Program Memorandum Intermediaries/Carriers

Department of Health and Human Services (DHHS)
HEALTH CARE FINANCING ADMINISTRATION (HCFA)

Transmittal AB-01-49 **Date: MARCH 30, 2001**

CHANGE REQUEST 1605

SUBJECT: Follow On Instructions to HCFA Business Partners Systems Security Requirements

The purpose of this Program Memorandum (PM) is to provide supplemental instruction on how, when, and where to submit the following:

1. Core Security Requirements Self-Assessment, Selected Supporting Documentation, and Information Systems Security Funding Requirements and
2. Security Plan Architecture Report.

HCFA published the new Business Partners Systems Security Manual, and PM AB-01-11 on January 26, 2001. The manual, PM and associated change request can be found at www.hcfa.gov/pubforms/htmltoc.htm.

This supplemental instruction also applies to Medicare carriers and intermediaries, Durable Medical Equipment Regional Carriers (DMERCs), the Standard System Maintainers (SSMs), Coordination of Benefits (COB) Contractor, and the Program Safeguard Contractors (PSCs), with whom HCFA executes Federal Acquisition Rules (FAR) contracts.

Core Security Requirements Self-Assessment

HCFA has made a tool available to every Medicare contractor to use in assessing, documenting and reporting on your compliance with HCFA core security requirements (www.hcfa.gov/pubforms/htmltoc.htm). The use of this tool, referred to as the Contractor Assessment Security Tool (CAST), is mandatory. Detailed instructions for acquiring, installing and securing technical assistance on CAST plus answers to frequently asked questions about CAST are provided at www.hcfa.gov/extpart. In addition, you may contact the CAST help desk at (703) 713-0630, if you have questions regarding the CAST or experience any problems during installation.

Several Medicare contractors asked for guidance about how to conduct a core security requirements self-assessment. We consulted with the Medicare Contractor Systems Security Technical Advisory Group who helped us prepare the document entitled “Self-Assessment Process” that is included in Attachment A. It provides you with a suggested approach to performing the HCFA security self-assessment. This document is informational only. You may use any project management approach that you believe will enable you to meet the deadlines in PM AB-01-11. An electronic copy of the document is also available at www.hcfa.gov/extpart.

Security Plan Architecture Report

PM AB-01-11 requires you to prepare and submit a Security Plan Architecture Report. The Security Plan Architecture Report is a brief document that enables you to record the key elements of the systems, applications and networks which support your operation in fulfillment of your Medicare contracts. The Report also helps you identify which systems and networks require you to prepare a systems security plan. Systems security plans must be prepared in accordance with HCFA's systems security plan methodology (www.hcfa.gov/extpart). The system security plan architecture template and instructions are provided in Attachment B. The template and instructions will also be available at www.hcfa.gov/extpart. The completed template will serve as the basis for the security plan architecture report.

Data Center Information Collection

HCFA has received several inquiries about how a carrier or intermediary report the data center that it operates on behalf of other Medicare contractors when it conducts the CAST assessment and prepares a Security Plan Architecture.

The Medicare contractors and COB contractor are contractually and financially responsible for ensuring that the systems security requirements set forth in the HCFA Business Partner Systems Security Manual (and associated PM) are met by their respective data center whether they own it or contract for it. This shall include all significant IT suppliers (i.e. corporate data centers that provide front- and back-end processing services).

However, for the purpose of conducting the CAST assessment, security plan architecture and future productivity investment funding, data center security program documentation and security plan architecture should be reported by the carrier or intermediary that owns it rather than by its individual carrier or intermediary users. Data center users may incorporate by reference in their certifications that a CAST assessment and security plan architecture has been prepared and submitted by their data center owner.

National Medicare Contractor Security Teleconference

HCFA is planning to conduct a national audio conference in early May 2001 to present "lessons learned" from the Medicare Contractor Systems Security TAG about the CAST assessment and security plan architecture process and from the Fiscal Year 2000 Chief Financial Officers Audit conducted by the Office of the Inspector General. Additional information about the audio conference will be provided to you shortly.

