

IC ITE

DOING IN COMMON

WHAT IS COMMONLY DONE



INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY ENTERPRISE (IC ITE) TASK FORCE

FEBRUARY 2013

ACKNOWLEDGEMENTS

INSA CHAIRMAN

Ambassador John Negroponte

INSA STAFF

Joe DeTrani, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Chris Barnes, *INSA Senior Fellow*

Daniel Allen, *INSA Fellow*

INSA IC ITE TASK FORCE RESEARCH AND WRITING TEAM

Terry Roberts, *INSA Cyber Council Chairwoman and Vice President of Intelligence and Cyber, TASC*

Nuhad Karaki, *Executive Vice President and COO, Inceptre Corporation*

Paige Atkins, *Vice President for Cyber/IT Research, Virginia Tech Applied Research Corporation*

Robert Giesler, *Senior Vice President for Cyber Programs, SAIC*

Dan Doney, *CMU SEI*

Larry Hultberg, *Accenture*

EDITORIAL REVIEW

Joseph M. Mazzafro, *Oracle National Security Group*

Beth Finan, *Copy Editor*

Introduction

The purpose of this paper is to communicate the perspectives and vision of the Intelligence Community (IC) Chief Information Officers (CIOs) regarding the IC Information Technology Enterprise (ITE). The INSA Cyber Council's IC ITE Task Force engaged IC and Department of Defense (DoD) thought-leaders to explore the challenges and opportunities in the IC IT environment. Through interviews and research, this paper includes inputs from key senior IC officials responsible for the IC IT Enterprise implementation, as service providers as well as users.

As the first component in a series of white papers, which will ultimately form the basis for a comprehensive assessment and recommendations, this study presents a decidedly optimistic perspective regarding opportunities and challenges in implementing IC ITE. The intent is to convey government planning and expectations so that the community at large, at a minimum, can identify senior-level expectations that are driving changes in Information Technology (IT). Ideally, the thoughts in this paper will add transparency and understanding, to broadly inform the Defense Industrial Base (DIB), large and small businesses and other partners on the direction and challenges of implementing the IC ITE. Future papers will explore actionable steps the IC can pursue to ensure successful implementation, focusing in particular on how private industry will be affected and how it can prepare to anticipate and support major changes. No doubt, ultimate success will depend on cultural, process, and organizational shifts within government, industry and academia to be successful in such a major transition.

In order to successfully implement the IC ITE vision, the IC needs to take four actions requiring near-term investments with long-term, sustainable benefits:

1. Determine the IC ITE Architecture, from the Agency, Mission and User standpoint
2. Define what common IT is for this first wave of transformation
3. Deploy common IT services to gain experience and shape the next wave
4. Establish the priorities for the leadership, technology, workforce, and cultural challenges to achieve a broader, deeper implementation

With strong leadership, constant evaluation, and the right incentives, these actions should lead to an agile process for implementation of key IC ITE components, leading to realization of the fiscal and mission benefits of the enterprise for the IC.

Background

In 2012, the Director of National Intelligence (DNI) approved an ambitious strategy proposed by the IC CIO. This strategy was developed in coordination with the CIOs of the big five intelligence agencies (the Central Intelligence Agency (CIA), National Security Agency (NSA), Defense Intelligence Agency (DIA), National Reconnaissance Organization (NRO), and the National Geospatial-Intelligence Agency (NGA)) to change from the historically agency-centric IT approach to a new model - that of a common architecture and operations as an IC-wide enterprise. The primary objective is that the majority of IC Missions will benefit from improved agility, scalability, and security while realizing lower operating costs through the shared use of commercially developed IT and computing advances such as cloud technologies, virtualization, thin-client

desktops, big data analytics, application stores, and improved security.¹ Another key driver behind this IC-wide strategy was that in late 2011 the Intelligence Community anticipated it would need to formulate how it would take its share of the upcoming government budget reductions. The Office of the Director of National Intelligence (ODNI) submitted plans to reduce the budgets of intelligence agencies over the next decade, and IC leaders expect to reap a significant portion of their savings in information technology efficiencies.

As a result, in 2012 the IC CIO embarked on a significant IT transformation for the IC. This transformation, guided by the Intelligence Community Information Technology Enterprise (IC ITE) Strategy, focuses on enabling greater integration, information sharing, and information safeguarding through a common IC IT approach that proposes to improve mission and business processes, and substantially reduce costs. The IC ITE Strategy directly supports the ODNI strategic initiative of delivering global and assured services that are always functioning, accessible and taking full advantage of agile and efficient mission capabilities.¹ This strategy lays the groundwork to enhance information sharing – through improved infrastructure, capabilities, business operations, governance, oversight, and strategic partnerships. The IC ITE Strategy intends to guide the IC IT community over the next 5 years, moving the IC from historical agency-specific IT models to a new, more common architecture – one that, through shared services, will become the strategic IT venue for the IC. A key challenge is striking the balance between fully leveraging state of the art IT and enterprise approaches, while sustaining and enhancing mission agility, information sharing, information assurance, and satisfaction of unique customer requirements.

