Attachment B

INSTRUCTIONS FOR SECURITY CONTROL TESTING

BACKGROUND

In accordance with both the Federal Information Security Act of 2002 (FISMA) and the Federal Managers' Financial Integrity Act of 1982 (FMFIA), it is incumbent upon certification officials, business owners, and system developers/maintainers of CMS systems, which have been identified for FISMA reporting, to test their internal controls at least annually. While it is infeasible to completely test every control for every CMS application annually, each application within a major application family and each general support system must have at least a subset of controls tested annually. It is in CMS' best interests to ensure uniformity in quality and approach in fulfilling this responsibility. Hence, the remainder of this Attachment is dedicated to assisting you to successfully test your internal security controls through a standardized process.

GETTING STARTED

OIS has published several methodologies as well as a reporting standard to guide the performance of System Test and Evaluation (ST&E) across the CMS in a standardized fashion. These documents should also be used to guide annual testing of security controls. It is important that the annual testing be conducted in accordance with the tenets of the established ST&E program to ensure uniformity and consistency in security testing. Tools that will be helpful to you in meeting this objective are available for download from the CMS Internet site. Titles to become familiar with include:

- *CMS Information Security Acceptable Risk Safeguards*
- *CMS Reporting Standard for Information Security Testing*
- *CMS Information Security Testing Approach*
- *CMS Reporting Standard for Information Security Testing*
- *CMS Information Security Certification and Accreditation (C&A) Program Procedure*

Before beginning your testing, be sure to check the CMS virtual handbook of security policies, procedures, standards and methodologies to ensure you are working with the most current versions of these documents. The virtual handbook is located at: http://www.cms.hhs.gov/informationsecurity/01_overview.asp

In addition, the National Institute of Standards and Technology's (NIST) Computer Security Resource Center (CSRC) provides excellent reference material for constructing the security test plan. The site may be accessed at: http://www.csrc.nist.gov/ . Two particularly instructive NIST Special Publications (SP) are:

- *NIST SP 800-53, Revision 1 Recommended Security Controls for Federal Information System, which may be downloaded at: http://www.csrc.nist.gov/publications/nistpubs/index.html*

- Draft NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information System*, which may be downloaded at: http://csrc.nist.gov/publications/drafts.html

Using these resources, the CMS business owner or his/her designates are supplied with a framework upon which to develop the scope of the annual testing; establish the test plan and script(s); execute the test; and document the test result. The Enterprise Architecture and Strategy Group, OIS ensures that the CMS-developed reference publications are regularly reviewed and updated in line with HHS and other federal mandates.

The purpose of testing is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. At CMS, the minimum safeguards that every system must meet are documented in the Acceptable Risk Safeguards (ARS). This document has been re-written to align with the NIST SP 800-53, Revision 1 compliance with which has become mandatory under Federal Information Processing Standard Pub 200 *Minimum Security Requirements for Federal Information and Information Systems*. We recommend using NIST SP 800-53, Revision 1, as well as the CMS ARS as your reference standards when developing your testing plan.

BUILDING THE TESTING PLAN

OIS advises leveraging the standards apportioned among seventeen control families contained in NIST SP 800-53 as well as the CMS ARS as the minimum standards against which to formulate the testing. Appropriate system management, typically the business owner and system maintainer, need to review these categories and identify the suite of Management, Operational, and Technical controls that will be examined and analyzed in the operational environment.

Once the controls have been selected, a test plan is developed. The test plan outlines general testing actions, such as the tools to be used, the types of assessment methods to be used, interview topics, test timeframes, test participants, requests for documentation, meetings and related information, which will govern the execution of the testing. Having established this general framework for the test, NIST SP 800-53A may be leveraged to construct the associated test script, which contains the detailed activities that will be performed to assess the effectiveness of the implemented control.

Several controls within NIST SP 800-53 require CMS to provide thresholds for its systems. If these controls are identified for inclusion in your test plan, please refer to version 3.0 of the CMS ARS or contact Maria McMahon, 410-786-3023, within the DITPPA for this information. In our example below, a control that requires a CMS-defined threshold is used. In this instance, CMS has defined 15 minutes as its organizational threshold.

To illustrate the process, we assume that the appropriate system management of a moderate impact level system has included the following access control (AC) standard in its testing:

AC-12 Session Termination:

The information system automatically terminates a session after 15 minutes of inactivity.

To assess the effectiveness of this – or any – security control, the tester may use a combination of techniques, as described in NIST 800-53A. For convenience, they are summarized for you below[1].

Assessment Method	***Definition***
Interview	The process of conducting focused discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.
Examine	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects[2] to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.
Test	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of the security control effectiveness.