Submission Requirements and Format

Document	**# of Copies**	**Format**
Signed Transmittal Letter *This letter should indicate that the CAST; Architecture and Cost Estimates have been reviewed and approved by appropriate corporate officials.	1	Paper
Business Partner System Security Plan (SSP) Architecture Report **Worksheets should not be submitted	2	CD-ROM or 3.5" floppy disk
Copies of supporting/existing SSPs or excerpts from third party SSPs to support Architecture Report	2	CD-ROM or 3.5" floppy disk
Copies of Risk Assessment supporting/referenced in SSPs.	2	CD-ROM or 3.5" floppy disk
CAST Output Reports	2	CD-ROM or 3.5" floppy disk

Note: The above submission requirements are in addition to those listed in the HCFA Business Partners Security Oversight Manual.

All submissions should be mailed to:

Health Care Financing Administration
Office of Information Services
Attention: Sherwin Schulterbrandt
7500 Security Boulevard
Baltimore, MD 21244

Confidentiality of Contractor Systems Security Submissions

HCFA understands that it is requesting information that is sensitive to both your Medicare line of business as well as your corporate operations. To that end, HCFA has implemented procedures to safeguard these submissions. These procedures include establishing an audit trail for tracking who receives, accesses, and handles these submissions. The submissions will be stored in a secure manner. HCFA's systems security contractor and its independent verification and validation contractors, in addition to their contract provisions on non-disclosure of sensitive information also have implemented security procedures for handling and storing your submissions while they are in temporary possession of them. These procedures have been reviewed and approved by HCFA.

You should also be aware that your submissions could be obtained by the public under the provisions of the Freedom of Information Act. In the event that HCFA receives such a request, we will edit the information provided in such a response to eliminate any sensitive information. Sensitive information could include such things as: contractor name and identification (if appropriate), IP Addresses and Port numbers, specific hardware or software identification, corporate security information that you have identified as sensitive or proprietary. If we are uncertain of the sensitive or releasable nature of any requested documents related to your submission, we will check with you and our Office of General Counsel first.

Security Questions and Concerns

HCFA expects that you may have questions or concerns about the submission of requested information, the new security requirements, CAST or this PM. In addition to the CAST help desk at (703) 713-0630, you may also refer questions to ContractorSystemsSecurity@hcfa.gov (use the question format provided on the web site). We will provide a prompt direct response as well as post it to a Frequently Asked Questions (FAQ) page on the HCFA Medicare Contractor Systems Security web site (www.hcfa.gov/extpart).

The *effective date* for this PM is March 30, 2001.

The *implementation date* for this PM is March 30, 2001.

These instructions should be implemented within your current operating budget.

This PM may be discarded after December 31, 2001.

If you have any questions, contact Sherwin Schulterbrandt at (410) 786-0743 or Max Buffington at (410) 786-6966.

Attachments:
A) Self-Assessment Process Document
B) System Security Plan Architecture Template and Instructions

Attachment A
Systems Security GAP Analysis

Self-Assessment Process

The following is a recommended process for performing the HCFA security self-assessment. This document was prepared to assist contractors in planning and executing the self-assessment. It was prepared with input and assistance from the Medicare Contractor Security Technology Advisory Group. It is advisory only.

A) Identify each HCFA contract control number (or business function) for which a HCFA Self assessment must be performed (Contract control numbers include: Part A, Part B, DMERC, CWF, Standard Systems Maintainers, and contracted Data Center services)

1) Make a worksheet for each contract control number to record the necessary preparation steps

a) Organize contract control numbers to identify shared systems and physical locations

2) For each contract control number, identify the following:

a) All applicable processing locations including (but not limited to):

(1) Data input

(2) Processing centers

(3) Print centers

(4) Data centers

(5) Backup storage locations

(6) Backup process locations and hot sites

(7) Security point(s) of contact and processing supervisor(s) for each physical location

b) All applicable processing systems including (but not limited to):

(1) Hardware platforms (mainframes)

(2) Networks

(3) Print/mail centers

(4) Data centers

(a) Major data centers (shared across multiple contract control numbers and/or contractors) shall have separate self-assessments performed to ensure proper identification of shared safeguards

(5) Systems interfaces (but not limited to):

(a) Interfaces with other systems within your organization

(b) Interfaces with remote company data centers

(c) Interfaces with remote contracted data centers

(d) Interfaces with CWF host (local and/or remote)

c) All applicable processing applications including (but not limited to):

(1) Standard systems (APASS, FISS, GTEMS, HPBSS, MCS, VMS)

(2) Major applications (Operating Systems, RACF, Oracle$^{®}$, MS SQL-Server$^{®}$, etc.)

