

DEPARTMENT OF HEALTH & HUMAN SERVICES  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard, Mail Stop N3-15-25  
Baltimore, Maryland 21244-1850




**OFFICE OF INFORMATION SERVICES**

---

**DEC 10 2007**

**CIO DIRECTIVE 07-05**

**TO:** CMS Centers and Office Directors

**FROM:** Julia Boughn  
CMS Chief Information Officer (CIO) and  
Director, Office of Information Services (OIS) 

**SUBJECT:** FY 2008 Annual Security Controls Testing--ACTION

**Background**

A critical factor for maintaining on-going compliance with Federal Information System Management Act (FISMA) of 2002, and the Federal Managers' Financial Integrity Act of 1982, is for business owners in coordination with developers/maintainers, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing), and person hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of corrective action plans for vulnerabilities noted during the testing.

The primary objective of the annual testing is to ensure that security controls are functioning as intended to protect the confidentiality, integrity and availability of the CMS information and information systems. A subset of controls in each application must be tested at a minimum each year. This is inclusive of the required annual test of the system or application contingency plan.

The annual test is intended to determine the extent to which the controls;

- ▶ are implemented correctly,
- ▶ operating as intended, and
- ▶ producing the desired outcome with respect to meeting the security requirements for the system.

The annual requirement has been interpreted by the Office of Management and Budget (OMB) as being within 365 calendar days of the prior test. Over a three year period **all** controls applicable to the system or application, as set forth in the *CMS Information Security Acceptable Risk Safeguards (ARS)*, must be tested. As the business owners, in coordination with the developer/maintainers of CMS applications and systems, it is your responsibility to meet this requirement.

### **Purpose**

This directive is to announce and provide instructions for the FY 2008 annual security controls testing. It requires action on the part the business owners of CMS applications and systems as reported under FISMA. Application and system developers/maintainers may assist in meeting the requirements. Completion of this requirement will be reported to the Department of Health and Human Services (DHHS) as part our FISMA compliance using the Department provided ProSight software. The results of this testing will also be reviewed by the Office of the Inspector General as part of their review of CMS FISMA compliance.

For each FISMA system, business owners are required to submit an attestation memorandum. To simplify CMS' reporting to DHHS and under FISMA, we request only one attestation for each FISMA reported system is submitted at the boxtop level. The certification officials and business owners for each FISMA reported system are responsible to coordinate and submit the required attestation.

Please submit this attestation to Sally Good-Burton, Director, Enterprise Architecture and Strategy Group (EASG), OIS, with a cc: to Richard Lyman, Chief Information Security Officer (CISO).

To aid in meeting the annual testing requirement, we have attached several key documents:

- ▶ Attachment A is a list of the FISMA systems that are reported to the DHHS. This list also contains the latest testing dates for the annual and contingency plan testing requirements.
- ▶ Attachment B provides the instructions and information on “Getting Started” to meet the testing requirement including references to the applicable CMS standards that must be observed.
- ▶ Attachment C is a sample attestation memorandum.
- ▶ Attachment D is a list of controls, as set forth in the CMS ARS, which may be tested. This list can be used to document your high level test plan showing the particular controls to be tested. Submission of this plan is not required, although a number of business owners did provide such plans last year.

**Timeframe**

There are two timeframes to be concerned with:

1. All FISMA systems with testing dates prior to May 30, 2007, must submit an updated attestation by April 30, 2008.
2. For systems with testing dates on Attachment A subsequent to April 30, 2007, an updated attestation should be submitted within 365 days of your prior test.

A meeting to brief the testing requirement will be scheduled by EASG following the release of this directive. In the interim, information on the security areas mentioned in this memoranda is available in the information security section of our website:

[www.cms.hhs.gov/informationsecurity](http://www.cms.hhs.gov/informationsecurity).

Questions may also be directed to Sally Good-Burton, Director, EASG, at 410-786-8227; or Dick Lyman, CISO, at 410-786-1934; or Maria McMahon, Technical Lead, EASG, at 410-786-3023.