U.S. Department of the Interior

Office of Inspector General

Compilation of **Information Technology** Challenges at DOI

A Blueprint for Change

Report No. ISD-EV-OSS-0017-2008

May 2008

Contents

Figures

Executive Summary

The Department's management of information technology is ineffective, costly, wasteful, and lacks accountability. The dismal results of the Department's IT program have been long reported by the Government Accountability Office (GAO), the Office of Management and Budget (OMB), and the Department's Office of Inspector General (OIG). The Department's own Chief Information Officer (CIO) acknowledged the Department is failing. Sweeping reform is required to correct deficiencies in the Department's IT program.

In contrast to what is required by law, the Department's CIO does not report to the *"head of the agency,"* has not been delegated the authority to ensure compliance with the Federal Information Security Management Act (FISMA), and is not in a position to ensure the cost effectiveness of the Department's IT program.

The Department's CIO does not control IT investments and, as a result, significant money has been wasted. As far back as 1999, the Government Accountability Office (GAO) reported that the Department *"had not followed sound management practices in the early stages of its effort to acquire the Trust Asset and Accounting Management System, a system designed to manage Indian assets and land records."* In September 2003 another GAO report stated – on the first line – *"The Department of the Interior has limited capability to manage its IT investments."* More than 5 years later, OMB stated, "*Less than 50% of [the Department's] business cases are acceptable.*" Between 3Q06 and 4Q07 the number of the Department's IT projects on the OMB's "High Risk List" climbed 600%.

For five consecutive years – from 2003 through 2007 – the OIG reported in its Annual Summary of Major Management and Performance Challenges, significant and continuing deficiencies in the Department's IT program.

In 2005, the Department was credited with spending an estimated 100 million dollars to improve security. In 2006, the OIG successfully penetrated the Department's network and applications 50% of the time, evidencing the problems with the Department's IT program will not be solved with money alone.

In January 2008, through pure happenstance, a lone security professional with the Department stumbled upon highly suspicious network traffic leaving the Department's network. The traffic patterns were so anomalous the Department retained outside expertise to help investigate. According to the outside expert, the Department "*does not have sufficient visibility into their networking infrastructure to conclusively monitor for potential intrusions or malicious activity*." Given the current environment – as documented by the Department's own outside expert – it is unfathomable anyone could give assurance the Department's network is secure.

Between fiscal years 2001 and 2006, the Department repeatedly received failing grades from the House of Representatives Committee on Oversight and Government Reform on its compliance with FISMA, falling below government-wide averages 5 out of 6 consecutive years.

In 2002, the Department's own outside expert concluded, *"Management reform is needed within the OCIO to establish the structure and environment of the OCIO as the leader of IT management for DOI."* By failing to implement recommendations contained in their own expert's report, the Department failed to realize nearly 400 million dollars in potential savings and cost avoidance in its IT program.

In September 2003, GAO issued a report in which it stated, "*Over the past decade, Congress has enacted a series of laws that require centralized management*" The same GAO report went on to state "*Under the Clinger-Cohen Act, the Department of the Interior's CIO has the ultimate responsibility for ensuring the cost effectiveness of decisions made by program managers to expend funds on IT in support of the agency's mission needs."*

Numerous examples evidence the Department's governance processes are so complex establishing accountability is all but impossible. Numerous examples evidence the Department's current strategy of a decentralized, collaborative, federated model for IT management has not produced satisfactory results.

In 2008, the Department's own CIO warned, *"We are behind and falling further behind. Unless we act now and change how we approach these problems, we will fail."*

For fiscal year 2009, the President has requested 965 million dollars in IT budget for the Department up from 918 million dollars in fiscal year 2008. The OIG recommends a systematic and phased approach to realign the IT program under the Department's CIO thus establishing a clear line of authority and accountability before even more dollars are wasted.

Compliance with Federal Law

Federal Information Policy requires the head of each agency to designate a CIO who shall *"report directly to such agency head to carry out the responsibilities of the agency under this subchapter."* However, the Department's policy establishes a Department CIO who reports to an Assistant Secretary.[1]

The GAO released report number GAO-04-823, entitled FEDERAL CHIEF INFORMATION OFFICERS: Responsibilities, Reporting Relationships, Tenure, and Challenges, in July 2004. According to this report, CIOs at 19 of 27 agencies reviewed reported *"directly to their agency heads."*[2]

At the conclusion of its report, GAO stated, *"As it holds hearings on and introduces legislation related to information and technology management, we suggest that the Congress consider the results of this review and whether the existing statutory requirements related to CIO responsibilities and reporting to the agency heads reflect the most effective assignment of information and technology management responsibilities and reporting relationships."*[3]

- On July 6, 2004, P. Lynn Scarlett, Assistant Secretary, Policy, Management and Budget, Department of the Interior (DOI) authored a memorandum to David M. Powner, Director, Information Technology Management Issues, GAO, in response to report GAO-04-823. In her memorandum, Ms. Scarlett stated, *"In one particular area, the Department of the Interior (DOI) recommends the requirements remain constant: the Chief Information Officer reports directly to the Secretary. This level of attention to IT is critical to being able to accomplish all the other requirements. The Secretary's personal involvement in IT at DOI, along with the personal involvement of her management team, are key factors in the evolutionary improvements we have made."*[4]

In the same report, GAO stated, *"We identified the following 13 major areas of CIO responsibilities as either statutory requirements or critical to effective information and technology management."*[5]

1. IT/IRM (Information Resource Management) strategic planning. CIOs are responsible for strategic planning for all information and IT management functions— thus, the term IRM strategic planning [44 U.S.C. 3506(b)(2)].