(3) General support applications (e-mail, web host, dial-in host, etc)

(4) Program (application) administrator(s) and/or database administrator(s) for each application

d) Systems administrator(s) and/or database administrator(s) for each processing system

3) Identify the flow-path of Medicare data

B) Identify the personnel available to ACTIVELY participate in the self-assessment

1) Security personnel to address specific areas of concern such as:

a) Policies

(1) Identification/definition of "Sensitive Data"

(a) Federal Tax Information (FTI)

(b) Health Care Data

(2) Management policy

(3) Corporate policy

(4) Chain of responsibility

(5) Security policies

(6) Risk assessments

(7) Personnel resources (HR)

(8) Access control policies and procedures

b) Plans

(1) Systems security plans

(2) Contingency plans

(a) Disaster recovery

(b) Testing

(3) Business continuity plans

(a) Emergency processing

(b) Hot sites

- c) Training
  - (1) Training plans
  - (2) Employee training
  - (3) Training records
- d) Security program
  - (1) Internal audit records
  - (2) Incident response
  - (3) Access control
    - (a) Permanent access
      - (i) Access limits
        - 1. Levels of access (need-to-know)
        - 2. Authorized transactions
        - 3. Exceptions
    - (b) Temporary access
    - (c) Granting and revoking access
      - (i) Hiring procedures
      - (ii) Termination procedures
      - (iii) Auditing/reviewing access list
    - (d) Segregation of duties
- e) Physical infrastructure
  - (1) Physical security
    - (a) Physical access control procedures
    - (b) Physical access control implementation
  - (2) Physical layout
    - (a) Environmental
      - (i) Plumbing
      - (ii) Power supplies
      - (iii) Alarm systems
    - (b) Fire protection
  - (3) Contingency testing

2) Systems personnel to address specific areas of concern such as:

a) Systems security

(1) Telecommunications

(2) Networking

(3) Remote access

(4) Firewalls

(5) System(s) boundaries

b) System backups

(1) Data backups

(a) Backups

(b) Identification

(c) Contingency planning

(2) Critical operating/application systems

(a) Backups

(b) Identification

(c) Contingency planning

c) Automated audit trails

(1) Monitoring audit logs

(2) Response to unauthorized actions

d) Logical access controls to systems

(1) Maintenance of access control lists

(2) Maintenance of access control systems

(3) Access to access-control applications \

(4) Systems utilities access controls

e) Passwords, tokens, or other access control devices

f) Processes for system software changes

(1) Process

(a) Normal

(b) Emergency

(2) Permissions

(3) Logs

(4) Libraries

g) Configuration management

(1) Software distribution

(2) Inventory

(3) Change documentation

3) Software personnel to address specific areas of concern such as:

a) Logical access controls to software

(1) Database and DBMS access controls

(2) Application (programming) access controls

(3) Installation and modification

(4) Passwords, tokens, or other access control devices

b) Processes for application software changes

(1) Process

(a) Normal

(b) Emergency

(2) Permissions

(3) Logs

(4) Libraries

c) Software completeness controls

(1) Verification of data accuracy

(2) Verification of data completeness

d) Transaction logging

e) Standard Systems

C) Organize your available personnel into teams to address specific areas of the HCFA Core Security Requirements (CSRs)

1) Assign categories and/or general requirements to the applicable team/personnel.

2) Encourage communication between teams and team members.

a) Many CSRs will cross boundaries between teams

b) Specific CSRs may fall outside of a teams expertise areas

c) Many CSR concepts span multiple Categories

d) Pass worksheets around for validation

D) Answer CSRs.

