



ed States General Accounting Office

stimony

re the Subcommittee on Immigration and Claims,
ommittee on the Judiciary, U.S. House of Representatives

For Release on Delivery
Expected at
10:00 a.m. EDT
Thursday,
October 11, 2001

SECURING AMERICA'S BORDERS

INS Faces Information Technology Planning and Implementation Challenges

Statement of Randolph C. Hite
Director, Information Technology Systems Issues



Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on the Immigration and Naturalization Service's (INS) use of information technology (IT) to secure America's borders. My statement is based on reports we have issued during the last year that address INS' institutional IT management process controls, and our recent follow-up work to determine progress in implementing the recommendations that we made in these reports.¹

IT management process controls, such as investment management and enterprise architecture management, are recognized indicators of whether an organization, like INS, can successfully develop, acquire, implement, operate, and maintain IT systems and related infrastructure. Together, enterprise architecture management and investment management, respectively, serve to explicitly blueprint the future operational environment, in both business and technology terms, needed for an organization to effectively and efficiently achieve its strategic mission, and to assure adequate senior executive involvement in the crucial capital investment decisions required to effectively and efficiently put in place this target environment.²

In summary, INS has yet to implement the set of practices (e.g., policies, activities, abilities, measures) associated with effective IT investment and enterprise architecture management. As a result, INS is not positioned to know that its ongoing and planned IT investments are the "right things to do," meaning it does not know whether these investments will produce mission value commensurate with costs and risks or whether these investments are superior to competing investment alternatives. Further, INS does not know that these investments are "being done the right way," meaning it does not know whether investments are aligned with an agencywide blueprint (architecture) that defines how the agency plans to operationally and technologically function in the future, and it does not

¹*Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture* (GAO/AIMD-00-212, August 1, 2000) and *Information Technology: INS Needs to Better Strengthen its Investment Management Capability* (GAO-01-146, December 29, 2000).

²The importance of both agency architectures and IT investment management is recognized by the Clinger-Cohen Act and guidance from the Office of Management and Budget (OMB), as well as leading private and public sector organizations. (In the fiscal year 1997 Omnibus Consolidated Appropriations Act, P.L. 104-208, the name "Clinger-Cohen Act of 1996" was given to Divisions D (the Federal Acquisition Reform Act) and E (the Information Technology Management Reform Act) of the 1996 DOD Authorization Act, P.L. 104-106.)

know whether each of its ongoing investments are meeting their cost, schedule, and performance commitments.

In light of the recent terrorist attacks, INS' border security mission has gained prominence. How effectively INS can perform this vital mission will depend in part on how well it can leverage both existing and new IT resources. Given the difficulty of this mission, effectively and efficiently leveraging technology would be a challenge even if INS had the requisite management process controls. Since it does not, INS' challenge becomes even more challenging. In the recommendations that we made in our recent reports, we recognized that INS would have to make near-term investments to meet pressing mission needs before it had established IT management process controls. A key to INS' doing so effectively is for its leadership to proactively compensate for missing management controls by ensuring that the requisite human capital skills and expertise are brought to bear on IT projects supporting its border security mission. While this is clearly not a long-term solution to the agency's IT management challenges, this strategy can serve as a temporary "crutch" until INS can follow through on its ongoing efforts to establish and implement effective management process controls and devote the resources to ensuring that these controls are practiced agencywide.

Background

The mission of INS, an agency of the Department of Justice, is to administer and enforce the immigration laws of the United States. To accomplish its mission, INS has three interrelated business areas—enforcement, immigration services, and corporate (i.e., mission-support) services. Enforcement includes border inspections of persons entering the United States, detecting and preventing smuggling and illegal entry, and identifying and removing illegal entrants. Immigration services include granting legal permanent residence status, nonimmigrant status (e.g. students and tourists), and naturalization. INS efforts to protect our nation's borders are performed under both of these core mission areas. Corporate services include functions such as financial and human capital management. INS' field structure consists of 3 regional offices, 4 regional service centers, 3 administrative centers, 36 district offices, 21 Border Patrol sectors, and more than 300 land, sea, and air ports of entry.

To carry out its responsibilities, INS relies on IT. For example, the Integrated Surveillance Intelligence System (ISIS) is to provide "24 by 7" border coverage through ground-based sensors, fixed cameras, and

computer-aided detection capabilities. Also the Student Exchange Visitor Information System (SEVIS) is to manage information about nonimmigrant foreign students and exchange visitors from schools and exchange programs.

Each year INS invests, on average, about \$300 million in IT systems, infrastructure, and services.

INS' Longstanding Problems in Managing IT Projects Have Been Well Chronicled

Recent studies have identified significant weaknesses in INS' management of IT projects. In August 1998, the Logistics Management Institute (LMI) reported that INS did not track and manage projects to a set of cost, schedule, technical, and benefit baselines.³ LMI noted that while INS had defined good procedures for developing systems, it did not consistently follow them. Similarly, in July 1999, the Justice Inspector General (IG) reported that INS was not adequately managing its IT systems.⁴ In particular, the IG reported that (1) estimated completion dates for some IT projects had been delayed without explanation, (2) project costs continued to spiral upward with no justification for how funds are spent, and (3) projects were nearing completion with no assurance that they would meet performance and functional requirements.

