United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

MAR 2 0 2006

TAKE PRIDE IN AMERICA

OCIO Directive 2006-009

To: Heads of Bureaus and Offices

From: W. Hord Tipton
Chief Information Officer

Subject: Information Technology (IT) System Inventory Requirements

Purpose:

This directive requires:

- information systems to be properly mapped to associated security accreditation boundaries within the Department of the Interior (DOI) Enterprise Architecture Repository (DEAR) and the respective bureau EA Repositories (BEARs);
- the population and maintenance of data elements associated with Individual Indian Trust Data (IITD) systems; and
- Certification and Accreditation (C&A) performance metrics, previously maintained within Command Center, to be populated and maintained within DEAR and BEAR for each accreditation boundary.

This directive provides supplemental guidance to OCIO Directive 2004-010 on system inventory requirements.

Policy:

DOI bureau and office Chief Information Officers (CIOs) are responsible for ensuring the accuracy and completeness of their system inventories in the DEAR and the respective BEARs, including the proper mapping of each information system to an associated security accreditation boundary.

This policy also establishes DEAR as the authoritative source for the identification and inventory tracking of information systems that "house" or provide "access" to IITD. Bureau and office CIOs are responsible for ensuring data elements and attributes are populated and updated to enable tracking of IITD systems in DEAR.

Bureaus and offices maintaining stand-alone instances of their BEARs are responsible for providing timely updates for synchronization with DEAR, at a minimum on a quarterly basis or as otherwise requested by the Office of the Chief Information Office (OCIO).

The CIOs are also responsible for ensuring that security accreditation packages include all member systems within the security accreditation boundary of each parent General Support System (GSS) and/or Major Application (MA). Security accreditation packages must include risk impact ratings, security categorizations, and evidence of applicable security controls. In addition, the following requirements must be met, as applicable:

- Member systems mapped to security accreditation boundaries must undergo the appropriate Security Testing and Evaluation (ST&E) and be certified and accredited as a part of the GSS or MA.
- Member systems may have different potential risk impact ratings and security categorizations than the parent GSS or MA with which they are associated. In those cases:
  - Each member system shall have a risk assessment conducted to determine the impact rating and security categorization, which must be included in associated GSS or MA accreditation package.
  - Where member system risk impact ratings and security categorizations have been identified as higher than their parent GSS or MA ratings and categorizations:
    - the GSS or MA will inherit the ratings and categorizations of the highest-rated member system;
    - existing security controls will be reassessed; and
    - if appropriate, a recertification and accreditation may be required.

Scope:

This directive applies to all information systems, including those operated by contractors and application service providers, wholly or partially funded by DOI, that process, store, transmit or house DOI information. Information systems include all General Support Systems (GSSs) and Major Applications (MAs) including any associated minor applications

Time Frame:

This directive is effective immediately for all new information systems. For existing information systems, bureaus and offices should immediately begin implementation, and ensure full compliance by August 31, 2006.

Background:

All operational information systems must be covered under a security accreditation boundary that has been certified and accredited (C&A) in conformance with OCIO Directive 2006-008. Security accreditation boundaries and associated data have been

tracked in the C&A Module of the DOI Command Center system. That data has been imported into DEAR and the BEARs to provide a more seamless mechanism for tracking, mapping and reporting on DOI's information systems inventory, including the association of systems to accreditation boundaries. The C&A module of Command Center will be retired in the near future, at which time DEAR will become the authoritative source for tracking security accreditation boundaries. The system security plan for each system is the authoritative document from which accreditation boundaries shall be tracked within DEAR.

OCIO Directive 2004-010, dated April 27, 2004, established DEAR and its subsystem BEARs as the authoritative source for information on all DOI information systems and enterprise architecture (EA) artifacts. Under that directive, the CIOs are responsible for ensuring the accuracy and completeness of their respective information systems inventories.

Contact:

If you have any questions regarding this directive, please contact me at (202) 208-6194. Staff may contact Ms. Colleen Coggins, Chief Architect, at (202) 208-5911, or Mr. Larry Ruffin, Acting Chief, Cyber Security Division, at (202) 208-5419.

Attachment: Definitions

cc: Bureau Chief Information Officers
Interior Architecture Working Group
Bureau Information Technology Security Managers

Attachment 1

OCIO Directive 2006-009 Definitions

For the purpose of this directive, the following definitions apply, as set forth by the United States District Court:

"Access"— the ability to gain entry into Information Technology Systems.

"House"— The storage by electronic means of Individual Indian Trust Data.

"Individual Indian Trust Data"— Information stored in, or transmitted by or through, any Information Technology System that evidences, embodies, refers to, or relates to—directly or indirectly and generally or specifically—a Federal Record that reflects the existence of Individual Indian Trust Assets, and that at any time either: (1) has been, or is now, used in the Management of Individual Indian Trust Assets; (2) is a title or ownership record; (3) reflects the collection, deposit, and/or disbursement or withdrawal of income or interest—imputed or actual—relating to Individual Indian Trust Assets whether or not such assets are held in a particular account or are identifiable to any particular individual Indian trust beneficiary by name, number, or other specific identifier; (4) reflects a communication with, or on behalf of, an individual Indian trust beneficiary; or (5) has been, or is now: (a) created for, or by, Interior or any bureau, office, agency, agent, or contractor thereof, or for, or by a Tribe in connection with the Management of Individual Indian Trust Assets; (b) provided to, or received by, Interior or any such bureau, office, agency, agent, or contractor thereof, or any Tribe, for use in the Management of Individual Indian Trust Assets, and (c) used or housed by Interior or any such bureau, office, agency, agent, or contractor thereof, or any Tribe, in connection with the government's Management of Individual Indian Trust Assets.

Other applicable definitions include the following.

"Accreditation Boundary"— All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term *security perimeter* defined in Committee on National Security Systems (CNSS) Instruction 4009 and Director of Central Intelligence Directive 6/3. (Source: NIST Special Publication 800-37)

"Accreditation Package"— The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones. (Source: NIST Special Publication 800-37)

"C&A Boundaries" — See *Accreditation Boundary*.

"General Support System"— An interconnected set of information resources under the same direct management control which shares common functionality. A system normally

includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). (Source: OMB Circular A-130, Appendix III)

"*Information*"— Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Source: OMB Circular A-130, Revised, Transmittal Memorandum No. 4, Paragraph 6.j.)

"*Information System*" — A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. (Source: OMB Circular A-130, Revised (OMB Circular A-130, Revised, Transmittal Memorandum No. 4, Paragraph 6.q.)

"*Major Application*"— An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. *Note:* All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Source: OMB Circular A-130, Appendix III)

"*Member System*" — A logically separable system included with others within an Accreditation Boundary for purposes of security certification and accreditation.

"*System Boundaries*" — Refers to the process of uniquely assigning information resources to an information system that defines the security boundary for the system. Agencies have great flexibility in determining what constitutes an information system (i.e., major application or general support system). When a set of information resources is identified as an information system, the resources should generally be under the same direct management control. Direct management control does not necessarily imply that there is no intervening management. It is also possible for an information system to contain multiple member systems.