1) Answer CSRs on a worksheet before entering into the CAST (**NOTE**: Entries in the CAST are not editable once entered. Changed answers will need to be re-entered as a new record.)

a) Worksheets should be generated to allow for review and concurrence between team members.

b) Final worksheets (CSR answers) should be reviewed by applicable team leaders for final concurrence before entry into CAST tool.

c) It is recommended that entry of data (CSR answers) into the CAST tool be deferred until all similar CSRs are addressed.

E) Develop safeguards

1) Develop safeguard(s) that address each and every non-compliant CSR.

a) Develop safeguards that can address multiple CSR requirements

(1) When initial list of safeguards is complete, check for goal overlaps (where intent of several safeguards can be accomplished by a single safeguard).

(2) Reorganize safeguards for maximum impact and cost effectiveness

2) Determine costs for each safeguard

a) Determine **Total Safeguard Cost.** Total cost includes all those costs incurred as a result of implementing the safeguard. These will include purchases, leases, setup and delivery, consultant services, applicable overhead, depreciation, amortization, cost of money, and all other associated costs in accordance with disclosure practices. *Note: As this submission will be used for budgetary purposes it must be an estimate. It is advised that finance, accounting, or other personnel familiar with the application of cost estimating practices be consulted.*

b) Determine **Percent Cost Applied to HCFA,** or the percentage of cost of the safeguard that will be charged to HCFA. This is the percentage of cost that HCFA will carry for safeguards that will be shared between HCFA Medicare systems and corporate systems.

c) Determine **Percent HCFA Cost applied to this contract control number.** This is the percentage of cost of the safeguard that will be charged to *this* HCFA contract control number. This is the percentage of cost that this HCFA contract control number will carry for safeguards that will be shared between HCFA (Medicare) contract control numbers.

d) Determine **Shared Cost Contract control numbers.** This is a listing of all of the HCFA contract control numbers that will share the cost of this safeguard. The totals of the "percent HCFA Cost Applied to this contract" for this safeguard in each of the contractor self-assessment costing estimate should equal the total cost to HCFA for this safeguard. The percent "HCFA Cost applied to this contract" for each of the applicable contractors should total 100 percent for this safeguard.

e) Determine **Safeguard Type.** This is the type of safeguard that is planned. The user will choose from a dropdown list of safeguard type that includes Outsource, Hardware, Software, Facilities, and/or Personnel. The safeguard can be of any combination of one or more of the four possibilities. This information is used by HCFA to determine approximately where requested monies will be applied.

f) Determine **Responsibility.** This assigns responsibility to either the entity performing the self-assessment (you), or to the Standard System Maintainer (for Standard Systems Software changes required for meeting this CSR).

g) Determine **Projected Recurring Cost.** This is the projected recurring cost to HCFA to maintain this Safeguard for the following FY.

3) **Prioritize** safeguards. This is the ranking of priority of each safeguard as perceived by you (the Business Partner). *Note: One way of assigning Priority might be to compare the potential Annual Loss Exposure (possibly derived from your triennial risk assessment) of not installing this safeguard. The safeguards with a higher Annual Loss Exposure would be the higher priority safeguards.*

F) Populate the Database

1) Input all of the safeguards into the database.

a) By inputting the safeguards first, they will be readily available during the entry of CSR status entries (which will include a pointer to the applicable safeguard).

2) Input all of the CSR compliance descriptions and status's.

a) Ensure that each CSRs entry includes:

(1) A selected STATUS

(2) A complete description of the safeguards in place currently to meet this requirement. See appendix A of the *HCFA/Business Partners Systems Security Manual.*

(3) .At least one safeguard for each CSR answered as PLANNED, PARTIAL, or NO.

(4) Any notes associated with the CSR. *NOTE: These notes are for local use only. They are not to be used for amplifying information to HCFA.*

(5) Enter any *Projected Completion Dates* for each CSR answered as PLANNED, PARTIAL, or NO.

G) Print out a report (automatically filled-in) of your entire self-assessment.

1) Review with team members.