2. IT capital planning and investment management. CIOs are responsible for IT capital planning and investment management [44 U.S.C. 3506(h) and 40 U.S.C. 11312 & 11313].

3. Information security. CIOs are responsible for ensuring compliance with the requirement to protect information and systems [44 U.S.C. 3506(g) and 3544(a)(3)].

4. IT/IRM workforce planning. CIOs have responsibilities for helping the agency meet its IT/IRM workforce or human capital needs [44 U.S.C. 3506(b) and 40 U.S.C. 11315(c)].

5. Information collection/paperwork reduction. CIOs are responsible for the review of agency information collection proposals to maximize the utility and minimize public "paperwork" burdens [44 U.S.C. 3506(c)].

6. Information dissemination. CIOs are responsible for ensuring that the agency's information dissemination activities meet policy goals such as timely and equitable public access to information [44 U.S.C. 3506(d)].

7. Records management. CIOs are responsible for ensuring that the agency implements and enforces records management policies and procedures under the Federal Records Act [44 U.S.C. 3506(f)].

8. Privacy. CIOs are responsible for compliance with the Privacy Act and related laws [44 U.S.C. 3506(g)].

9. Statistical policy and coordination. CIOs are responsible for the agency's statistical policy and coordination functions, including ensuring the relevance, accuracy, and timeliness of information collected or created for statistical purposes [44 U.S.C. 3506(e)].

10. Information disclosure. CIOs are responsible for information access under the Freedom of Information Act [44 U.S.C. 3506(g)].

11. Enterprise architecture. Federal laws and guidance direct agencies to develop and maintain enterprise architectures as blueprints to define the agency mission, and the information and IT needed to perform that mission.

12. Systems acquisition, development, and integration. We have found that a critical element of successful IT management is effective control of systems acquisition, development and integration [44 U.S.C. 3506(h)(5) and 40 U.S.C. 11312].

13. E-government initiatives. Various laws and guidance direct agencies to undertake initiatives to use IT to improve government services to the public and internal operations [44 U.S.C. 3506(h)(3) and the EGovernment [*sic*] Act of 2002]."

The E-Government Act of 2002 was signed by the President on December 17, 2002, with an effective date for most provisions of April 17, 2003. Title III of the E-Government Act is entitled Federal Information Security Management Act (FISMA). FISMA required the Department CIO be delegated the

authority to *"ensure compliance."*[6] Rather 4 months prior to FISMA on August 7 2002, Gale Norton, Secretary of the Interior, issued a memorandum establishing an Information Technology Management Council (ITMC).[7] In addition, on November 12, 2002, Secretary Norton signed order number 3244 entitled Standardization of Information Technology Functions and Establishment of Funding Authorities.

Through her memorandum, Secretary Norton established the ITMC as the governing body for information technology. In contrast to what is required by federal law, authority to ensure compliance with FISMA has been delegated to a committee of Bureau and Office CIOs.

- The ITMC Charter, dated January 2005, states, *"The purpose of this Charter is to establish the Council as the collaborative governance of Information Technology (IT) and Information Resources Management (IRM) within the Department."*
- The ITMC Charter goes on to state *"The Council will report to the Secretary of the Interior"*
- The ITMC Charter further states, *"The Office of the Chief Information Officer (OCIO) will provide executive assistance and staff support for the ITMC."*

Through her order, Secretary Norton established a *"stand-alone CIO"* for each organization within the Department with 5,000 or more employees who reported to Bureau directors and deputy directors. In contrast to what is required under federal law, the authority necessary to ensure compliance with FISMA has been delegated to individual Bureau and Office CIOs.[8]

The Department's own CIO has warned "*Organizational culture, resistance to change, us vs. them mentality - We don't want the Department to know what we are doing.*" This is in contrast to what is required by law and an impediment to achieving success in the Department's IT program.[9]

Less than Fully-Effective Results

Since establishment of the ITMC and Bureau-specific CIOs, the Department has failed to establish an effective and efficient agency-wide information technology program.

For five consecutive years – beginning the first year after the ITMC and Bureau-specific CIOs were established – the OIG reported in the Annual Summary of Major Management and Performance Challenges, significant and continuing deficiencies in the Department's information security program.[10]

These deficiencies continue in 2008. In January 2008, a lone security professional with the Department exploring the capabilities of a security tool provided to the Department free-of-charge by the Department of Homeland Security discovered highly suspicious patterns for network traffic leaving the Department. The traffic patterns were so anomalous the Department retained outside expertise to help investigate. According to the outside expert, "*Based on a short term packet capture of packets at the*

Reston gateway where content matched a regular expression targeted at finding Social Security Numbers, it appears that there were several instances of a period of approximately two hours where SSN information was transmitted in cleartext [sic] over DOI networks. While, perhaps, there is a business case for the transmission of this data, it should never be transmitted in the clear over a potentially hostile network environment." The Department's own outside expert went on to state the Department "… does not have sufficient visibility into their networking infrastructure to conclusively monitor for potential intrusions or malicious activity."[11]

In a presentation to agency leadership in 2008, the Department CIO acknowledged, *"OMB mandates to improve IT security and privacy have not been completed in Interior"* and "*2 years behind on mandated security and privacy protections*".[12]

According to the Department's own analysis, nearly *70*% of the network traffic leaving the Department through a single one of its Internet gateways during the month of January 2008 was bound for known-hostile countries[13] and the Department lacked the capability to even determine what the traffic was. If it had not been for a lone security professional stumbling across anomalous traffic patterns through happenstance, the Department would not even have known nearly *35*% of all network traffic leaving the Department's network was bound for non-U.S. recipients – some of whom are known to be hostile to the U.S.

