
VIP0000  006  UNASSIGNED         A        *Y4  *
VIP0000  007  UNASSIGNED         A        *Y4  *

                                                    MM/DD/CCYY 08:30 00000
```

Example of the "Operator Control System" screen. This screen can be used to better understand the switches displayed above at the individual user level. Security assignment descriptions can be found in Appendix B.

Figure 4 Operator Control System Screen



```
_________                    OPERATOR CONTROL SYSTEM                   VMSOP01

USER-ID FSSMTO   NAME JAMES DAVIS           PW PASSWORD   CARRIER 99999
OPER ID TEW       PROVIDER 00000_____ STATUS A   EAR IND NN    CONTRACTOR 1
LAST-MAINT 02051997-000

 OPER-IDS: Y  SUPEROP: 4   VTPD UPD: ACCUM:  SAVINGS:  SWTCH 06:  TABLE DATA:

                                                    MM/DD/CCYY 08:30 00000
```

(This Page Intentionally Blank)

SuperOp - VMS

Example of the Operator Security Detail (SE5501) report. The corresponding SuperOp security switches can be found in Appendix B with valid values being either a “Y” or “N”.

Figure 5 Operator Security Detail (SE5501) Report

```
CARRIER: CARR#                                          CARRIER NAME                                          RUN DATE: MM/DD/YY
PROGRAM: VMSSE550                                     MEDICARE PART B                                         RUN TIME: HH:MM:SS
REPORT:  SE5501                                    OPERATOR SECURITY DETAIL                                      PAGE:          1

 REQUESTOR ID: V000000    DATE/TIME:  MM/DD/YY   HH:MM:DD   SWITCH NUMBER: 999

                                                SECURITY INFORMATION

USER ID: 0000000     NAME: ELIZABETH JOHNSON                          STATUS:A

DEPT: CARR        JOB FUNCTION:                                          CARRIER: CARR#

OPER ID: 000         PROVIDER:                EAR IND:  NN                CONTRACTOR: 1
COMMENTS:


                                                SECURITY SWITCHES
          0                   1                   2                   3                   4                   5
--RANGE--  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
001 - 050  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
051 - 100  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
101 - 150  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
151 - 200  Y Y Y Y Y Y Y Y N N N N Y N N N N N N N N N N N N Y Y Y Y Y N N N N N N N Y Y Y Y N N Y Y Y N Y Y
201 - 250  Y Y Y Y N Y Y Y Y Y Y N N N Y Y Y Y Y Y N N N N N N N N N Y Y Y Y Y Y Y Y Y Y Y Y N Y Y Y Y Y Y Y
251 - 300  Y Y Y Y Y Y Y Y Y Y Y N N N N N N N N N N Y Y Y Y N N N N N N N N N N Y Y Y N N N N N N N Y N N N
301 - 350  N N N N N N N N Y N Y Y Y Y N N N N N Y Y Y N N N N N N N Y Y Y Y N Y Y Y N Y Y Y Y Y Y Y Y Y Y Y
351 - 400  Y Y Y Y Y Y Y Y Y Y Y N N N N N N N N Y N N Y Y Y Y Y Y N N N Y Y Y N N N N N N N N Y N N N Y N N N
401 - 450  N Y N N N Y Y N N Y Y Y Y Y N N N N N N N N N N N N Y Y Y N Y Y N N N Y Y N N N N N N N N N Y N N
451 - 500  N N N N N N N N N N N N N N N N Y Y Y Y Y Y Y Y Y Y Y Y N Y Y N N Y N N N N N N N N N N N N N N Y
501 - 550  N N N N N N Y N N N N N N N N N Y N N N N N Y Y Y Y N N N N N N N Y Y Y Y N N N N N N N N N N N N
551 - 600  Y N N N N Y N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
601 - 650  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
651 - 700  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
701 - 750  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
751 - 800  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
801 - 850  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
851 - 900  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
901 - 950  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
951 - 999  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
```

Example of the Operator Security List (SE5502) report. Those operators listed are those that have access to the switch value identified at the top of the report.

Figure 6 Operator Security List (SE5502) Report

```
CARRIER: CARR#                                        CARRIER NAME                                                RUN DATE: MM/DD/YY
PROGRAM: VMSSE550                                                                                  MEDICARE PART B
RUN TIME: HH:MM:SS REPORT:  SE5502                                                                         OPERATOR SECURITY LIST
                       PAGE:         1

