OFFICE OF INFORMATION SERVICES

CIO DIRECTIVE 08-01

DATE: April 4, 2008

TO: CMS Centers and Office Directors
Consortia Administrators

FROM: Julie Boughn, CMS Chief Information Officer (CIO) &
Director, Office of Information Services (OIS) /s/ William Saunders for

SUBJECT: Annual Role-Based Information Security (IS) Training Requirements -- ACTION

Background

CMS is required to provide role-based IS training to employees and contractors who have specialized roles within CMS' IS program in accordance with the Federal Information Security Management Act (FISMA) of 2002 and 5 CFR 930, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems*. CMS is implementing annual IS training requirements for role-based groups that require minimum training hours to be received by means of professional development, certificate programs and/or traditional college credit courses. CMS encourages personnel to leverage training sessions that are offered by OIS, such as briefings, forums, seminars, Lunch & Learns, professional development workshops, conferences and approved professional independent reading and research. Such training will focus on improving the security skills and competencies of personnel managing, designing, developing, acquiring and administering CMS' information technology resources.

Purpose

The purpose of this directive is to implement mandatory role-based IS training requirements. This directive facilitates the development and strengthening of a comprehensive, measurable and cost-effective IS program which supports CMS' mission critical objectives and reinforces individual core competencies. Such measures also allow managers to identify training deficiencies and plan training schedules according to organizational priorities.

Timeframe

Training requirements are based upon a cycle that begins June 1st and ends May 31st of the subsequent year.

Role-based Minimum Requirements

CMS Policy for the Information Security Program (PISP) dated November 15, 2007, Section 5 outlines the roles and responsibilities of each entity that has specialized role-based duties. Table 1: Minimum role-based training requirements, depicts the specialized roles with the associated annual training requirements.

Table 1: Minimum role-based training requirements [1]

Specialized Roles	Minimum annual training requirements
Executives	1 hour
Chief Information Officer (CIO)	4 hours
Chief Technology Officer (CTO)	4 hours
Managers	4 hours
Information Systems Security Officers (ISSO)	6 hours
System/Database Administrators	6 hours
Chief Information Security Officer (CISO)	8 hours
IS Program Staff	8 hours

Required Documentation

Specialized role-based training verification must include:
- Date training was completed
- Description of course attended/completed
- Type of training
- Training hours completed

Verification of training will be requested by OIS annually through a separate data call letter.

Training Plan

Managers shall be held accountable for enforcing training requirements of subordinate personnel and are responsible for documenting an official training plan for each employee. The training plan must at least identify proposed training milestones that reflect minimum requirements. Individual training plans must be reviewed and approved by both management and the employee.

If you have any questions or require additional information, please contact Bill Pollak, Division of IT Policies, Procedures & Audits, Enterprise Architecture & Strategy Group, OIS at 410-786-3018 or William.Pollak@cms.hhs.gov. Thank you in advance for your prompt attention to this request.

---

[1] Revised per Dick Lyman, Chief Information Security Officer, as of July 24, 2008. Further refinements of this directive are anticipated in the near future.