Evidence of the inefficiencies and ineffectiveness of the Department's IT program are abundant and consistent. As an example, problems with systems necessary for financial management have not been addressed in a timely or efficient manner. [14] Significant investments in IT are not being managed under the purview of the Department's CIO and as a direct result, many are drastically behind schedule and have a record of subpar performance.

The GAO released report number GAO-03-1028, entitled Departmental Leadership Crucial to Success of Investment Reforms at Interior, in September 2003. The report begins with *"The Department of the Interior has limited capability to manage its IT investments."* More than 5 years later, OMB stated about the Department *"Less than 50% of business cases are acceptable."*[15] OMB went on to state *"Project overruns and shortfalls average less than 30%."* The decentralized, federated, collaborative approach to managing IT investments has not produced satisfactory results.

GAO report GAO-03-1028 went on to state *"In April and July of 1999, we reported that Interior had not followed sound management practices in the early stages of its effort to acquire the Trust Asset and Accounting Management System, a system designed to manage Indian assets and land records."* Nearly 10 years later, the Cobell litigation is still ongoing and potentially stands to cost the U.S. tax payers millions of dollars.

In August 2005, OMB established its "High Risk List" to ensure agencies and programs were meeting their intended goals and producing results. Projects on the High Risk List are those requiring special attention from the highest level of agency management.

- OMB's High Risk List for third quarter 2006 contained 3 of the Department's projects, including:
    1. Financial Business Management System (FBMS)
    2. DOI Geospatial One-Stop (GOS)
    3. DOI Recreation One-Stop (ROS)
- OMB's High Risk List for fourth quarter 2007 contained 18 of the Department's projects, including:
    1. FM LoB Center of Excellence
    2. Financial Business Management System
    3. Recreation One-Stop
    4. DOI – IMARS
    5. Geospatial One-Stop
    6. IDEAS
    7. NBC - HR LoB Shared Service Center
    8. Geospatial Line of Business
    9. E-Rulemaking Migration
    10. FAS – Migration
    11. E-Travel Migration
    12. E-Authentication Migration – SSCR
    13. EHRI – Migration
    14. E-Authentication Infrastructure Utility
    15. BLM – ePlanning
    16. MMS - OCS Connect
    17. FWS - Federal Aid Information Management System (FAIMS)
    18. BIA – TAAMS

On April 12, 2007, the House of Representatives Committee on Oversight and Government Reform issued its Seventh Report Card on Computer Security at Federal Departments and Agencies. The report

card detailed the Department's performance between 2003 and 2006 as well as reported on the government-wide averages. Three out of four consecutive years, the Department was below average with failing grades.

- For FY2003: F (Government-Wide Average: D)
- For FY2004: D+ (Government-Wide Average: D+)
- For FY2005: F (Government-Wide Average: D+)
- For FY2006: F (Government-Wide Average: C-)

On March 16, 2006, the House of Representatives Committee on Oversight and Government Reform issued its Sixth Report Card on Computer Security at Federal Departments and Agencies. The report card contained details on the Department's performance for 2001 and 2002 (not included in seventh report card) as well as reported on the government-wide averages.

- For FY2001: F (Government-Wide Average: F)
- For FY2002: F (Government-Wide Average: F)

The Congressional report cards document the Department has failed 5 out of 6 years to meet minimum acceptable standards for computer security and evidence the Department's mismanagement of the information technology program has had a substantial and prolonged negative impact on security.

The Department's CIO recently acknowledged, *"Interior is one of only five agencies still failing to comply with FISMA"* and went on to state "5+ years – spent >$285 million and still getting failing grades on Congressional FISMA scorecard"[16]

Costly and Wasteful Approach

The Department's management of IT is rife with missed opportunities to improve and full of waste.

Between December 2001 and June 2002, the Department retained Science Applications International Corporation (SAIC) to perform an Information Technology Management Reform (ITMR) study.[17] There were 203 interviews conducted involving 836 interviewees during the 6-month study.[18] The study concluded, *"Management reform is needed within the OCIO to establish the structure and environment of the OCIO as the leader of IT management for DOI."* The report stated, "*Consolidation benefits sited [sic] were lower cost of centralized IT functions and potential economies of scale. Other sited [sic] benefits of consolidation were improved performance levels, improved security, better standardization and less redundancy."*

The SAIC ITMR study identified several specific problems such as: *"Decentralized organization resists enterprise change," "lack of enterprise-level visibility into IT resources,"* and *"lack of strong career program."*[19] The study went on to state, *"Decentralized organization/culture drives longer time lines and more cost to achieve enterprise-wide reforms."*

The SAIC ITMR study identified several significant opportunities that the Department has failed to realize. The study found that consolidation of data centers would avoid 35.6 million dollars in cost. In addition, consolidation of help desks would save 35 million dollars in labor alone. Moreover, productivity improvements in desktop support would save 130.6 million dollars and productivity improvements in application development and maintenance would save another 71.8 million dollars. Cost savings and avoidance related to data and voice networks totaled 115.9 million dollars. In conclusion, the SAIC ITMR study found that *"OCIO Management Reform"* was the best option for the Department and would result in more than 388 million dollars in total benefit.[20]

In a presentation provided to agency leadership in 2008, the Department's CIO conceded, *"5+ years – Failed to realize $388 million in potential infrastructure efficiencies"*