Despite Recent Progress, INS Lacks Important Institutional IT Management Controls

In light of the reported problems on individual projects, we reviewed INS' institutional approach to managing IT to determine the root cause of project problems and to provide the basis for recommending fundamental management reform. In doing so, we focused on two key and closely related IT management process controls: investment management and enterprise architecture management. In August 2000 and December 2000, we reported that INS lacked both of these management process controls

³*Reengineering Information Technology Management at the Immigration and Naturalization Service*, Logistics Management Institute, August 1998. LMI is a private, nonprofit corporation that provides management consulting, research, and analysis to governments and other nonprofit organizations.

⁴*Follow-up Review: Immigration and Naturalization Service Management of Automation Programs*, Office of the Inspector General, Audit Division, U.S. Department of Justice, July 1999.

because the former agency leadership had not viewed either as an institutional priority. We also provided INS, through our recommendations, a roadmap for establishing and implementing both controls.⁵ INS agreed with our findings and recommendations, and it committed to implementing the recommendations. Although INS has made progress to date in doing so, much remains to be accomplished before it will have implemented these management controls and have the capability to effectively and efficiently manage IT.

Effective Planning and Implementation of IT Requires Architecture-Centric Investment Management

As defined by the Clinger-Cohen Act of 1996 and associated Office and Management and Budget instructions, and as practiced by leading public and private sector organizations, effective IT investment management requires implementing process controls for maximizing the value and assessing and managing the risks of investments. The goal is to have the means in place and functioning to help ensure that IT projects are being implemented at acceptable costs, within reasonable and expected time frames, and are contributing to tangible, observable improvements in mission performance.

To help agencies understand their respective IT investment management capabilities, we developed the Information Technology Investment Management (ITIM) maturity framework. The ITIM framework is a tool that identifies critical processes and practices for successful IT investment and organizes them into a framework of increasingly mature stages.⁶ A fundamental premise of the framework is that each incremental stage lays a foundation on which subsequent stages build. The initial stage focuses on controlling investments already underway, while also starting to establish a way to select new investments. Later stages emphasize managing investments from a portfolio perspective in which individual investments are evaluated as a set of competing options based on their contribution to mission goals and objectives. The goal is to arrive at the optimal mix of projects in which to invest resources. Agencies can use the framework for assessing the strengths and weaknesses of their existing investment management processes and for developing a roadmap for improvement. The Chief Information Officers Council has endorsed the ITIM framework.

⁵GAO/AIMD-00-212, August 1, 2000 and GAO-01-146, December 29, 2000.

⁶*Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Exposure Draft) (GAO/AIMD-10.1.23, May 2000).

In order for an agency to achieve a minimum level of IT management effectiveness, it needs to first gain control of its current investments. To do this, it must establish and implement processes and practices for ensuring that projects have defined cost, schedule, and performance expectations; that projects are continuously controlled to determine whether commitments are being met and to address deviations; and that decisionmakers have this basic investment information to use in selecting new projects for funding and deciding whether to continue existing projects. Once it has established these project-specific control and selection processes, the agency then should move to considering each new investment not as a separate and distinct project, but rather as part of an integrated portfolio of investments that collectively contribute to mission goals and objectives. To do this, the agency should establish and implement processes and practices for analyzing the relative pros and cons of competing investment options and selecting a set of investments that agency leadership believes best meets mission-based and explicitly defined investment criteria.

Integral to an effective IT investment management process is having a well-defined enterprise architecture or blueprint for guiding the content and characteristics of investments in new and existing IT systems, infrastructure, and services. The goal is to help ensure that the new and modified IT assets will, among other things, be designed and implemented to promote interoperability and avoid duplication, thereby optimizing agencywide performance and accountability.

In more specific terms, an enterprise architecture is a comprehensive and systematically derived description of organization's operations, both in logical terms (including business functions and applications, business rules, work locations, information needs and users, and the interrelationships among these variables) and in technical terms (including IT hardware, software, data, communications, security, and performance characteristics and standards). If defined properly, enterprise architectures can clarify and help optimize the connections among an organization's interrelated and interdependent business operations and the underlying IT supporting these operations.⁷ A complete enterprise

⁷In our experience with federal agencies, attempts to define and build major systems without first completing an enterprise systems architecture often result in systems that do not effectively optimize mission performance, being duplicative, not well integrated, and unnecessarily costly to maintain and interface. See, for example, *Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization* (GAO/AIMD-97-30, February 3, 1997) and *Customs Service Modernization: Architecture Must Be Complete and Enforced to Effectively Build and Maintain Systems* (GAO/AIMD-98-70, May 5, 1998).

architecture includes both the current architecture (as it is now) and the target architecture (the goal), as well as a plan for moving between the two. To assist agencies in developing, maintaining, and implementing enterprise architectures, we collaborated with the Chief Information Officers Council to develop a practical guide for enterprise architecture management.⁸

INS Has Taken Steps to Improve IT Investment Management But Effective Processes and Practices Have Yet To Be Implemented

In December 2000 we reported that while INS had some investment control elements, it nevertheless lacked the full set of foundational investment management processes and practices needed to effectively control its ongoing IT projects and ensure that it was meeting cost, schedule, and performance commitments and contributing to measurable mission performance and accountability goals. For example, INS had not consistently (1) developed and maintained project management plans that specified cost and schedule baselines, (2) linked projects to INS mission needs, and (3) tracked and monitored projects to determine whether they were meeting project baselines and mission needs. Without this information, the investment review board (that, to its credit, INS had established to make investment selection decisions) could not act to effectively address deviations. The result was increased risk that the technology needed to support mission goals, such as securing America's borders, would not be delivered on time and on budget and would not perform as intended.

