Program Memorandum Intermediaries/Carriers

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

Transmittal AB-01-136 **Date: SEPTEMBER 25, 2001**

CHANGE REQUEST 1844

SUBJECT: Supplemental Instructions on CMS Business Partners Systems Security Requirements

The purpose of this Program Memorandum (PM) is to provide supplemental instructions on two aspects of the business partners security initiative:

- Annual Compliance Audit; and
- FY 01 Medicare Contractor Self-Assessment Funding.

I. Annual Compliance Audit

An Annual Compliance Audit has been a CMS systems security requirement for many years. The CMS Business Partner Systems Security Manual continues this requirement. The Manual modified the old requirement by:

- Specifying that the audit should be conducted by an independent entity;
- Specifying that the audit should be directed by an accredited systems security professional; and
- Limiting the scope of the audit to a subset of core security requirements selected by CMS. Annually, CMS would notify business partners of which core security requirements (CSRs) are to be audited. The four categories that must be audited in FY 01 are: access control; segregation of duties; service continuity; and application software development and change control.

Many business partners have begun to prepare for the Annual Compliance Audit and have requested clearer specifications on the nature and scope expected of the audit. A compliance audit is a performance review of a business partner's systems security program that tests whether the systems security controls comply with CMS's CSRs (Appendix A of the CMS Business Partners Systems Security Manual) and are implemented properly. The audit will be documented through an Annual Compliance Audit Report.

1. The Annual Compliance Audit Report must include the following:

- **A Summary of Controls:** These controls are those instructions the business partner has implemented to comply with the CMS CSRs. The summary of controls should be derived from the source documentation referenced in the Contractor Assessment Security Tool (CAST).
- **A Description of Review Procedures and Tests:** This description must include procedures and tests performed by the organization (internal or external) performing the annual compliance audit as well as a description of the results of such tests.

2. A SAS-70 audit will meet the requirement for the Annual Compliance Audit as defined in the HCFA/External Business Partners Systems Security Manual. If a SAS-70 audit is to be used to meet the requirements for the Annual Compliance Audit in FY 01, **the SAS-70 audit MUST have been directed by CMS and must have been performed for FY 01**.

No opinion or other information (typically included in a SAS-70 if relied upon for purposes of the annual compliance audit) is required. The primary objective of the audit is to report on compliance with CMS's Systems Security Requirements as defined in the CMS Business Partners Systems Security Manual (www.hcfa.gov/pubforms/84_ssm/bp_sys_security_manual.htm).

The SAS-70 alternative shown above is due to the time and resources associated with performing a redundant audit. **It should be noted that per PM AB-01-11, the Annual Compliance Audit is to be completed "No Later Than September 30, 2001". We are extending that due date for the FY 01 requirement to November 15, 2001, to ensure compliance with the specifications above.**

II. FY 01 Medicare Contractor Self-Assessment Funding

In order to perform the systems security self-assessment process, CMS provided funding to each Medicare contractor/business partner. Not all allocated funding may have been used for the self-assessment process. **If any funds from the initial allocation are remaining, the funds are to be used to initiate activities related to the development of a Master System Security Plan.** The development of a Master System Security Plan by each business partner will be a major focus of CMS in FY 02 and FY 03.

For additional information on developing a Master System Security Plan (and its hierarchical relationship to general support systems and major applications, see section 3.1 of the Business Partners Systems Security Manual and the system security plans methodology, December 2000 version at: www.hcfa.gov/extpart.

Systems Security Questions and Concerns

CMS expects that you may have questions or concerns about the supplemental instructions provided in this PM. You may send them directly to: contractorsystemssecurity@hcfa.gov or use the question form provided at the Medicare Contractor Systems Security Web site at: www.hcfa.gov/extpart. We will provide a prompt, direct response as well as posting it to a Frequently Asked Questions (FAQ) page on the Web site.

The *effective date* for this PM is September 25, 2001.

The *implementation date* for this PM is September 25, 2001.

These instructions should be implemented within your current operating budget.

This PM may be discarded after September 30, 2002.

If you have any questions, contact Peter Koza at (410) 786-2630