In the OIG's FY2005 Summary of Major Management and Performance Challenges, the Department was credited with establishing *"a body of policy and guidance"* as well as investing in various security technologies *"at an estimated cost of $100 million"* needed to *"create a control environment which allows testing of the networks, systems, and programs comprising the Department's IT assets."* However, during FY2006, the OIG staff was able to successfully penetrate the Department's network and applications 50% of the time. A year later, in the FY2007 Summary of Major Management and Performance Challenges, the OIG reported *"the evaluations revealed ineffective internal intrusion detection and prevention capabilities."* The summary went on to say, *"We determined that the Department has not fully implemented continuous monitoring and system testing, which is an essential part of the federal Certification and Accreditation guidance."*

In December 2007, Gartner,[21] an outside consultant, concluded a study at the Department in support of OMB's IT Infrastructure Line of Business. Gartner's presentation concluded there were opportunities for improvement at the Department. Specifically, Gartner concluded, "*DOI's staffing level for Client & Peripherals is 68% higher than the bottom of the Industry range."*[22] Gartner went on to state, *"DOI supports fewer users and clients per FTE than the top of the Very Large Industry range"* and that "*the Department employed significantly more full-time employees in support of IT than other comparably-sized organizations*."[23]

Lack of Accountability

The governance model utilized by the Department is complex and, as a result, lacks accountability. To improve its information technology management and overcome the barriers that have resulted in failures time after time, the Department must completely overhaul its IT governance model and

establish the Department's CIO as the top management official responsible – and more importantly, accountable – for the IT program.

FISMA requires each agency's CIO to train and oversee *"personnel with significant responsibilities for information security."*[24] In February 2008 – nearly 6 years after FISMA was signed into law – the OIG requested the Department's Chief Information Security Officer (CISO), the Department's top IT security official and a senior member of the CIO's staff, to provide a list of *"personnel with significant responsibilities for information security"* along with basic identifying information. After more than 30 days, the OCIO was unable to provide a comprehensive list, providing data on only an estimated 65 – 70% of relevant personnel. There were no data provided for 4 of the Bureaus at all. Clearly, the CIO cannot *"oversee"* what cannot even be identified.

Based on the partial data provided by the OCIO, personnel with the following job titles were found to have "*significant responsibilities for information security"*:

"Realty Specialist" (BLM)	"Power Manager" (BOR)	"Research Hydrologist" (USGS)	"Hydraulic Engineer" (BOR)
"Road and Right of Way Specialist" (BLM)	"Purchasing Agent" (BOR)	"Supervisory Geophysicist" (USGS)	"Economist" (MMS)
"Petroleum Engineer" (BLM)	"C&I Mechanic" (BOR)	"Supervisory Hydrologist" (USGS)	"Supervisory Civil Engineer" (BOR)
"Natural Resource Specialist" (BLM)	"Natural Resource Specialist" (BOR)	"General Engineer" (BOR)	"Visual Information Specialist" (BOR)
"Maintenance Worker" (BLM)	"Procurement Technician" (BOR)	"Environmental Engineer" (BOR)	"Procurement Analyst" (BOR)
"Land Surveyor" (BLM)	"Civil Rights Specialist" (BOR)	"Manager Civil Rights Office" (BOR)	"Hydrology Group Leader" (BOR)
"Interdisciplinary Geographer" (BLM)	"Budget and Finance Analyst" (BOR)	"Human Resources Manager" (BOR)	"Hydrologist" (USGS)
"Geographer" (BLM)	"Public Affairs Specialist" (BOR)	"Management Analyst" (BOR)	"Archeologist" (BLM)
"Geologist" (USGS)	"Physical Scientist" (BOR)	"Fishery Biologist" (USGS)	"Financial Specialist" (USGS)
"Geophysicist" (USGS)	"Cartographer" (USGS)	"Research Geologist" (USGS)	"Ecologist" (BLM)
"Forester" (BLM)	"Financial Analyst" (MMS)	"Research Geophysicist" (USGS)	"Human Resources Assistant" (NBC)
"Executive Assistant" (MMS)	"Client Executive" (MMS)	"Accountant" (MMS)	"Civil Engineer" (BOR)

Figure 1 Personnel with Significant Security Responsibilities

Either "*significant responsibilities for information security"* has been poorly defined, or the Department has placed its security in the hands of personnel who are likely ill-prepared to carry out the job.

The current governance model has created a "'turf war" between the OCIO and Bureaus and has left the Department unable to manage its IT program efficiently and effectively.

- On March 19, 2008, the CISO at Minerals Management Service (MMS) wrote an email to the Department's Cyber Security Division email distribution list objecting to the fact he was being asked to provide information about *"personnel with significant responsibilities for information security."* When the Director of the OIG's Information Security Division answered his email, he replied stating, *"How we train is a bureau-level issue."* When the Department's Deputy CISO intervened and explained the need for MMS CISO's cooperation, he replied *"I will not blindly follow memos or requests that I do not understand or agree with without further clarification. Blind faith is not one of my strong suits."*

- On March 20, 2008, the CIO at the Bureau of Land Management (BLM), sent an email to BLM personnel announcing the CISO of BLM had been reassigned to *"a special Project Assignment"* and another person had been appointed as *"Acting Bureau IT Security Manager."* The Department's CISO was not consulted on this change of *"personnel with significant responsibilities for information security"* and did not even know of the change before the announcement was publicly made. Clearly, the Department CIO is not permitted to *"oversee personnel with significant responsibilities for information security"* as required by law.

