

Department of Commerce

Commerce Interim

CITR-004

Technical Requirement

February 23, 2008

1. PURPOSE

This policy specifies requirements for the DOC Certification and Accreditation (C&A) process.

2. BACKGROUND

The Office of Management and Budget Information System Security Line Of Business (ISSLOB) on FISMA Reporting requires the use of a Shared Service Center (SSC) to strengthen the ability to identify and manage information security risks, to improve and make consistent and measurable information security processes and controls across an enterprise, and to achieve savings or cost-avoidance through reduced duplication and economies of scale. The DOC has implemented the Cyber Security Assessment and Management (CSAM) tool provided by the Department of Justice SSC in support of the ISSLOB goals.

3. SCOPE

These requirements apply to all unclassified information systems owned by or operated on behalf of DOC where the Department has the legal and/or contractual authority to dictate requirements. Classified information and systems are not within the scope of this document; however, unclassified information pertaining to the management of classified systems is within scope. The requirements herein apply only to systems for which certification and accreditation is required during FY 2009 and beyond, and where a material level of effort has not already been exerted on C&A activities.

4. AUTHORITY

The DOC Chief Information Officer (CIO) has the authority to develop, implement, and manage IT security processes and procedures to protect the availability, confidentiality, and integrity of the Department's IT resources. The DOC Chief Information Security Officer (CISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and Federal Information Security Management Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget (OMB) policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirements.

5. CANCELLATION OF EXISTING POLICY

This CITR will replace the following sections defined in the 2005 U.S. Department of Commerce IT Security Program Policy:

6.0 Certification, Accreditation, and Security Assessment

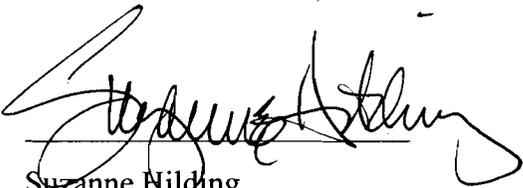
Appendix H: IT System Security Certification and Accreditation

6. POLICY

1. All Operating Units must follow NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* for the DOC C&A process.
2. Each DOC C&A package shall minimally contain artifacts¹ listed in Table 1.
 - a. OUs shall use a DOC template for artifacts designated with an “X” under the *Core* column. OUs may append structured content to the artifacts.
 - b. OUs shall use an OU-defined template for artifacts designated with an “X” under the *Information Requirement* column.
 - c. OUs shall use a DOC template for artifacts designated with an “X” in the *Contingent Format/DOC* column, when applicable. OUs may use an OU-defined template for artifacts designated with an “X” in the *Contingent Format/OU column*, when applicable.
3. OUs shall integrate the Cyber Security Assessment & Management (CSAM) tool into their Security Program with the following milestones:
 - a. OUs shall utilize CSAM for FISMA reporting, IT System Inventory, and Plan of Actions & Milestones upon the effective date of this policy.
 - b. OUs shall utilize CSAM for new (developmental) and existing systems in a phased approach where the artifacts must be completely transitioned during the system’s C&A cycle. Further direction concerning the implementation schedule and actions required for the conduct of C&A and continuous monitoring will be provided at the conclusion of the CSAM pilot by the CSAM Working Group.
 - c. Use of CSAM is not mandatory for systems which will be retired over the next C&A cycle.
4. OUs shall integrate the following DOC quality control (QC) tools into their Security Program:
 - a. The Smart Spot Check (SSC) criteria shall be used for all systems at the outset of the C&A process and, as necessary at the commencement of each phase of the C&A process.
 - b. The Authorizing Official (AO) Matrix shall be completed and incorporated into the C&A package for high impact systems, and systems submitted for an Office of the Inspector General (OIG) audit or evaluation, as requested by the DOC SAISO. In lieu of the AO Matrix, the following data points shall be collected and documented in a form presentable to the Authorizing Official for Low and Moderate impact systems prior to the authorization decision:

¹ Artifacts are documented outputs and work products specific to the C&A process.

- i. Final outcome of each control's assessment, per component.
 - ii. Percentage of assets² satisfied, in a component, per control
 - iii. Sampling rate for the assessment of each component, per control.
 - iv. Number of controls and/or enhancements added or removed from the 800-53 baseline, per component.
5. OUs shall minimally create individual CSAM accounts for personnel in each of the following roles: System Owner, Certification Agent, Information System Security Officer (ISSO), and Information Technology Security Officer (ITSO). Each must be granted access commensurate with their responsibility, as defined by the OU.
6. For artifacts that exist outside of the CSAM system boundary, OUs shall implement security controls to protect C&A artifacts commensurate with moderate for confidentiality, excluding any artifact or portions of artifacts that are publicly available or suitable for public dissemination.



Suzanne Nilding
Chief Information Officer



Approval Date

² Components are major and individually assessable classes of software, hardware, or firmware that are critical to a system's operation and security posture. For example, components can include web servers, application servers, databases, operating systems, routers, and firewalls. Components consist of component assets which make up the physical and/or virtual instantiations of the components. Decomposing a system into its components must occur through a risk management process that balances operational and security requirements and considers resource constraints.

7. Minimum DOC Certification and Accreditation (C&A) Artifacts

DOC will utilize standardized C&A templates in conjunction with the Cyber Security Assessment & Management tool for the DOC C&A process. Table 1 lists which templates will be standardized and maintained by DOC and which templates OUs can build and maintain. Artifacts associated with the Contingency column should be expected in the DOC C&A package only when required.

Table 1 – Minimum DOC Certification and Accreditation Artifacts

	Artifact Name	Core (DoC Format)	Information Requirement (OU Format)	Contingent Format	
				DOC	OU
Initiation	C&A Work Plan		X		
	System Security Plan ³	X			
	Risk Assessment ³		X		
	Rules of Behavior				X
	Component Inventory		X		
	MOU/MOA/ISA/SLAs				X
	Contingency Plan	X			
	Incident Response Plan				X
	Continuous Monitoring Plan ³		X		
	E-Authentication Threshold Analysis	X			
	E-Authentication Risk Assessment			X	
	Privacy Threshold Analysis	X			
	Privacy Impact Assessment			X	
Certification	Security Assessment Plan ³	X			
	Vulnerability Scan Analysis Report		X		
	Contingency Plan Test Results		X		

³ Artifact is at least partially or completely generated by CSAM.

	Penetration Test Summary Results (High Impact System Only)				X
Accreditation	Plan of Actions and Milestones (POA&M) ³	X			
	Security Assessment Report (SAR) ³	X			
	Security Accreditation Letter	X			