Information Sharing: Paving the Road to Transformation

WHITE PAPER

Sponsored by: Cisco Systems Inc.

Judith A. Carr, Ph.D. Jenny V. Whitmer
March 2007

GOVERNMENT INSIGHTS OPINION

Governments at all levels — federal, state, and local — as well as defense and national security organizations are challenged to reposition, reinvent, and realign themselves in light of increasing demands for a more cost-effective, citizen-centric, and networked government. A combination of economic, political, strategic business, and technical advances has positioned the public sector to transform the way it orchestrates the business of government — moving away from autonomy toward a connected, cross-boundary business model in which information is shared in a secure environment.

The road to transformation is not a journey without risk. Governments and their private sector partners must work to identify collaborative technologies and insert these technologies where appropriate to streamline government business functions. Government Insights believes that paving the road to transformation will require innovation and a shift in strategic focus and offers the following recommendations to drive the process:

- Develop strategic partnerships to address the critical technical and organizational issues inherent in transformation. Cross-boundary business models require collaborative efforts across constituencies.
- Address information sharing as a business initiative and design technology solutions that align with the mission and facilitate collaborative business models. Initiatives that do not address the organizational and "softside" issues will fail.
- Engage executive leadership to create a culture and organizational processes that leverage the technical infrastructure and enable innovative funding, governance models, and metrics to support the new enterprise business models.
- Address political and organizational issues prior to or in tandem with technical issues. Many organizations focus on the technical issues first, leaving the more complex big-picture issues for another time. Working the high-level issues earlier rather than later will remove many of the roadblocks to the technology implementation.

March 2007, Government Insights #GI206007

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.government-insights.com

IN THIS WHITE PAPER

This Government Insights White Paper provides the background for cross-government information sharing initiatives and provides an analysis of the technical, business, political, and organizational issues that constitute critical roadblocks to transformation. This paper also highlights a current initiative related to information sharing: Secure Information Sharing Architecture (SISA), a private sector collaborative effort that provides the technology framework for connecting government in a secure environment.

SITUATION OVERVIEW

Information sharing is critical to government's ability to serve citizens. Broadening agency missions require teams that comprise public employees from multiple agencies, contractors, and nonprofit organizations. These teams demand the ability to interact and collaborate across organizations. Teams are distributed globally with military, civilian officials, and contractors working internationally. Workers require timely, secure access to accurate data, information, and knowledge to accomplish their missions. Yet, while the information exists, siloed government technology infrastructure and policy do not adequately support information processing and exchange.

Charles Allen, Assistant Secretary for Intelligence and Analysis and Chief Intelligence Officer, Department of Homeland Security, cites three key principles of information sharing: partnership, infrastructure, and respect for privacy and civil liberties. The vision that grew out of the lessons of 9/11 is of a seamless community of intelligence; Department of Defense (DoD); and federal, state, and local governments so that vital information can flow freely across all levels of government. In support of this vision, 43 intelligence fusion centers have been established by local governments to collect and analyze information in support of national security. DoD, the intelligence community, and federal agencies are key partners and provide resources for this community-based effort.

Information sharing and collaboration are priorities for newly named Director Mike McConnell, Office of the Director of National Intelligence (DNI). In support of the information sharing initiative, Dale Meyerrose, DNI Associate Director and CIO, was recently named the Information Sharing Executive for the Intelligence Community. The appointment is significant because it institutionalizes the "need to share" paradigm across a previously siloed community. It is likely that the broader government community will follow suit to create a new job category, much like the community of chief knowledge officers that gained momentum in the late 1990s.

Although the information sharing initiative is formalized in legislation and is gaining momentum in terms of commitment, the initiative is not without its challenges. The remainder of this paper discusses those challenges and highlights opportunities for progress.

TRANSFORMATIONAL CHALLENGES/OPPORTUNITIES

Achieving the collaborative vision for transformation requires a new definition for the concept of "enterprise." The enterprise in collaborative government spans multiple organizations and/or levels of government and is much broader than a single agency.