The first two sentences in the Department's 46-page document entitled *"E-Government Strategy Governance Framework FY2004 – FY2008"* dated December 2003, state, *"With Interior facing the challenge of using technology to provide citizen-centered, integrated, secure services, the need for effective governance – accountable decision-making and the structures and processes that turn decisions into actions – has never been greater. Governance issues are complex and easy to get wrong, but E-Government success depends on getting them right."* The Department's E-Government Strategy Governance Framework contained a diagram in paragraph 3.0:

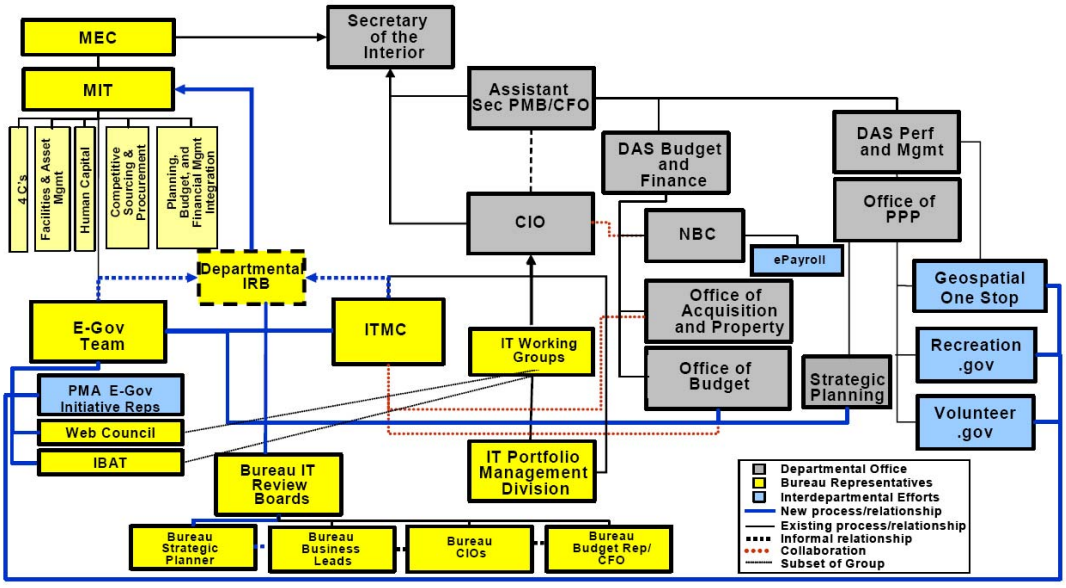

Figure 2 DOI E-Government Governance Model

In June 2005, the Enterprise Architecture Division made a presentation entitled *"DOI IT Governance,"* which listed the committees and teams involved in the governance of information technology at the Department. That list included:

- Interior Business Architecture Team (IBAT)
- Management Excellence Committee (MEC)
- Management Initiatives Team (MIT)
- Information Technology Management Council (ITMC)
- Data Advisory Committee (DAC)
- Investment Review Board (IRB)
- E-Government Team
- Interior Architecture Working Group
- Chief technology Officer Council (CTOC)
- Domain Advisory Teams
- Core modernization Blueprint Team
- Core Modernization Implementation Team
- Architecture Review Board
- DEAR IPT

The Enterprise Architecture Division concluded the current governance structure: "*Has too many standing technology teams," "has too much overlap;"* and *"has redundancy."*

The Department's own CIO acknowledged the complicated governance process has not delivered fundamental results: *"5+ years – Enterprise Service Network still not done"* and *"5+ years – still no common DOI email solution."*

A project plan submitted to the ITMC in March 2008 contained the following diagram to help readers understand the complicated governance process for the project: [25]

