Program Memorandum Intermediaries/Carriers

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal AB-02-019 **Date: FEBRUARY 8, 2002**

CHANGE REQUEST 2010

SUBJECT: Supplemental Systems Security Information For FY 02

This Program Memorandum (PM) provides supplemental instruction on the implementation of new or revised CMS Business Partner Systems Security Manual (BPSSM) requirements. It applies to all carriers, intermediaries, their data centers, DMERCs, and standard systems maintainers.

Updated Requirements

CMS's Business Partner Systems Security Manual has been revised:

- Core Security Requirements have been updated and revised.
- Contingency Plan Methodology has been updated.
- Annual Compliance Audit requirements from PM AB-01-136 (CR 1844) are made permanent.

CMS has also modified its methodology for preparing systems security plans (SSP). Use Systems Security Plans (SSP)Methodology, Final Version 2, December 11, 2001 in preparing your systems security plans. Version 2 simplifies many of the steps in preparing an SSP.

You should review both the Manual and the SSP Methodology and then adjust your policies and procedures accordingly.

Contingency Plan Methodology

You do not have to revise your Contingency Plans to apply the new methodology until your annual review reveals that your risk contingency plan needs substantial modification.

Core Security Requirements Assessment

You must review your Core Security Requirements Assessment (BPSSM, Section 3) to verify that all information is current and correct. CMS will provide you with its own assessment of your FY 01 Core Security Requirements assessment (CAST submission) and with our independent verification and validation contractor's assessment. You should review both assessments and make all appropriate revisions prior to submitting your Core Security Requirements (CAST) to CMS by May 31, 2002. Use CAST v.2 for this submission. CMS will use your information to make its productivity investment funding decisions on systems security for FY 03.

Annual Compliance Audit for FY 02

BPSSM (Section 3.5) states that you must focus the audit on 4 categories of the core security requirements specified in advance by CMS. The 4 categories that must be audited in FY 02 are Entity-wide Security Program Planning and Management; System Software; Application Authorization Controls; and Networks.

Summary of Key Dates

- Conduct your core security requirements self-assessment and submit CAST - by May 31, 2002.
- Conduct your Annual Compliance Audit - No later than September 30, 2002.
- Conduct your Triennial Risk Assessment or update review - No later than September 30, 2002. (Note that the methodology to perform the risk assessment has not been changed.)
- Update your Contingency Plan and conduct test - No later than September 30, 2002.

CMS-Pub. 60AB

Security Questions and Concerns

CMS expects that you may have questions or concerns about the BPSSM revision, CAST or this PM. You may send them to ContractorSystemsSecurity@CMS.hhs.gov. We will provide a prompt direct response as well as posting it to a Frequently Asked Questions (FAQ) section on the CMS Medicare Contractor Information Systems Security web page. Its address is: http://www.HCFA.gov/EXTPART.

The *effective date* for this PM is February 8, 2002.

The *implementation date* for this PM is February 8, 2002.

These instructions should be implemented within your current operating budget.

This PM may be discarded after December 31, 2003.

If you have any questions, contact ContractorSystemsSecurity@CMS.hhs.gov**.**