Using each of these assessment methods, the testers would perform the following steps to assess the effectiveness of AC-12 in its operational environment:

- ✓ Step 1: **Interview** a sample of personnel to confirm that sessions are disconnected forcibly after fifteen (15) minutes of inactivity.
- ✓ Step 2: Examine the configuration settings of the information system to determine if the system automatically terminates a session after 15 minutes of inactivity.
- ✓ Step 3: **Test** the session termination mechanism by allowing a valid user session to remain inactive 15 minutes to determine if the session automatically terminates.
- ✓ Step 4: **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that session terminations are implemented correctly within the information system.

The steps listed above comprise the annual test script. In developing the full annual test script, a representative sampling of standards are selected and assessed in this manner.

[1] NIST SP 800-53A *Guide for Assessing Security Controls in Federal Information Systems,* http://www.csrc.nist.gov/publications/drafts/sp800-53A-ipd.pdf

[2] An assessment object is defined as any or a combination of the following: a specifications (e.g., policies, plans, procedures, system requirements, designs); mechanisms (e.g., hardware, software, firmware, physical devices); or activities (e.g., system operations/administration/management, exercises, drills).

As each test scenario is executed, the tester documents the results of each step. The interview notes, screen shots, procedure documents, et al, that accompany the test activity are collectively known as “working papers” and need to be retained along with the final report. Any gaps between the protections provided the system by the implemented control and the protection afforded the system through full compliance with the security standard needs to be noted as a ‘finding’.

The CMS reporting standard provides a format for documenting all aspects of the annual testing as well as information for determining both the risk a finding presents to CMS data as well as determining the level of effort associated with a risk mitigation activity. Both the system accreditation and on-going FISMA compliance ultimately rely on the successful completion of the selected test scenarios and objectives as documented in the annual test plan, associated test script(s), and the resulting test report. The test results are used to identify and document security findings that present risk to the system. Findings that are not closed during the testing period of performance need to be tracked through the Plan of Actions and Milestones (POA&M) process. Any risks that are accepted by the business owner need to be formally documented and accounted for in the applicable Information Security Risk Assessment and associated System Security Plan.

CORRECTIVE ACTION PLAN MANAGEMENT AND POA&M REPORTING

When gaps in control functionality exist, they must be tracked and reported to the Department of Health and Human Services (DHHS) through the CMS Plan of Action and Milestones (POA&M) process. The POA&M reporting process is well established at CMS and operates under the *CMS Information Security Plan of Action & Milestones (POA&M) Guidelines*. The Enterprise Architecture & Strategy Group (EASG), Division of IT Policy, Procedures, and Audits (DITPPA), supports the process.

Subsequently, when findings are not closed during the testing period of performance, the business owner needs to develop corrective action plans (CAP) for their remediation. The status of each CAP needs to be reported to DHHS quarterly through the POA&M process. Timeliness of CAP creation and compliance with the actions and timeframes established for the risk mitigation activities are critical elements evaluated by the Office of Inspector General (OIG) during the FISMA audit and by DHHS on a quarterly basis. Based on feedback from prior reviews, an acceptable timeframe for CAP creation and reporting in the POA&M is 30 days after the finding is discovered and reported to management. Priority of effort should be given to high level findings.

OIS monitors the receipt of CAPs for formal, independent, ST&E performed under contract. It is incumbent upon certification officials, business owners and system developers/maintainers to ensure that EASG/DITPPA is kept current on the status of new and existing CAPs resulting from your annual testing. While this information will be accepted on a flow basis, at least quarterly DITPPA will survey business owners for this information. CAPs should be entered directly into the CMS Integrated Security Suite (CISS) tool. Most components have had training and already have access to the CISS tool, and this is the management tool of choice going forward for CAP management in CMS. Points of Contact for each FISMA reported system are available to assist in the CISS entries. Owners of findings will need to work with their POCs to ensure the appropriate entries are made into the CISS. Please contact Desmond Young, 410-786-5113, for any clarification that is needed on the CAP management process. Mr. Young also helps review CISS CAP entries on a flow basis.

TESTING OPTIONS

Testing processes, including for formal ST&E, as well as the CAP management and POA&M reporting processes are well-established at the CMS and numerous resources are available to respond to inquiries in these areas. The CMS business owners and his or her delegates have been intimately involved in the testing processes, especially the independent ST&E leading to certification and accreditation. For example, the business owners are responsible for ensuring the adequacy of the testing scope, assigning resources to participate in the testing process, taking appropriate action to remedy identified findings, and tracking their remediation through the POA&M process. To fulfill the obligation for annual testing, the CMS business owner may either:

- Contract for these services with an external contractor; or
- Form a local test team, provided the test participants are not directly responsible for implementing the controls that are to be tested.