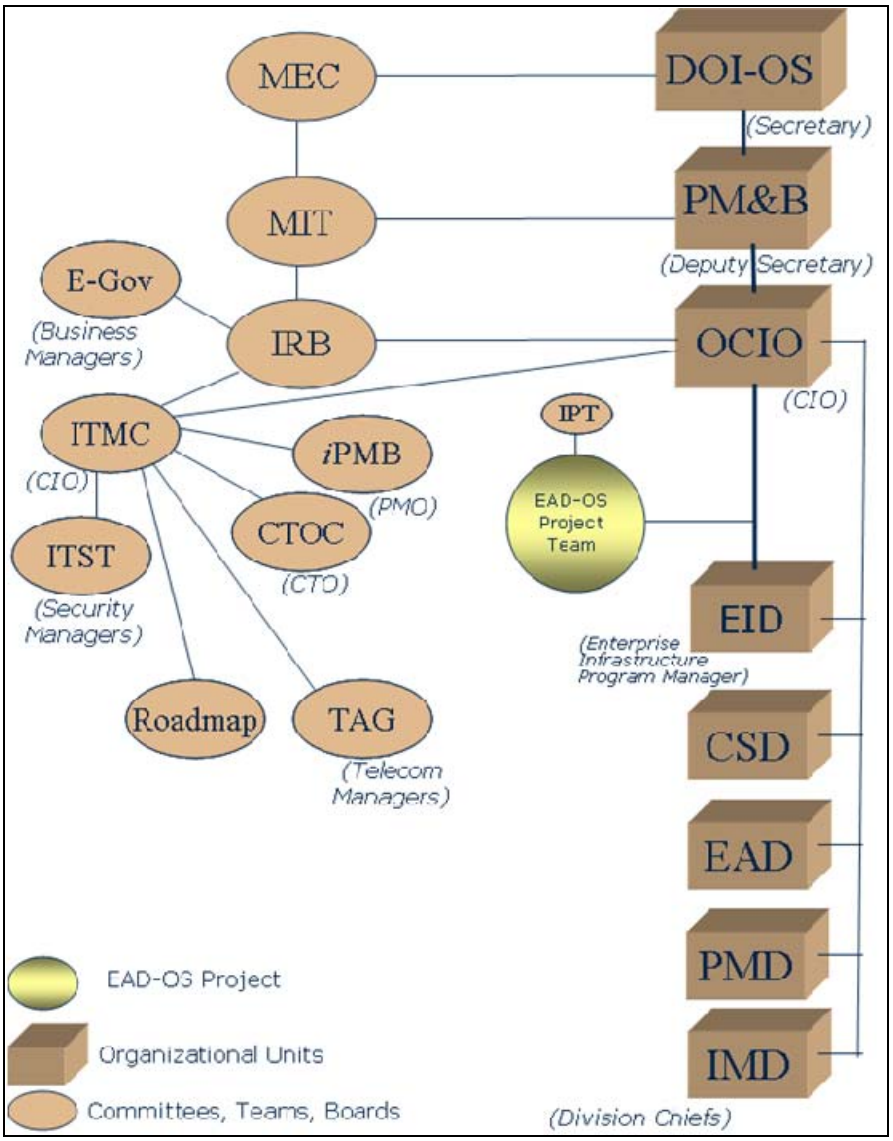

Figure 3 DOI Information Technology Governance Process

With so many teams and committees empowered to make decisions, when decisions get made-- if ever- it is not possible to establish who is accountable for them.

The Department's CIO cautioned agency leadership, *"The old way of doing things is too slow and ineffective."*

Reorganizing and Realigning

In October 2005, the Department of Veterans Affairs (VA) announced it would realign its information technology functions under the Department CIO, in part, to improve accountability. In its FY2005 Report

to Congress on Implementation of FISMA, OMB documented the following facts that can be used to compare the Department to the VA at the time the VA decided to realign:

- Agency Inspectors General were asked several questions to evaluate whether the agency maintains an effective plan of action and milestones process to remediate IT security weaknesses.
    - Interior: No
    - VA: Yes
- Agency Inspectors General were asked to evaluate the quality of agency certification and accreditation processes.
    - Interior: Poor
    - VA: Satisfactory
- Agency Inspectors General were asked to evaluate the extent to which an agency system inventory has been developed.
    - Interior: 81-95%
    - VA: 81-95%

In two of three measured categories, the Department fared worse than the VA and mirrored the VA in the third, at a time when the VA determined it needed to reorganize and centralize to improve its own accountability.

In FY2007, the Department's result in an essential element of information technology security management was the same as FY2003: Effective Plan of Action and Milestones (POA&M) process – NO.

In four of five consecutive years of "*collaborative governance of Information Technology,"* the Department has failed to meet a minimally acceptable standard in a key measurable item reported to Congress through the OMB.

In testimony before the House Committee on Resources on February 14, 2007, the Department's Inspector General (IG) testified, *"A significant impediment to improving cyber security and gaining full compliance with FISMA is DOI's decentralized IT management structure. My office supports the concept of reorganizing and centralizing key IT security functions."* The IG's testimony went on to state *" a stronger centralized CIO function with adequate resources for technical efforts such as computerized asset management and continuous monitoring would materially improve cyber security at DOI."*

Conclusion

OMB, GAO, the Department's Inspector General, and the Department's own Chief Information Officer all have documented the Department's failure to effectively and efficiently manage its IT program. The Department has persistently failed to meet minimum standards in information security. The Department has failed to realize hundreds of millions of dollars in cost savings, cost avoidance, and productivity improvements. Many of the Department's most critical projects are entered on the OMB High Risk List. Even still, neither information security nor enterprise projects are centrally-managed under the purview of the Department CIO. Federal law mandated that the Department CIO be empowered to ensure compliance with FISMA yet, the authority to manage has been delegated to Bureau and Office CIOs and the authority to govern has been delegated to non-accountable committees. While the Department has produced sporadic and unstained improvements in various elements of its IT program over the years, early results of FY2008 evaluations – yet again– indicate no material improvements. It is time for sweeping and fundamental change to the way the Department manages information technology.

A Blueprint for Change

Recommendations

1. Realign Bureau-specific IT personnel under the purview of the Department CIO.
2. Realign all IT funding under the purview of the Department CIO.
3. Organize the IT program along technology and security boundaries rather than along organization boundaries. For example, create a Deputy CIO for infrastructure rather than a Deputy CIO for Bureau A.
4. Manage all IT projects under the purview of the Department CIO.

Recommended Milestones

FY08

1. Maintain the Department CIO's current level of input (25%) in Bureau and Office CIO's annual performance report through the end of FY08.
2. Maintain the Department CISO's current level of input (0%) in Bureau and Office CISO's annual performance report through the end of FY08.
3. Make no change to the current budget authority for IT budgets.
4. By the end of FY08, rescind Secretarial Order 3244.
5. By the end of FY08, issue a new Secretarial Order establishing the Department CIO at the Assistant Secretary level and reporting directly to the Secretary of the Interior. The order should clearly establish the Department CIO's management and budgetary authority for all information technology management.
6. By the end of FY08, update the Department Manual to synchronize with the new Secretarial Order
7. By the end of FY08, rescind Secretarial Memorandum establishing the Information Technology Management Council (ITMC) and issue a new Secretarial Memorandum establishing a Transition Team under the direct authority and control of the Department CIO. The Transition Team Charter should expire by the end of FY11.

8. By the end of FY08, rewrite charters of all committees and teams removing their decision-making authority for information technology and, if necessary, reestablish the teams and committees as advisors to the Department CIO.

9. By the end of FY08, realign authority to grant "Authority to Operate" for all systems under the purview of the Department CIO.

10. By the end of FY08, realign "hiring / firing" authority for all Bureau and Office CIO's, Deputy CIO's, CISO's, and Deputy CISO's under the purview of the Department CIO.