REQUESTOR ID: 0000000    DATE/TIME:  MM/DD/YY   HH:MM:SS    SWITCH NUMBER: 111

USER ID    OPID  NAME                          ST  TYPE  JOB FUNC  DEPT  COMMENT
0000000    010   UNASSIGNED
0000000    011   MARY-S                        A    3              CARR
0000000    012   UNASSIGNED                    A    3              CARR
0000000    013   JAMES-D                       A    3              CARR
0000000    014   UNASSIGNED                    A    3              CARR
0000000    015   PATRICIA-J                    A    3              CARR
0000000    016   UNASSIGNED                    A    3              CARR
0000000    017   UNASSIGNED                    A    3              CARR
0000000    018   UNASSIGNED                    A    3              CARR
0000000    019   BARBARA-J                     A    3              CARR
0000000    020   UNASSIGNED                    A    3              CARR
0000000    021   UNASSIGNED                    A    3              CARR
0000000    022   WILLIAM-M                     A    3              CARR
0000000    023   ELIZABETH                     A    3              CARR
0000000    024   UNASSIGNED                    A    3              CARR
0000000    025   UNASSIGNED                    A    3              CARR
0000000    026   UNASSIGNED                    A    3              CARR
0000000    027   UNASSIGNED                    A    3              CARR
0000000    028   UNASSIGNED                    A    3              CARR
0000000    029   UNASSIGNED                    A    3              CARR
0000000    030   LINDA-W                       A    3              CARR
0000000    031   UNASSIGNED                    A    3              CARR
0000000    032   ROBERT-W                      A    3              CARR
0000000    033   UNASSIGNED                    A    3              CARR
0000000    034   MICHAEL-T                     A    3              CARR
0000000    035   UNASSIGNED                    A    3              CARR
0000000    036   UNASSIGNED                    A    3              CARR
0000000    037   UNASSIGNED                    A    3              CARR
0000000    038   JOHN-M                        A    3              CARR
0000000    039   UNASSIGNED                    A    3              CARR
0000000    040   BARBARA-S                     A    3              CARR
0000000    041   UNASSIGNED                    A    3              CARR
0000000    042   UNASSIGNED                    A    3              CARR
0000000    043   LINDA-J                       A    3              CARR
0000000    044   UNASSIGNED                    A    3              CARR