2) Adjust as required.

a) Adjustments require a new entry in the applicable CSR form. The CAST tool does not allow editing of entries after they are entered.

3) Review with management.

H) Submit to HCFA including:

1) A printed copy of the self-assessment
2) The complete CAST_BE.mdb database

Attachment B

HCFA

Health Care Financing Administration

BUSINESS PARTNERS
SYSTEM SECURITY PLAN ARCHITECTURE
WORKSHEET
AND
INSTRUCTION
MANUAL

MARCH, 2001

TABLE OF CONTENTS

INTRODUCTION 3
DETAILED INSTRUCTIONS...3
EXISTING SYSTEM SECURITY PLANS 4
HIGH LEVEL DIAGRAM...5
ADDITIONAL INFORMATION 5
APPENDIX A - WORKSHEET..6
APPENDIX B - SSP MATRIX 10

INTRODUCTION

Systems Security Plans (SSP) must cover every system that processes Medicare data. It is recognized that this will require several, perhaps, many security plans depending on the nature, extent, and mode of operation of your Medicare business. HCFA will not be able to provide sufficient funds in FY 2001 to develop all the necessary plans. Instead, you are required to prepare a security plan architecture in which you will identify which of your systems require a plan and for which you will provide an estimate of the cost to develop the security plans in FY 2002.

At the highest level is the Master System Security Plan. The master plan follows the same format as all the system security plans and defines the enterprise-level security controls that are in place within your company. The master plan will contain all the security attributes that are standard enterprise-wide such as personnel controls, physical controls for the site, disaster recovery, etc. What this means is an SSP created by an individual organization inherits the attributes of the master plan and needs only to reference it without repeating the details. When the master plan is modified, all those plans that are dependent will not have to be changed.

At the next level are the General Support System (GSS) and Major Application (MA) System Security Plans.

This document provides detailed instructions that Business Partners must follow when completing their System Security Plan Architecture. For completeness purposes you must follow the instructions carefully.

NOTE: All funding requirements for these System Security Plans need to be aligned (and included) with the safeguard for Core Security Requirement 1.10.4 in the CAST tool.

DETAILED INSTRUCTIONS

Step 1

In the spaces provided below, in Table 1, list the contractor control numbers for each of your HCFA Medicare contracts.

Table 1 - HCFA Contractor Control Number

Step 2

Review the HCFA Security Plans (SSP) Methodology dated December 2000. Additionally, it is highly recommended that if you are not familiar with developing system security plans that you review the documents listed in the additional information section at the end of this document. The HCFA Systems Security Plan Methodology is available at www.hcfa.gov/extpart.

Step 3

Complete a worksheet (see Appendix A) for each of the contractor control numbers listed in Table 1 above.

Step 4

Download the System Security Plan Architecture template from www.hcfa.gov/extpart. This document template is in MS© Word format. Use the information on the worksheets to assist you in completing the template.

Step 5

Complete the SSP MATRIX (see Appendix B) for each contract control number.

In the first column of this table list the General Support System or Major Applications used in support of your HCFA Medicare contract. In the second column of this table, indicate whether or not you have an existing SSP.

EXISTING SYSTEM SECURITY PLANS

In the event that you already have current system-specific security plans that satisfy HCFA requirements, you do not need to develop new ones. Medicare contractors, however, should reference standard system maintainers, claims processing data centers and CWF host sites' systems security plans in their IT system security plans that impact their security plan architecture. You should also prepare a crosswalk to the features of those security plans to the core security requirements that facilitate compliance assessments.

Step 6

HIGH LEVEL DIAGRAM

Each contractor shall include a one-page high-level diagram of system connectivity and external connections. The drawing shall include all communication paths and circuits used for the interconnection beginning with the contractor-owned system(s) traversing through all interconnected systems to the non-contractor end-point. The diagram should support our understanding of the contractor systems security architecture.

The drawing should depict the logical location of all components. (e.g., mainframe computers, host processors, hubs, firewalls, encryption devices, routers, frame relay devices, secure frame units (SFU), communications service units (CSU), data service units (DSU), etc.)