Although an enterprise can be viewed as an individual organization (e.g., the Federal Aviation Administration) or a functional area such as disaster management that crosses more than one organization (e.g., all 22 agencies that fall under the Department of Homeland Security umbrella), it can also be defined globally to include all civilian, DoD, federal, state, and local agencies that provide security-related services across geographies. The mission of government can be as broad as national security or as narrow as paying unemployment benefits.

The challenge lies in scoping the definition of an enterprise to be congruent with new multi-agency initiatives requiring unprecedented collaboration and information sharing. The complexity of the challenge increases exponentially as the definition of enterprise expands to include more and more horizontal and vertical levels of government and defense and their private sector partners.

Technical and organizational issues that seem monumental for a single agency increase exponentially as the enterprise expands to address the global requirements of today's environment. How do you create an infrastructure that spans an infinite and changing number of organizations? How do you migrate multiple agencies from "as is" to "to be" architectures that leverage existing legacy systems and build the capability to support large-scale information sharing? How do you address policy issues that hold individual missions sacred while enabling governments to engage in broader initiatives? How do you govern and organize the transformation process? How do you finesse the cultural requirements and the change management process? The questions and issues are numerous. If answers are to be found, then government executives and their partners must address these critical issues with innovation and collaboration.

Creating the Technical Foundation for Transformation

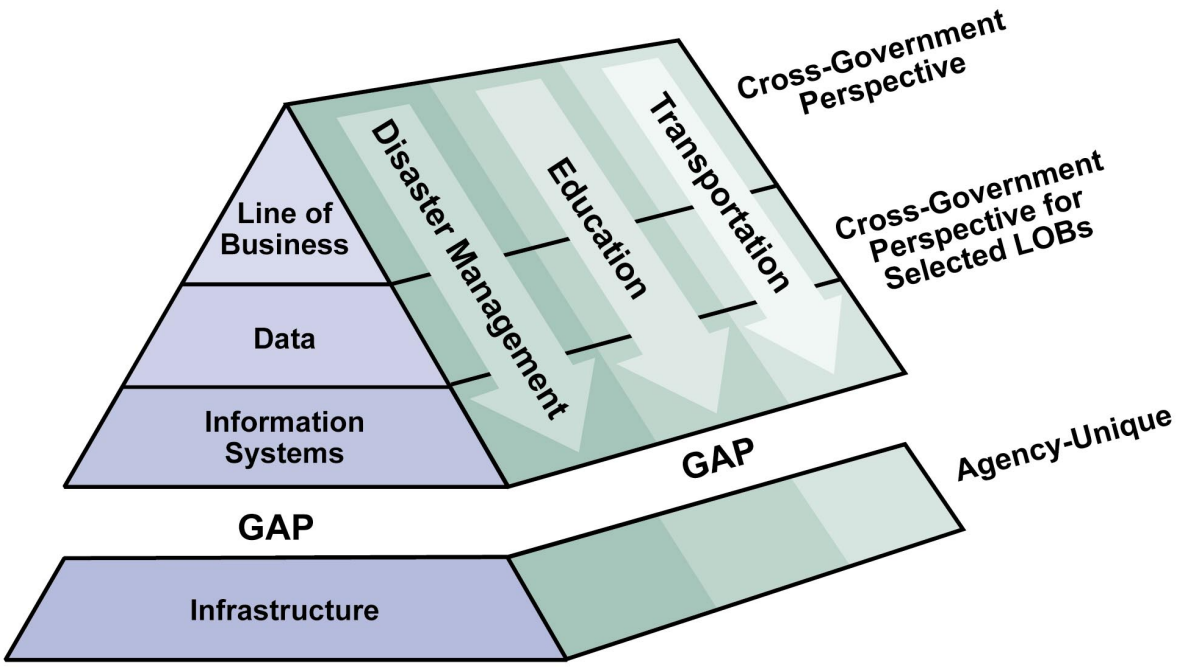
An enterprise architecture (EA) is a blueprint describing the current and desired states of an organization or functional area in both programmatic and technical terms, as well as a plan for transitioning between the two states. The technical challenge is to create an EA that transcends the definition of enterprise — an EA that enables information sharing and collaboration in a secure environment regardless of agency participation and/or technical infrastructure.