0000000    045   UNASSIGNED                    A    3              CARR
0000000    046   PATRICIA                      A    3              CARR
0000000    047   UNASSIGNED                    A    3              CARR
0000000    048   JOHN-D                        A    3              CARR
0000000    049   UNASSIGNED                    A    3              CARR
0000000    050   UNASSIGNED                    A    3              CARR
```

APPENDIX B - SUPEROP SECURITY SWITCH VALUES

Figure 7 SuperOp - FISS

Switch	Value	Description
OPER-IDS	*Blank*	No access to OPFL (default)
	Y	Access to OPFL
SUPEROP	*1*	INQUIRE only **Note:** INQUIRE also includes access to all event and value set search functions (for example, add/change criteria, start search, view results).
	2	INQUIRE/ADD/UPDATE/INACT/ACTIVE/COPY/RESTORE
	3	INQUIRE/ADD/UPDATE/INACT/ACTIVE/COPY/RESTORE/DELETE
	4	INQUIRE/ADD/UPDATE/INACT/ACTIVE/COPY/RESTORE/ DELETE/PROD
VTPD UPD	*Y*	VTPD update authority (HIMR Only)
ACCUM	*1*	INQUIRE only
	2-4	UPDATE
SAVINGS	*1*	INQUIRE
	2-4	UPDATE
SWTCH 06	*Blank*	**FISS users only.** See *Mass Adjustment and Random Sampling Systems User Guide*.
TABLE DATA (previously SWITCH 07)	*1*	INQUIRE **Note:** This allows inquiry/view authority.
	2	UPDATE **Note:** This allows inquiry/view authority and update capability to entries on existing table records.
	3	DEFINE TABLE DATA **Note:** This combines 1 and 2 and allows the capability to define/add table data records.
	4	DROP TABLE DATA **Note:** This combines 1, 2 and 3 and allows capability to drop/delete the table data records.

Table 2 SuperOp - VMS

Security Switch Values Sorted by Transaction ID				
Tran ID	Question #	Question Text	Switch #	Values
SUPR	01	Authority for this Transaction	086	N No authority for this transaction Y Authority to access SuperOp
SUPR	02	Maintain XMOD, XADJ Events	556	N No authority for this transaction Y Authority to maintain XMOD and XADJ SuperOp Events
SUPR	03	Maintain VOQC Events	557	N No authority for this transaction Y Authority to maintain VOQC SuperOp Events
SUPR	04	Maintain SURE Events	570	N No authority for this transaction Y Authority to maintain SURE Events
SUPR	05	Maintain all other Events	558	N No authority for this transaction Y Authority to maintain all other SuperOp Events
SUPR	06	Question # 2 plus Delete XMOD, XADJ Events	559	N No authority for this transaction Y Authority to maintain and delete XMOD and XADJ SuperOp Events
SUPR	07	Question # 3 plus Delete VOQC Events	560	N No authority for this transaction Y Authority to update and delete VOQC Events
SUPR	08	Question # 4 plus Delete SURE Events	571	N No authority for this transaction Y Authority to maintain and delete SURE Events