ADDITIONAL INFORMATION

The following documents should be used for additional guidance while developing this architecture:

- Swanson, Marianne. *Guide for Developing* **{***PRIVATE* **}***Security Plans for Information Technology Systems*. Special Publication 800-18. National Institute of Standards and Technology, December 1998.

http://csrc.nist.gov/nistpubs/Planguide.PDF

- Swanson, Marianne and Guttman, Barbara. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Special Publication 800-14. National Institute of Standards and Technology, September 1996.

http://csrc.nist.gov

- *System Security Plans (SSP) Methodology*. Health Care Financing Administration, December 2000.

http://www.hcfa.gov/extpart.

APPENDIX A

WORKSHEET	INSTRUCTIONS
GENERAL INFORMATION	
COMPANY NAME:	Enter your company' s Name.
LIST CONTRACTOR CONTROL NUMBER:	Each HCFA contract is assigned a unique Contractor Control Number or contract number. This number may be a combination of alphabetic and numeric characters and can be used in combination with the system name. In this section list the unique control or contract number for your system.
TYPE OF CONTRACT:	In this field, enter the type of contract (i.e., Part A, Part B, DMERC, CWF Host site, etc.).
COMPANY ADDRESS:	Enter your company' s street address, city, state and zip code.
RESPONSIBLE ORGANIZATION	
SSO NAME:	This part specifies the Business Partner SSO responsible for the system being reported. Be specific about the organization and do not abbreviate.
SSO PHONE NUMBER:	
SSO E-MAIL ADDRESS:	
CONTRACTUAL DESCRIPTION	
MEDICARE CONTRACT RESPONSIBILITIES:	Define the functions and the entities served by this contract. Example: "Part A processor for MA, MN, NH, and VT."

WORKSHEET	INSTRUCTIONS
DATA CENTER(S): MEDICARE CLAIMS DATA CENTER: CORPORATE DATA CENTER: CORPORATE DATA CENTER FUNCTIONS:	Enter the name and location of the data center(s) used for your Medicare Claims processing. *If Medicare Data is in anyway used on your corporate data center include the name and location.*
STANDARD SYSTEM(S):	Enter all Standard System(s) used to support this contract. The Standard Systems used during Medicare Claims processing are FISS, VMS, CWF, APASS, MCS, GTEMS and HPBSS.
PROCESSING SYSTEMS GENERAL ARCHITECTURE	
MAJOR SYSTEM PLATFORMS:	IBM 3090 would be an example of major system platform.
MAJOR SYSTEMS SOFTWARE:	OS/3090, UNIX, RACF, Oracle®, MS SQL-Server®, etc. would be examples of major system software.
MAJOR SYSTEM APPLICATIONS:	Examples of major system applications are e-mail, web host, dial-in host, PeopleSoft, SAP, etc.

HCFA

APPENDIX B

HCFA

SSP MATRIX

GENERAL SUPPORT SYSTEMS	EXISTING SSP (Yes/No)	DATE OF LAST UPDATE

A General Support System (GSS) consists of interconnected information resources under the same direct management control that shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and people and provides general support for a variety of users and/or applications. As a rule of thumb, think of a GSS as the physical platform upon which applications run.

MAJOR APPLICATIONS	EXISTING SSP (Yes/No)	DATE OF LAST UPDATE

Major Applications (MA) are systems, usually software applications, that perform clearly defined functions for which there are readily identifiable security considerations and needs. (e.g., SAP, People Soft, etc.) A major application might be comprised many individual programs and might have hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function.

Specific security plans for other applications are not required because the security controls for those applications or systems would be provided by the general support systems in which they operate. For example, a department-wide financial management system would be a major application requiring its own security plan. A local program designed to track expenditures against an office budget might not be considered a major application and would be covered by a general support system security plan for an office automation system or a local area network**{** XE "local area network" **}** (LAN). Standard commercial off-the-shelf software (such as word processing**{** XE "processing" **}** software, electronic mail software, utility software, or other general- purpose software) would not typically be considered a major application and would be covered by the plans for the general support system on which they are installed.