FY09

1. By the end of the first quarter of FY09, realign all Bureau and Office CIO's under the Department CIO as "Deputy Department CIO's" and establish the Department CIO as their reporting official. Allocate 50% of the performance rating of Deputy Department CIO's to the Heads of Bureaus and Offices for which they are assigned.

2. By the end of the first quarter of FY09, realign all Bureau and Office CISO's under the Department CISO as "Deputy Department CISO's" and establish the Department CISO as their reporting official. Allocate 50% of the performance rating of Bureau and Office CISO's to the Heads of Bureaus and Offices for which they are assigned.

3. By the end of FY09, realign all Bureau-specific IT funding under the purview of the Department CIO.

4. By the end of FY09, establish a centralized Incident Response Team under the purview of the Department CIO and realign all incident response personnel, tools, hardware, software, and funding to the Department CIO.

5. By the end of FY09, realign management of network infrastructure under the purview of the Department CIO. "Network infrastructure" is defined as all circuits, firewalls, routers, switches, and other devices providing connectivity and / or security between the end user, applications, or systems and the Internet along with the personnel responsible for managing these devices. In short, "end-to-end" but, excluding actual end-user devices and applications.

6. By the end of FY09, establish a Program Management Office under the purview of the Department CIO and realign management and budget authority over all projects on the OMB High Risk List to the Program Management Office along with personnel responsible for managing these projects in their current alignment.

FY10

1. By the end of the first quarter of FY10, reduce allocation to 25% of the performance rating of Department Deputy CIO's to the Heads of Bureaus and Offices for which they are assigned.

2. By the end of the first quarter of FY10, reduce allocation to 25% of the performance rating of Department Deputy CISO's to the Heads of Bureaus and Offices for which they are assigned.

3. By the end of FY10, realign all program-specific IT funding under the purview of the Department CIO along with personnel responsible for managing this funding in its current alignment.

4. By the end of FY10, realign management of all end user devices (e.g. laptops, Blackberry's, desktops, etc.) under the purview of the Department CIO along with personnel responsible for managing these devices in their current alignment.

5. By the end of FY10, realign management and budget authority over all IT projects under the purview of the Department CIO along with personnel responsible for managing these projects in their current alignment.

6. By the end of FY10, realign management and budget authority over all data centers and hosting centers under the purview of the Department CIO along with personnel responsible for managing these centers in their current alignment.

7. By the end of FY10, realign management and budget authority over all help desks under the purview of the Department CIO along with personnel responsible for managing these help desks in their current alignment.

FY11

1. By the end of the first quarter of FY11, reduce allocation to 0% of the performance rating of Department Deputy CIO's to the Heads of Bureaus and Offices for which they are assigned.

2. By the end of the first quarter of FY11, reduce allocation to 0% of the performance rating of Department Deputy CISO's to the Heads of Bureaus and Offices for which they are assigned.

3. By the end of FY11, realign all IT funding under the purview of the Department CIO along with personnel responsible for managing this funding in its current alignment.

4. By the end of FY11, realign management of all applications and systems under the purview of the Department CIO along with personnel responsible for managing these applications and systems in their current alignment.

5. By the end of FY11, realign management of any remaining IT personnel under the purview of the Department CIO.

Notes and References

[1]Appointment of Chief Information Officer

- United States Code (U.S.C.) Title 44, Subchapter 1 "Federal Information Policy," Section 3502, Paragraph 1 states "the term "agency" means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency…"

- U.S.C. Title 5, Section 101 "Executive Departments" lists "The Department of the Interior."

- U.S.C. Title 44, Subchapter 1 "Federal Information Policy," Section 3506 "Federal Agency Responsibilities," Paragraph a(2)A states "Except as provided under subparagraph (B), the head of each agency shall designate a Chief Information Officer who shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter."

- The E-Government Act of 2002 was signed by the President on December 17, 2002, with an effective date for most provisions of April 17, 2003. Title III of the E-Government Act is entitled "Federal Information Security Management Act" (FISMA). FISMA, Section 3544 "Federal Agency Responsibilities," states, in pertinent part:
- Paragraph (a) "In General.–The head of each agency shall–"

- Paragraph (a)3 "delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section)..."

- Department Manual, Part 110, Chapter 18, Paragraph 18.1 (dated July 23, 2001) states "**Office of the Chief Information Officer**. The Office is headed by the Chief Information Officer (CIO) who is responsible to the Secretary with operational responsibility to the Assistant Secretary - Policy, Management and Budget. The CIO is assisted by a Deputy CIO."

[2] GAO-04-823, What GAO Found

[3] GAO-04-823, Matter for Congressional Consideration

[4] GAO-04-823, Appendix VII, Comments from the Department of the Interior

[5] GAO-04-823, Legislative Evolution of Agency CIO Roles and Responsibilities

[6] Authority to Ensure Compliance

- FISMA, Section 3544 "Federal Agency Responsibilities," Paragraph (a)3 states:
- Paragraph (a) "In General.–The head of each agency shall–"
- Paragraph (a)3 "delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—"

[7] Information Technology Resources Management, August 7, 2002, Secretary Norton

[8] Secretarial order number 3244, "Standardization of Information Technology Functions and Establishment of Funding Authorities"

- Paragraph 5(c) of Secretary Norton's Order states "The following IT functions must be under the purview of all bureau and office CIO organizations:
  (1) technology management (enterprise architecture, capital planning and investment control (CPIC) processes, and information technology acquisition);
  (2) security management (system accreditation and certification, access control, and compliance);
  (3) information management (records management, Freedom of Information Act, information quality, Privacy Act, and the Government Paperwork Elimination Act);
  (4) telecommunications management (network security and optimization, bill auditing and analysis, radio spectrum management, and wireless communication);
  (5) inventory and asset management (tracking and accounting of information resources and equipment);
  (6) strategic planning (development and redesign of the organization's IT work processes);
  (7) project management (monitoring the project scope, schedule, and budget targets); and
  (8) IT career/skills management (developing standards and training requirements for IT professionals).