SUPR	09	Question # 5 plus Delete all other Events	561	N No authority for this transaction Y Authority to maintain and delete all other Events
SUPR	10	Question # 6 plus Change Status to Production for XMOD, XADJ Events	562	N No authority for this transaction Y Access SuperOp as a super reviewer; allows the operator to maintain XMOD and XADJ Events; to delete XMOD and XADJ Events; and to change the status of XMOD and XADJ Events to Production
SUPR	11	Question # 7 plus Change Status to Production for VOQC Events	563	N No authority for this transaction Y Authority to maintain VOQC SuperOp Events, to delete VOQC SuperOp Events, and to change the status of VOQC Events to Production
SUPR	12	Question # 8 plus Change Status to Production for SURE Events	572	N No authority for this transaction Y Authority to maintain SURE Events, to delete SURE Events, and to change the status of SURE Events to production
SUPR	13	Question # 9 plus Change Status to Production for all other Events	564	N No authority for this transaction Y Authority to maintain all other Events, to delete all other Events, and to change the status of all other Events to Production

Security Switch Values Sorted by Transaction ID				
SUPR	14	Question # 10 plus Archive XMOD,XADJ Events	565	N No authority for this transaction Y Access SuperOp as a super reviewer; allows the operator to maintain XMOD and XADJ Events; to delete XMOD and XADJ Events; to change the status of XMOD and XADJ Events to Production; and to archive XMOD and XADJ Events
SUPR	15	Question # 11 plus Archive VOQC Events	566	N No authority for this transaction Y Authority to update SuperOp VOQC Events, to delete VOQC Events, to change the status of VOQC Events to Production, and to archive VOQC Events
SUPR	16	Question # 12 plus Archive SURE Events	573	N No authority for this transaction Y Authority to maintain and delete SURE Events, to change the status of SURE Events to production, and to archive SURE Events
SUPR	17	Question # 13 plus Archive All other Events	569	N No authority for this transaction Y Authority to maintain all other Events, to delete all other Events, to change the status of all other Events to production, and to archive all other Events
SUPR	18	Savings Inquiry Only	575	N No authority for this transaction Y Authority to view the Event Category Savings Statistics and Event Savings Statistics List screens.
SUPR	19	Savings Update for Event Categories	576	N No authority for this transaction Y Authority to update the Event Category Assignment/Definition screen. Note: There is no inquiry authority for the Event Category Assignment/Definition and the Event Category Salary Information screens.
