

### 3. Information Technology Security

The Department's FY 2010 budget for IT is \$995 million. That budget funds the network infrastructure, IT security, and various IT investments, which are intended to align with Departmental mission objectives. IT supports the Department's diverse programs meant to protect and manage our Nation's natural resources and cultural heritage; provides scientific and other information about those resources; and honors its trust responsibilities or special commitments to American Indians, Alaska Natives, and affiliated Island communities. IT security strives to assure the confidentiality, integrity and availability of information assets.

The Department continues to employ a decentralized and fragmented IT governance framework, which does not optimally operate or fully comply with legislation and Federal policy. Despite some improvements and progress, decentralized management, resource gaps, disconnection from the internet related to the *Cobell v. Salazar* case, a lack of centralized asset management capability and other factors have left the Department struggling to meet information security and privacy mandates. A lack of strategic direction in implementation of information technology resulted in inadequate oversight even when appropriate technology exists.

The Federal Information Security Management Act of 2002 requires the Secretary of the Interior to delegate to the Department's Chief Information Officer (CIO) "the authority to ensure compliance with the requirements imposed on the agency under this subchapter." We routinely found that guidance issued by the CIO was not implemented.

- In August 2006, the CIO directed all bureaus and offices to transition to the Department's remote access system by January 31, 2007. In FY 2010, we found that many bureaus still operate their own separate, remote access systems.
- In June 2006, OMB Memorandum 06-16 "recommends allowing remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer." Of the users who utilize the Department's Remote Access Solution, 78 percent did not use the two-factor authentication.
- In December 2009, the CIO directed all bureaus and offices to utilize the Departmental Access System for on-boarding employees and contractors prior to initiating IT user access accounts. We found in FY 2010, not all bureaus were following this guidance.

During 2010, our evaluations revealed:

- Inaccuracies in IT asset inventory
- Duplicative IT functions
- Resistance to consolidated IT operations and management
- A fragmented continuous monitoring program
- Inadequate departmental oversight
- Incomplete assessments of privacy risk

The Department launched an initiative in June 2010 called the DOI Innovation and Efficiency Team (DIET) which currently is in the planning phase. Per the DIET charter, "this initiative was created to identify and implement immediate and long-term solutions to realize cost savings, cost avoidance, cost efficiencies and/or innovations across the DOI IT environment." That initiative includes objectives directly related to its IT Security Program. As the Department moves forward in implementing various facets of the initiative, they have the potential to address a number of IT security challenges.