The U.S. Federal Enterprise Architecture (FEA) provides a good example or model plan for driving interoperability and citizen-centric service delivery models, consolidating redundant processes and systems across agencies, and reducing the cost of federal government in general. Although positioned as a key enabler of government transformation, the FEA has not yet achieved all the required outcomes. According to the General Accountability Office (GAO-06-831), FEA is "a work in progress," leaving much to be done in terms of actualizing organizational transformation.

The U.S. federal government Line of Business (LOB) initiative (see Figure 1) illustrates the information sharing challenges still inhibiting cross-agency collaboration in the United States and in other governments as well.

FIGURE 1

Federal Enterprise Architecture in Current State



Source: Government Insights, 2007

As Figure 1 illustrates, integration has started to take place at the business layer. LOB initiatives such as disaster management, education, and transportation require a cross-government perspective, which has encouraged integration between agency data and information sharing efforts. Success has been somewhat limited to selected lines of business. The most obvious failing is at the infrastructure layer, which remains, for the most part, agency-unique. Closing the gap is a goal of the FEA and will support information sharing across agencies.

The U.S. federal government spent over $3.5 billion on IT security in FY06.

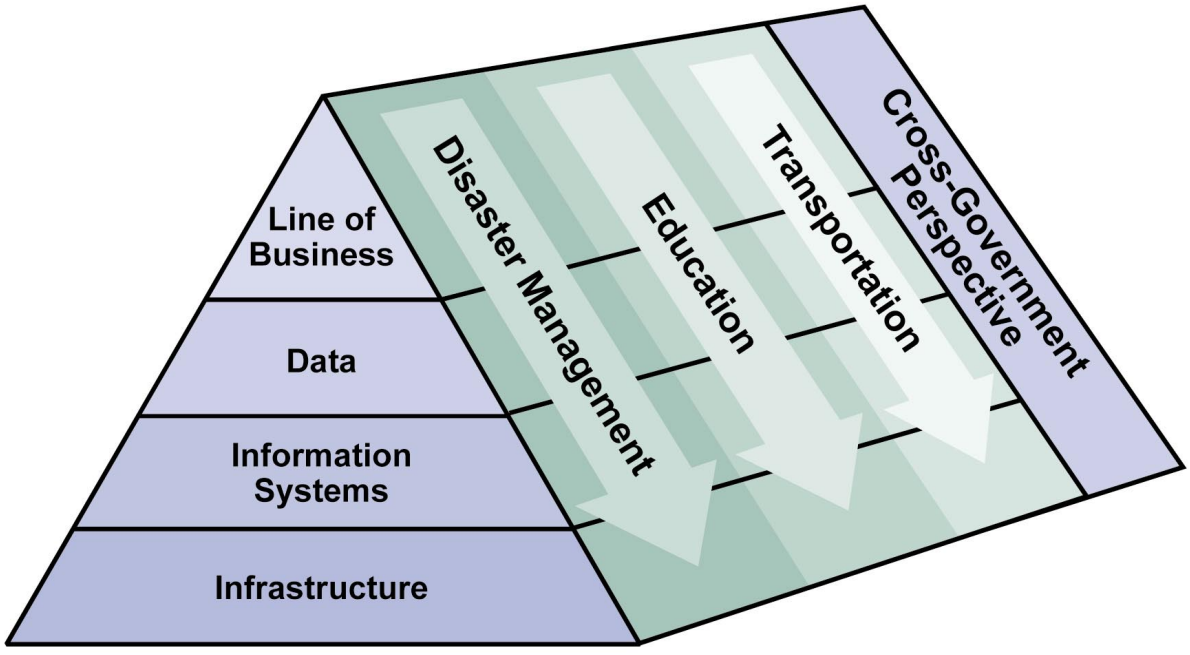
Agency executives cite one obvious explanation for clinging to agency-unique infrastructures as shown in Figure 1 — they are reluctant to let go of infrastructure control because they are accountable for mission outcomes derived from the layers supported at the infrastructure level. Executives continue to weigh the trade-off between security and information accessibility, as evidenced by the more than $3.5 billion spent on IT security in FY06. The challenge is that a system can be made so secure that it fails to share data in a timely manner with those who need it most. A system is most valuable when it is both secure and quickly accessible to valid users.