[9] Presentation to the Assistant Secretaries and Bureau Directors, entitled "Addressing Critical Information Technology Problems in Interior," dated February 25, 2008

[10] Annual Summaries of Major Management and Performance Challenges

- In FY2003, "Shortcomings in policies, procedures, and controls need to be addressed before Information Technology (IT) systems and data at DOI are adequately protected." The summary went on to state "…DOI's overall security program does not demonstrate that all information systems supporting its operations and assets are adequately protected."

- In FY2004, "Although improvements have been made to information system security controls over financial management systems, more needs to be accomplished to ensure that all DOI entities fully comply with all Federal financial management systems requirements specified in Appendix III to OMB Circular A-130, "Management of Federal Information Resources."

- In FY2005, "…after thorough evaluation to assess compliance with FISMA, we have determined that there are significant weaknesses in the DOI IT security program and compliance with FISMA requirements." The summary went on to state "DOI lacks an effective agency-wide strategy to implement and provide oversight for the various policies and procedures issued."

- In FY2006, "…significant weaknesses remain in the DOI IT Security Program."

- In FY2007, "…our evaluation determined the DOI information security program has not been consistently implemented throughout the Department and the resulting weaknesses hinder achievement of full compliance with FISMA."

[11] IntelGuardians, Inc., Findings and Recommendations Report, March 28, 2008, Paragraph 6.0 Conclusions

[12] Presentation to the Assistant Secretaries and Bureau Directors, entitled "Addressing Critical Information Technology Problems in Interior," dated February 25, 2008

[13] Internet Outbound Flow Statistics for the Month of January 2008 (Draft)

[14] Financial Business Management System

- FY2003 Annual Summary of Major Management and Performance Challenges, "The Department of the Interior's (DOI or the Department) financial management systems do not produce timely, accurate and reliable information throughout the course of the year."

- FY2004 Annual Summary of Major Management and Performance Challenges "Although the Department has made some progress, internal control weaknesses continue to hinder DOI financial management systems. As a result, tests performed by the auditors assigned to conduct the Departmental consolidated audit disclosed instances where the Department's financial management systems did not substantially comply with the Federal Financial Management Improvement Act." and "The cornerstone of the Department's plan to transform financial management is the FBMS. FBMS will replace a variety of outdated, stand-alone, mainframe-based systems that are costly to operate and difficult to secure, cannot provide timely financial and performance information, and do not comply fully with all financial system standards."

- FY2005 Annual Summary of Major Management and Performance Challenges "On September 29, 2005, DOI removed BearingPoint, their contractor from the project. While the vision and the goals of the project remain the same, DOI is currently revising their implementation timelines and their training schedules."

- BearingPoint Quarterly Report to the Securities and Exchange Commission, dated June 30, 2007, "…in September 2006, the Company filed a lawsuit against the DOI in the U.S. Court of Federal Claims, seeking to overturn the termination for cause. On April 30, 2007, the U.S. Court of Federal Claims granted the Company's motion to dismiss the lawsuit, holding that the DOI's termination for default was procedurally invalid."

- FY2006 Annual Summary of Major Management and Performance Challenges, "The Department began implementing FBMS in FY2005 and planned to have the system fully implemented by the end of FY2008. However, on September 29, 2005, DOI removed BearingPoint, its contractor, form the project. DOI then awarded a new contract to IBM Consulting Services on February 28,

2006, to replace BearingPoint as the system integrator and revised the implementation date from FY2008 to FY2011."

- FY2007 Annual Summary of Major Management and Performance Challenges, it was noted the implementation date for FBMS was FY2012.

[15] Supplement to Analytical Perspectives Budget of the United States Government Fiscal Year 2009, ISBN 978-0-16-079690-6, Table 9.1, Effectiveness of Agencies IT Management and E-Gov Processes

[16] Presentation to the Assistant Secretaries and Bureau Directors, entitled "Addressing Critical Information Technology Problems in Interior," dated February 25, 2008

[17] Information Technology Management Reform Study Executive Summary

[18] Information Technology Management Reform Study Final Report Presentation Deck Slide 5

[19] Information Technology Management Reform Study Final Report Presentation Deck Slide 9

[20] Information Technology Management Reform Study Final Report Presentation Deck Slide 27

[21] http://www.gartner.com/it/about_gartner.jsp. Gartner, Inc. (NYSE: IT) is an information and technology research and advisory firm headquartered in Stamford, Connecticut. Gartner clients include many large corporations and government agencies, as well as technology companies and the investment community. The company consists of Gartner Research, Gartner Executive Programs, Gartner Consulting and Gartner Events. Founded in 1979, Gartner has 4,000 associates, including 1,200 research analysts and consultants in 75 countries.

[22] IT Infrastructure Line of Business Final Data Analysis Report Gartner 19 December 2007, slide 10

[23] IT Infrastructure Line of Business Final Data Analysis Report Gartner 19 December 2007, slide 19

[24] The E-Government Act, Section 3544 "Federal Agency Responsibilities," Paragraph(a)3(d) states, "In General.–The head of each agency shall– delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including— training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities…"

[25] Enterprise Active Directory Operational Standardization Project Charter and Statement of Work, Figure 2 "Project Governance Context"