We also reported in December 2000 that INS was not effectively managing its IT investments, both new proposals and ongoing projects, as a portfolio, meaning that INS' investment review board was not making portfolio selection and control decisions in terms of what mix of proposed and ongoing projects collectively best supported achievement of mission needs and priorities. In particular, INS had not defined, and thus was not using, investment selection criteria that were linked to mission needs and addressed cost, schedule, benefits, and risk. Without such criteria, the board lacked the basic information needed to assess the relative merits of and make trade-offs among its options for increasing IT capabilities, including acquiring new, enhancing existing, and operating and maintaining existing systems and infrastructure. By not employing

⁸A Practical Guide to Federal Enterprise Architecture, version 1.0 (Chief Information Officer Council, February 2001).

portfolio investment management, we concluded that INS was at risk of not having the right mix of technology in place to support critical mission priorities, such as protecting America's borders against the threat of terrorism. Accordingly, we made a series of recommendations to INS aimed at, among other things, treating the development and implementation of IT investment management process controls as an agency priority and managing them as such.

Since our December 2000 report, INS has taken steps to implement our recommendations for establishing and following rigorous and disciplined investment management controls. In particular, it has developed a guide for IT investment management that, according to INS, defines many of the missing processes and practices. The key for INS will be to ensure that these processes and practices are effectively implemented. Given that the Justice IG, in reporting on IT project problems, found that INS was not following established project management procedures, successful implementation of INS' newly developed investment guide cannot be taken for granted, and needs to be given the attention it deserves.

INS Is Taking Steps to Develop an Enterprise Architecture, But It Still Lacks this Important IT Management Tool

In July 2000, we reported that INS did not have an enterprise architecture, including a description of both its "as is" and "to be" operational and technology environments and a roadmap for transitioning between the two environments. Moreover, we also reported that the efforts underway to develop the architecture were flawed and unlikely to produce useful architectural products.⁹ In particular, the development efforts were limited to a producing a bottom-up description of INS' current IT environment (e.g., hardware and system software computing platforms, data structures and schemas, software applications) and mapping the software applications to mission areas. While this was a reasonable start to describing the current architectural environment, important steps still needed to be accomplished, such as linking the systems environment description to a decomposed view of agency mission areas, including each area's component business functions, information needs, and information flows among functions. Moreover, doing this reliably required the participation of agency business owners; however, these owners were not involved.

⁹*Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture* (GAO/AIMD-00-212, August 1, 2000).

Also, INS had not begun developing either a target architecture or a capital investment plan for sequencing the projects that will allow it to migrate from its current architecture to its target architecture. These two components would be integral to INS' previously mentioned need to implement effective investment management processes and practices because both controlling and selecting IT projects requires ensuring that these projects are provided for in the sequencing plan and are aligned with the target architecture. By doing so, investment decisionmakers can know (1) how proposed projects contribute to the strategic mission goals, needs, and priorities and (2) whether these projects will be engineered according to the technical models and standards, that are both embedded in the target architecture descriptions.

Equally important, we reported that INS' architecture development efforts were not being managed as a formal program, including having meaningful plans that provided a detailed breakdown of the work and associated schedules and resource needs. Further, these efforts did not include performance measures and progress reporting requirements to ensure that the effort was progressing satisfactorily. As a result, we concluded that it was unlikely that INS could produce a meaningful architecture that could be used to effectively and efficiently guide and constrain IT investment and project decisionmaking. Accordingly, we made a series of recommendations to INS aimed at making development of an enterprise architecture an agency priority and managing it as such.

INS agreed with our recommendations and has since taken steps to improve its ability to manage development of its enterprise architecture. For example, INS reports that it has (1) established an enterprise architecture program office, (2) developed a business model of its current operational environment, (3) developed plans for defining a target architecture and capital investment sequencing plan, and (4) established teams representing all business units to define current and target business environments. While these are positive steps, they are only a beginning, and much remains to be accomplished before INS will have the kind of agency blueprint needed to support effective project investment and engineering decision-making.

In conclusion, INS is a challenged agency when it comes to effectively and efficiently managing IT. Nevertheless, immediate border security demands have emerged that require the agency to effectively leverage technology as part of its response to these demands. To address this situation in the near

term, INS will have to ensure that it compensates for management process control weaknesses by engaging the requisite human capital expertise on its border security efforts. In the long term, INS will need to continue to implement our open recommendations aimed at reforming the agency's IT management process controls.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be happy to address any question that you have.

(310222)