Another less obvious explanation is that individual agencies are still optimizing their own infrastructures, focusing on asset management, and repurposing existing inventory assets. In preparation for consolidation and cross-agency initiatives, agencies continue to evaluate siloed infrastructures to ensure they are technically prepared to transition to the new transformational models. Agencies must achieve a level of confidence in the infrastructure and technical solutions to fully capitalize on cross-agency collaboration and information sharing initiatives.

Figure 2 defines a transformational model for FEA that fully integrates business, data, information systems, and infrastructure to facilitate collaboration and the sharing of information across agencies. Two key changes are needed to move from the current state of FEA to this goal state. One, each level of integration must be seen from a cross-government perspective, not an agency-specific perspective. Two, the gap separating agency infrastructures must close, allowing the integration of infrastructures.

FIGURE 2

Federal Enterprise Architecture in Goal State



Source: Government Insights, 2007

Overcoming "Softside" Challenges to Transformation

In the context of this paper, transformation is defined as the use of IT to evolve or shift the way governments do business. Transformation can shatter silos and shift the model of government toward multi-agency coalitions. A single agency silo definition of enterprise is no longer adequate — a transformed government requires that information be shared across agencies to accomplish broad mission-critical strategies. This transformation constitutes one of the most profound change initiatives in the history of government. Realizing the vision of a fully connected government presents significant challenges.

While the major obstacles to achieving the vision have historically included technology, significant advances have been realized in that area. The most persistent problems relate to the "softside" issues of policy, organization, and people. Transformation requires significant changes in the culture of government and the fundamental tenets of how government is run — and government is slow to change. Several critical factors must be addressed to facilitate the change process:

- **Build a culture of trust.** Collaborative business models are built on trust. Government has its roots in bureaucracy where individual agencies were and still are accountable for outcomes directly associated with a single agency's mission. This silo psychology creates an environment in which resources and information are managed and protected to ensure that critical outcomes are met. U.S. federal agencies holding tight to agency-unique infrastructures illustrate a continued level of distrust in a transformation process that allows mission-critical information to cross organizational boundaries. Government executives must drive a culture of trust to enable collaboration without jeopardizing individual missions.

- **Implement collaborative funding models.** Operations and technology implementations have historically been funded with appropriations or earmarks for specific agencies or projects. Legislation, policy, and/or custom have precluded the commingling of funds for cross-agency initiatives. This funding model also holds true for funds recaptured through government efficiency initiatives. The challenge of implementing collaborative funding has been daunting across a single level of government (e.g., the federal government) but becomes monumental in light of vertical and horizontal partners engaged in transformational government. Collaborative funding models must be identified along with the political mandates for change. Cross-boundary technology initiatives must be articulated in terms of mission or political agenda to capture the attention and support of the policymakers needed to remove legislative barriers.

- **Engage executive leadership.** Transformation is a mission-critical issue with a strong technology component. Enterprise architecture provides the foundation for innovative technology solutions to support the vision of collaborative government. The challenge is that once the discussion moves to infrastructure, government executives often disengage and pass the baton to the office of the CIO. Organizations making this handoff run an increased risk of misalignment between the mission and its supporting technologies. The office of the CIO is well positioned to make technical decisions but is often ill equipped and/or positioned to work the more challenging enterprise issues of cross-boundary collaboration, funding, and driving change of significant magnitude. DNI CIO Meyerrose keeps senior leadership engaged by steering clear of techno-speak. He portrays EA as a vehicle for providing value to the mission and organization to keep it on the radar screen of executive leadership.