SUPR	20	Question # 18 and 19 for Savings	577	N No authority for this transaction Y Authority to view the Event Category Savings Statistics and Event Savings Statistics List screens and update the Event Category Assignment/Definition screen for Savings. Note: There is no inquiry authority for the Event Category Assignment/Definition and the Event Category Salary Information screens.
SUPR	21	Question #18 and 19 plus Category and Salary	578	N No authority for this transaction Y Authority to view the Event Category Savings Statistics and Event Savings Statistics List screens; update the Event Category Assignment/Definition screen for Savings, plus update Event Category Salary Information screens. Note: There is no inquiry authority for the Event Category Assignment/Definition and the Event Category Salary Information screens
SUPR	22	Can View Table Data?	579	N No authority for this transaction Y Authority to view table data

Security Switch Values Sorted by Transaction ID				
SUPR	23	Update Table Data	580	N No authority for this transaction Y Authority to update table data
SUPR	24	Define Tables	581	N No authority for this transaction Y Authority to define tables
SUPR	25	Drop Tables	582	N No authority for this transaction Y Authority to drop tables

APPENDIX C - 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 D - GLOSSARY

CMS	Centers for Medicare & Medicaid Services
CWF	Common Working File
DME	Durable Medical Equipment
DMERC	Durable Medical Equipment Regional Carriers
EDC	Enterprise Data Centers
FI	Fiscal Intermediaries
FISS	Fiscal Intermediary Shared System
MAC	Medicare Administrative Contractors
MCS	Multi Carrier System
MMA	Medicare Prescription Drug, Improvement and Modernization Act
SCF	System Control Facility
SDLC	System Development Life Cycle
VMS	VIPS Medicare System

APPENDIX E - CHANGE CONTROL PROCESS

Figure 8 Change Control Process

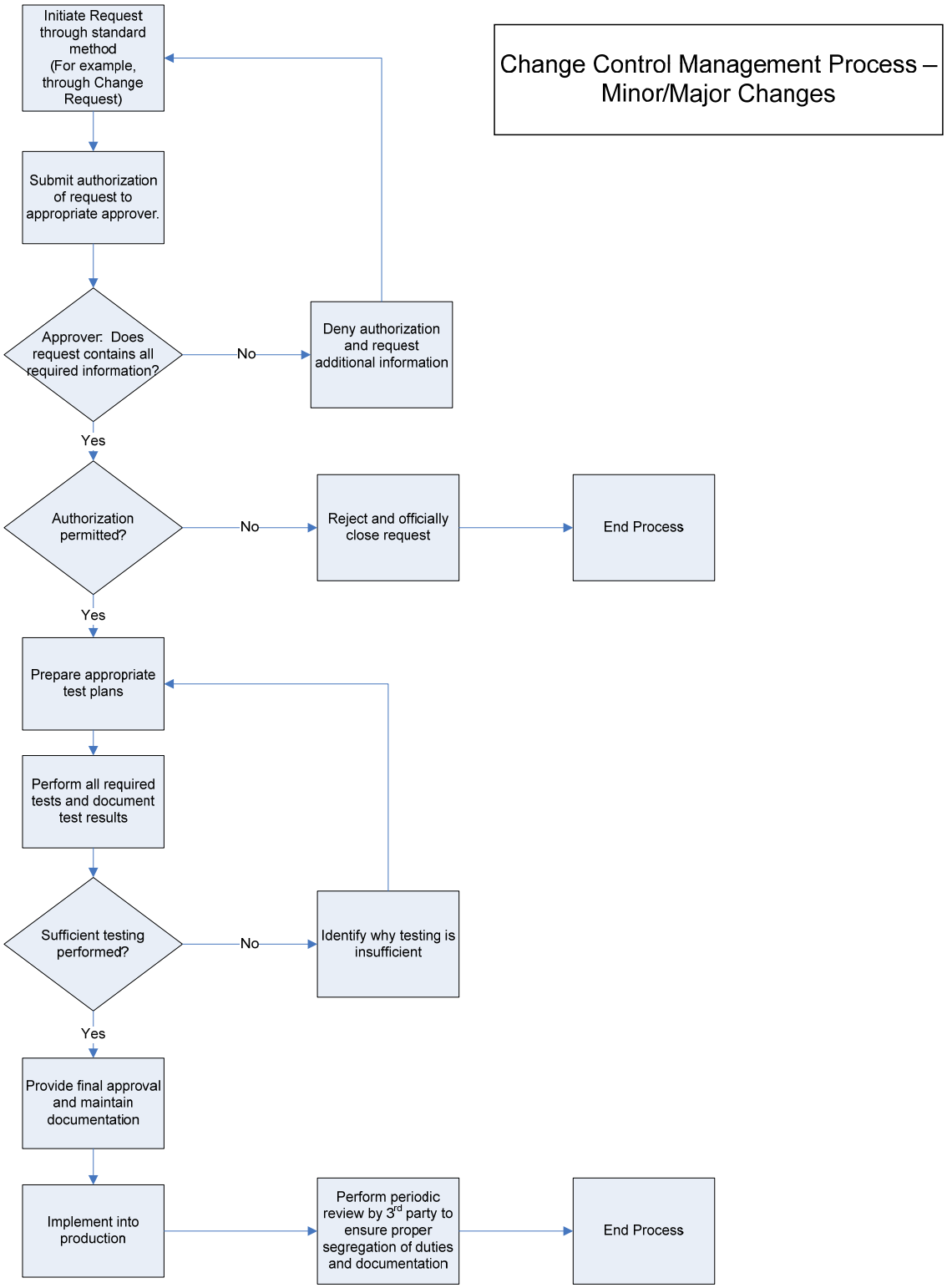
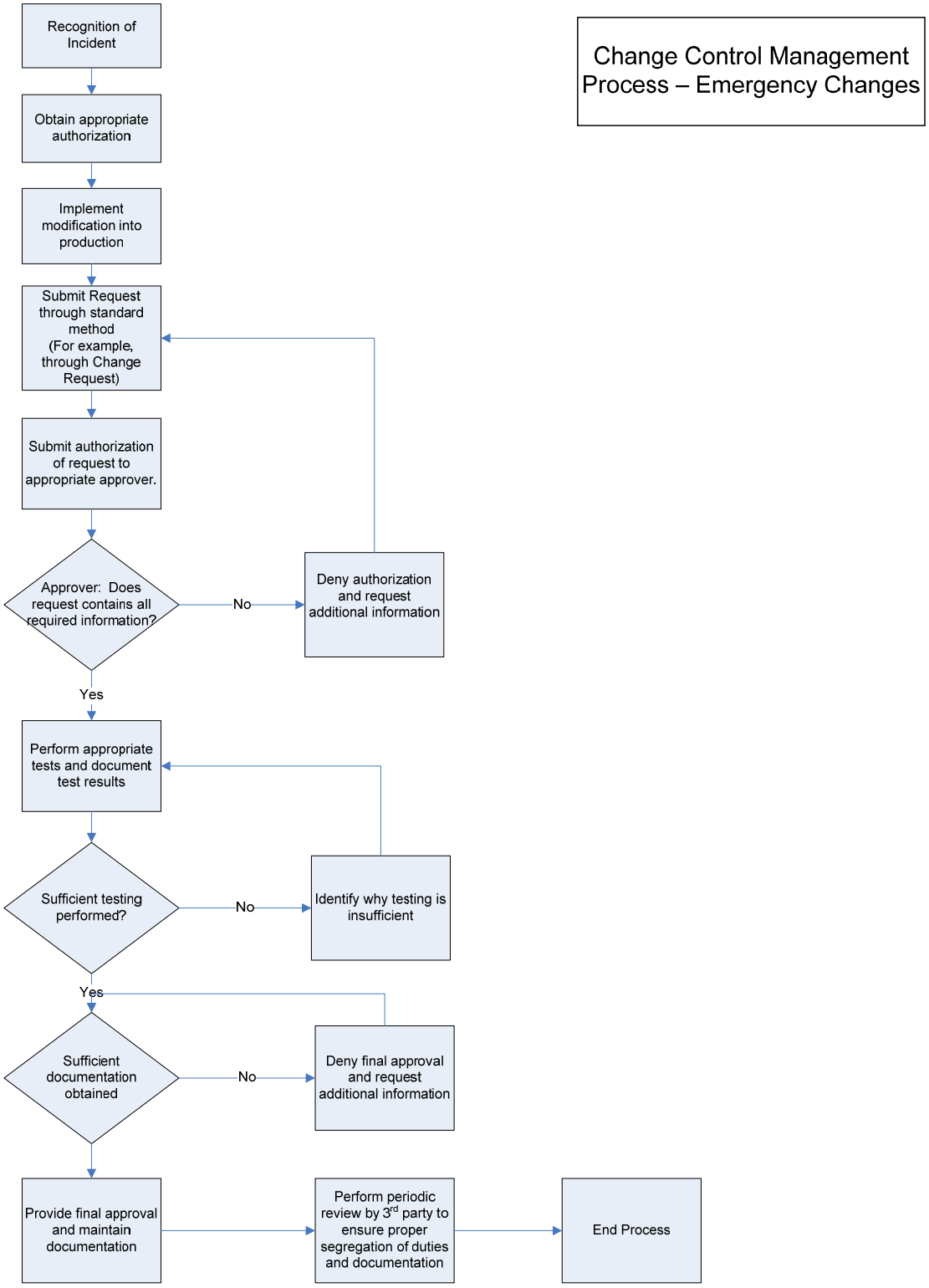


Figure 9 Emergency Change Control Process



APPENDIX F - REFERENCES

- *Certified Information Systems Auditor Review Manual* 2006, 16th edition, 2005
- *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, effective 01/2009
- *Federal Information System Controls Audit Manual (FISCAM)* Exposure Draft (GAO-08-1029G, July 2008)
- *Supervisor's Manual, MCS User Manual,* last updated 07/12/05
- *System Control Facility, MCS User Manual,* last updated 02/01/2006
- *ViPS SuperOp User Guide,* Version 9.0, 01/2007
- *ViPS SuperOp User Guide Supplement VMS-DMAC,* Version 9.0, 10/2006

(This Page Intentionally Blank)