Program Memorandum Intermediaries/Carriers

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

Transmittal AB-03-005 **Date: JANUARY 24, 2003**

CHANGE REQUEST 2518

SUBJECT: FY 2003 Systems Security Activities and Due Dates

The purpose of the Program Memorandum (PM) is to provide information and instructions on the security activities to be performed in FY 2003.

RISK ASSESSMENT AND SYSTEM SECURITY PLAN (SSP) DEVELOPMENT

In FY 2002, you were funded to develop an SSP(s) for your Medicare claims processing system(s). Training on the CMS SSP Methodology was provided in November and December 2002. The methodology required you to certify that your SSP complies with CMS requirements. The signed original CMS SSP Certification Form (TAB A, Appendix A of the CMS SSP Template) must be sent to CMS by close of business June 30, 2003. A copy of the CMS SSP Certification Form should be placed in your Systems Security Profile along with the SSP(s).

As briefed to you in the training, Version 3.0 of the System Security Plan Methodology and Version 1.1 of the CMS Information Security Risk Assessment Methodology should be used to perform the risk assessment and develop the required system security plans. The risk assessment used to support your system security plan(s) cannot be dated more than 12 months earlier than the SSP certification date.

Previously developed SSPs (should you have them) must be reviewed, updated (if necessary) and recertified 1 year after they were initially certified. A risk assessment should also be performed upon significant change. The signed original CMS SSP Certification Form (TAB A, Appendix A of the CMS SSP Template) must be received by CMS by the date of expiration. A copy of the CMS SSP Certification Form should be placed in your Systems Security Profile.

Should you require SSP technical assistance, direct your questions to: CyberTyger@cms.hhs.gov or to (703) 205-6006.

CONTRACTOR ASSESSMENT SECURITY TOOL (CAST)

The CMS will release CAST Version 3.0 to you during the second quarter of FY 2003. You must complete the CAST and submit a copy on CD-ROM to central office and your consortia contractor management officer (CCMO) or project officer (PO) by close of business *July 15, 2003*. A copy of the CAST should also be placed in your Systems Security Profile.

COMPLIANCE

The annual compliance audit (ACA) (Section 3. 5 of the Business Partners Systems Security Manual) must be completed by *September 30, 2003*. The categories of the CMS Core Security Requirements (CSR) to be audited this year are: *access controls, application systems completeness controls, and application system accuracy controls*. In lieu of auditing a fourth category of CSRs, your audit should review the implementation of your funded FY 2002 safeguards and SSPs. The audit should (1) assess the reasonableness of the safeguard to the CSR; (2) assess the reasonableness of the implementation cost (estimated or actual); (3) assess the reasonableness of the project plans to complete the safeguard; (4) assess the effectiveness of the implementation of the safeguard; and (5) assess the compliance of the SSP with CMS' SSP methodology and your adherence to the policies, procedures and controls set forth in the SSP. We recently released a letter to you, dated December 3, 2002, defining the requirement to add safeguards and SSP implementation to your ACA. This PM affirms that requirement.

The ACA should also assess the reasonableness and effectiveness of the corrective action plans (CAPs) developed as a result of any CMS directed Statement on Audit Standards No. 70 (SAS 70) and/or Office of Inspector General Chief Financial Officer's Electronic Data Processing Control (OIG CFO EDP) audit finding(s). The ACA should include a recommendation of whether the CAP implementation closes the finding(s).

The second component of compliance (found in Section 3.5 of the BPSSM) also requires the preparation a Corrective Action Plan (CAP). CAPs should be prepared within 10 working days after the completion of the ACA for any deficiencies noted. Medicare contractors should contact their respective CCMO or PO to determine what items should be submitted. A copy of the completed ACA and CAP should be placed in the Systems Security Profile, as well as submitted to your CCMO or PO by *October 15, 2003.*

We recommend the ACA report be organized by subject matter to facilitate the ease of review and use. The categories should include (1) CAST CSR Categories, (2) Funded FY02 Safeguards/SSPs, (3) OIG CFO EDP audit, (4) SAS 70 review and (5) any miscellaneous issues not covered by the above categories.

INFORMATION TECHNOLOGY (IT) SYSTEMS CONTINGENCY PLANS

IT Systems Contingency Plans must be reviewed, tested and updated (if necessary) (Section 3.4 of the BPSSM). Business partner's management and the system security officer (SSO) must approve updated IT systems contingency plans. Updated plans and test reports (results) should be placed in your Systems Security Profile.

Security Questions and Concerns

If you have questions about this PM, send them to CyberTyger@cms.hhs.gov.

The *effective date* for this PM is January 24, 2003.

The *implementation date* for this PM is February 24, 2003.

These instructions should be implemented within your current operating budget.

This PM may be discarded after November 30, 2003.

If you have any questions, contact Sherwin Schulterbrandt at sschulterbrandt@cms.hhs.gov or 410-786-0743.