- **Implement collaborative governance models.** Effective governance structures enable enterprises to make informed IT investment decisions in support of strategic and tactical initiatives. Individual agencies struggle to institutionalize executive-sponsored IT decision making to prioritize and fund competing investment requirements. The task becomes even more formidable as the definition of enterprise is expanded to include multiple partners across levels of government. There is no top-down requirement for multi-agency governance to support transformation. Transformational leaders cite governance as the most challenging roadblock to implementing cross-boundary collaboration and information sharing. Without an effective enterprise governance process, it will be extremely difficult to identify appropriate technology solutions and define issues such as risk management, business value, and business alignment.

Governments and their private sector partners will need to work the technology issues in tandem with the "softside" issues to achieve the desired outcomes of transformation.

CASE STUDY IN COLLABORATION

Industry giants Cisco and Microsoft have joined forces with Decru, EMC Corporation, and Titus Labs to develop the Secure Information Sharing Architecture (SISA) to meet governments' requirement for a secure collaborative framework for sharing information. This private sector collaborative initiative illustrates the innovative partnerships that are forming to address a government business challenge:

> "We are incapable of storing, moving, and accessing information. No government does these things well, especially big governments. We spend $150 billion a year on information technology. You'd think we could share information by now. But we are still an analog government in a digital economy and culture."
>
> Tom Davis, Chairman
> House Committee on Government Reform
> 109th Congress

SISA, a COTS-based architecture, was developed at the request of defense and civilian agencies to close the EA gap (refer back to Figure 1) between cross-government perspectives and the unique infrastructures that support each agency. SISA provides a viable alternative to the industry practice of funding, developing, and maintaining customized, agency-specific infrastructures to ensure the security of mission-critical information. Customized infrastructures are extremely costly to the citizens who finance the duplicative systems, and they restrict collaborating agencies' access to applications and data that reside on the agency-specific architectures. In this siloed environment, agencies must make trade-offs between the need for security and the need to share information. These trade-offs are no longer acceptable to government executives and citizens.

SISA enables communities of interest (COI) to share information across secure collaboration architectures. Each partner organization's information is kept separate yet is accessible to COI partners according to individual authorization levels. SISA technology supports the information sharing needs of the "enterprise" regardless of where the enterprise boundaries are drawn or the number and mix of partners included.

Several technical features of SISA are designed to enhance users' access to information. A consistent interface overlays the architecture to give users a single access point to various agency applications and files. SISA allows information storage on a single, consolidated network, allowing users to move between physical locations while retaining access to information. SISA is built from Cisco and Microsoft products, which allows organizations already using these technologies to leverage existing technology investments while growing their information sharing capabilities.

Having established access to information, SISA approaches the other half of the equation: security. The architecture provides multiple levels of protection across hardware, software, and storage. Users are limited to documents with classifications they are authorized to access. Safeguards exist to protect against inadvertent disclosure of files, documents, and emails. Compliance with security regulations is also supported by SISA.

SISA is an example of private sector corporations forming a partnership to develop a technology solution whose primary focus is addressing mission-critical challenges in government. The blend of expertise brought to the table by each company makes possible the integration of enterprise architecture and lines of business with an infrastructure that crosses organizational boundaries.

CONCLUSION

Governments have embraced the concept of transformation. Requirements to enhance national security, streamline operations, and evolve to citizen-centric service delivery models have driven a broader definition of enterprise and mission — one encompassing multiple agencies working together for common outcomes. Sharing information across boundaries is central to this vision for a transformed government.

Embracing the concept of transformation is a good first step, but it is not enough. Enormous technical, political, and organizational challenges must be overcome to actualize full transformation. Governments must fundamentally change how they orchestrate the business of government — from the technologies that provide the infrastructure to the policies and culture that define business and process. The task is daunting and the requirement for institutional change is monumental.