Both options require adherence to the CMS testing process as outlined in this attachment and detailed in the identified reference materials. Further, both options require participation of the Business Owner, and System Developer/Maintainer or their designees to answer inquiries, provide documentation, provide access to information system resources for testing, track and remedy testing findings via the CAP management process, and so on.

When using either contractors or a local team of resources to perform these services, it is important that both electronic and hard copies of all test reports, test plans, test scripts, working papers, and CAP management worksheets be maintained by business owners and system developers/maintainers for inclusion in the system’s file. If testing meets requirements to qualify as an independent ST&E, the tests should also be retained in the system or application Certification and Accreditation (C&A) file. A copy of the C&A file is required to be provided to the Chief Information Officer (CIO) to support system accreditation, re-accreditation, and authority to operate decisions. In addition, you may anticipate that auditors, such as the OIG in support of FISMA, will requested this information as they have in each of the past several years.

INDEPENDENCE REQUIREMENTS

In order to ensure that the testing meets independence requirements to be considered a formal ST&E, neither contractor resources nor CMS resources used to test a control may be responsible for the implementation of the control. If a contractor is the developer/maintainer of a CMS application, for example, then security testing performed by that contractor may not be used to meet CMS’ ST&E requirement. Similarly, a local system administrator may not perform security testing to ensure unnecessary services have been removed from a server within that administrator’s purview to fulfill the ST&E requirement. While removing unnecessary services is an integral part of a system administrator's responsibilities, their removal needs to be validated by an independent party.

One option for assuring independence requirements are met is to leverage local test teams across components. For example, Division A would test Division B's applications; and vice versa. Hence, OIS strongly advises developing agreements to ensure that testing is performed by independent parties. Leveraging teams in the suggested manner strengthens CMS's ability both to use in-house resources to perform ST&Es and to demonstrate to our auditors that such use meets the independence requirement.

Absent an internal arrangement as described, independence may be achieved by contracting with an independent third party. Historically, OIS has leveraged independent contractors to perform ST&Es on its behalf. If you choose this option, examples of previous statements of work (SOW) for performing ST&Es directly may be obtained from contracts. Please contact Carolyn Robinson, 410-786-7677, for an illustrative SOW and associated Rules of Behavior.

Annual security controls testing may also be used to satisfy the requirements for the Security Testing and Evaluation (ST&E) which is an integral component of the CMS Certification and Accreditation (C&A) Program. In order to be considered as part of a system's or application's ST&E, the annual security control testing must meet standards for independence. The testing must also be performed and documented according to the CMS standards.

TESTING THAT MAY BE USED TO FULFILL THE ANNUAL REQUIREMENT

All management directed testing may be used to meet the requirement for annual security controls testing. Management directed testing includes independent ST&E tests, testing performed pursuant to CMS compliance with OMB Circular A-123, evaluations and tests conducted under authority of Section 912 of the Medicare Modernization Act, SAS-70 internal control reviews, and testing results from local test teams organized for purposes of meeting this requirement.

Local test teams must ensure that the testing participants are not directly responsible for implementing the control that is being tested. Testing of electronic data processing controls conducted pursuant to the Chief Financial Officer audit of CMS financial statements may **not** be used. This testing is directed by the OIG.

During FY 2007, except for testing of contingency plans, most business owners and developers/maintainers used inherited tests, especially tests of enterprise or infrastructure controls for the general support system (GSS) platforms upon which their applications reside, to meet the annual testing requirement. OIS will again provide information regarding the particular controls tested for the GSS platforms for the Enterprise Data Centers (EDC) in Baltimore, Maryland; Columbia, South Carolina; and Tulsa, Oklahoma; and the legacy data centers processing Medicare claims data. Whereas a number of technical controls are continuously monitored for each of these platform systems, such as denial of service and malicious code protection activities, intrusion detection monitoring, review of log files etc., your testing of these controls would be redundant to efforts that are already underway. In this regard, we recommend against utilizing such testing as the sole basis for your compliance, especially if these tests were part of your testing plan last year. Instead, we recommend your efforts be on those application or system specific controls not covered by the enterprise or infrastructure tests. For example, there would be value in testing your procedures for change management or the appropriateness and currency of your access controls including procedures to limit developers from production data, if these controls have not otherwise been tested this year. Testing of application specific controls will help ensure that the testing covers all applicable controls over a three year period.

In addition to testing of system and application specific controls, applications and systems hosted at the Baltimore EDC may inherit tests of enterprise controls for personnel security and physical security that are being planned this fiscal year by the OIS with the cooperation of the Office of Operations Management (OOM). OOM has the lead within CMS for personnel and physical security for the Baltimore complex. Controls for personnel and physical security are documented in the CMS Master Security Plan and are not ordinarily described in individual GSS or Major Application system security plans.