



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

MAR 23 2011



OCIO Directive 2011-006

To: Heads of Bureaus and Offices

From: Bernard J. Mazer
Chief Information Officer

Subject: Information System Boundary Assessment & Authorization Package
Documentation and Inventory

This directive supersedes the Office of the Chief Information Officer (OCIO) memorandum entitled, *Mandatory Use of the Cyber Security Assessment Management (CSAM) Solution*, issued on September 23, 2008, and OCIO Directive 2009-002, *Population and Maintenance of the Departmental Enterprise Architecture Repository (DEAR)*, issued on February 6, 2009.

This directive applies to all information systems used or operated by the Department of the Interior (DOI), by a contractor of DOI, or by another organization on behalf of DOI. An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The set of information resources allocated to an information system defines the *information system boundary* for that system. With regard to the risk management process and information security, the term *information system boundary* is synonymous with *authorization boundary*.

It is also possible for multiple information systems to be considered as independent *subsystems* of a more complex information system. A subsystem is a major subdivision of an information system consisting of information, information technology, and personnel that perform one or more specific functions. This situation may arise when smaller information systems are coalesced for purposes of risk management into a larger, more comprehensive system. On a larger scale, an organization may develop a system of systems involving multiple independent information systems (possibly distributed across a widespread geographic area) supporting a set of common missions and/or business functions. While subsystems within complex information systems may exist as complete systems, the subsystems are, in most cases, not treated as independent entities because they are typically interdependent and interconnected. Collectively, when these discrete sets of information resources are coalesced as subsystems into a larger more complex information system, those subsystems become part of the information system boundary.

Effective December 31, 2010, the Departmental Enterprise Architecture Repository (DEAR) is formally decommissioned and the Cyber Security Assessment and Management (CSAM) system is designated as the official information system inventory repository and shall be used by Interior's bureaus/offices for:

- (1) development and maintenance of all information system boundary assessment and authorization (formerly referred to as Certification and Accreditation (C&A)) package documentation and all associated artifacts, to include the following:
 - a. System Security Plan (SSPs);
 - b. Security Configurations (may be included in the SSP as a supporting appendix or incorporated by reference to appropriate source(s));
 - c. Continuous Monitoring Strategy (may be included in the SSP as a supporting appendix or incorporated by reference to appropriate source(s));
 - d. Interconnection Security Agreements (ISA);
 - e. Memorandum of Understanding/Agreements (MOU/A);
 - f. Contingency Plan (CP), including documented results of annual tests of the plan;
 - g. Incident Response (IR) Plan (may be included in the SSP as a supporting appendix or incorporated by reference to appropriate source(s));
 - h. Configuration Management Plan (may be included in the SSP as a supporting appendix or incorporated by reference to appropriate source(s));
 - i. Risk Assessment (RA) Report;
 - j. Security Assessment Plan (SAP - formerly referred to as Security Test and Evaluation (ST&E) Plan);
 - k. Security Assessment Report (SAR - formerly referred to as Security Test and Evaluation (ST&E) Report);
 - l. Plan of Action and Milestones (POA&M);
 - m. Privacy Threshold Analysis;
 - n. Privacy Impact Assessment (PIA); and
 - o. Authorization Decision Document
- (2) entry and tracking of all weaknesses and associated corrective action plans for IT Security programs and information system boundaries as part of bureau/office POA&M processes consistent with the requirements identified in Interior's POA&M Processing Standard;
- (3) quarterly and annual FISMA performance metrics reporting; and
- (4) annual IT Security Assessments (e.g., security control testing for Internal Control Review (ICR) processes).

The information currently managed in DEAR that is not transferred to CSAM will continue to be provided by bureaus through notifications to EAD. As systems are defined or retired in CSAM, the system owners will be contacted to provide core enterprise architecture information. The information collected in DEAR will continue to provide insight at the Department level about the specific nature of systems that will not be available in any other tool. Rather than subjecting bureaus to regular data calls asking for EA information, the non-production EA repository will allow the OCIO to manage information as it emerges. It also will help facilitate the transition to a future EA Repository.

All information systems and their subsystems, including minor applications, must be covered by a system security plan. They should be included in the security plan, labeled as either a Major Application (MA) or General Support System (GSS), of an appropriate information system boundary within which they have been identified as being members of. A minor application is defined as an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. Specific system security plans for minor applications are not required because the security controls for those applications are typically provided by the MA or GSS in which they operate. In those cases where a minor application is not connected to an MA or GSS, the minor application should be briefly described in a GSS security plan that has either a common physical location or is supported by the same organization. To help ensure that the information system inventory data fields within CSAM and the information contained in the SSPs remain consistent with each other, and to avoid any such discrepancies as previously noted by the Office of Inspector General (OIG) in their annual FISMA reports in previous years, bureaus and offices shall:

- fully populate information system boundaries within CSAM with all associated information systems and subsystems (including minor applications);
- identify all subsystems, including minor applications, within the system inventory by designating them as a child of the parent information system boundary within CSAM; and
- utilize the automated SSP generation capability within CSAM to create and make updates to the SSP whenever the system inventory for an information system boundary changes, including:
 - incorporation of an architectural diagram depicting the most current information system boundary; and
 - ensuring that the Authorizing Official, or their Designated Representative, review and formally approve the most current SSP.

If you have any questions concerning this memorandum, please contact me at (202) 208-6194. Staff may contact the Department's Chief Information Security Officer, Mr. Lawrence K. Ruffin at (202) 208-5419.

cc: Bureau and Office Chief Information Officers
Bureau and Office Deputy Chief Information Officers
Bureau and Office Chief Information Security Officers
Interior Architecture Working Group