Each intelligence agency's mission to provide secure technology services to its own stakeholders has perpetuated the independent development of infrastructure and applications, and inhibited data sharing across organizational and mission lines. Even in light of the ODNI plan for an IC ITE and the progress made in establishing a high-level vision, strategic direction, and engineering level standards, the Community's IT capabilities remain largely agency-centric and independent. IT spending across the 17-plus agencies in the Community is estimated to be as much as 25 percent of the National Intelligence Program (NIP) funding not including IT funded as part of other program line items. In the face of fiscal uncertainty, this is a logical area to examine for savings with the added benefit of further integrating the Community.

As the IC moves towards implementing capabilities to enable discovery and data sharing to support the direction set out in IC Directive 501, leaders within the Community must accelerate the establishment and alignment of standards to allow technologists to apply leading edge capabilities in moving initiatives forward. For data to be shared across intelligence agencies, the Community will also need to rethink how it defines and executes its data security and access control in a virtualized, cloud-enabled delivery architecture.

Technological advancement and innovation in IT is being led by the private sector, often at a breathtaking pace. Prudent leveraging of these advancements has the potential to accelerate the DNI's strategic intent for information sharing across agencies, intelligence disciplines and mission sets. In order to manage these historic changes in operations and the supporting cultural shift to enable sharing data across the IC, CIOs and technology leaders within the IC will need to restructure the coordination, synchronization, and governance model from one centered on control within stovepipes to one that fully leverages innovation across the enterprise with agility.

Information sharing and the quality of analytics and operations are critical. Data sharing can help stakeholders make better decisions using advanced analytics. The IC's IT leaders have the opportunity to collaborate and help turn big data into enriched data, providing their mission partners—whether policy makers or warfighters—the right data at the right time and place to make the most informed decisions.

IC ITE Vision and Future Direction

“Do in common that which is commonly done.” This is the theme that is frequently cited by IT managers within the IC to explain the IC ITE. IC ITE is a significant shift in how to plan for, develop and operate IC IT – moving the community from a collection of agency-centric enterprises to a single, secure, coherent, mutually operated and integrated IC IT Enterprise.

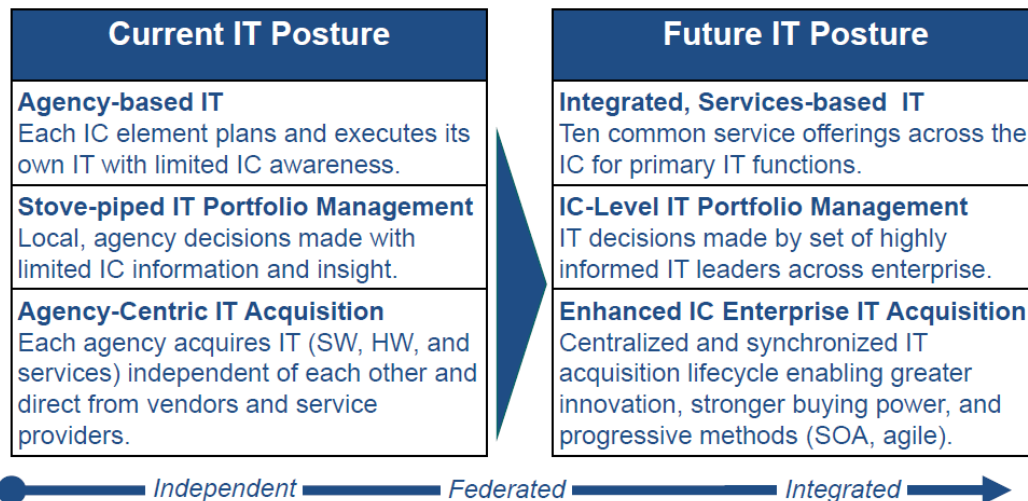


Figure 1 IC IT Current and Future

The IC ITE focuses on greater integration, information security, and information sharing while seeking substantial cost reductions through shared infrastructure and service models. The IC recognizes that each agency has particular strengths or core competencies that can be better leveraged by designating IC elements to act as Service Providers for specific capabilities for the entire Community. The DNI designates the IC Service Providers who are responsible for determining investment requirements and using their respective budget and acquisition and contract authorities to execute their IC ITE responsibilities. Currently identified common services and their respective providers include: the Desktop Environment, DIA and NGA; IC Cloud Services, NSA and CIA; Transport, NRO; Applications Mall, NSA; and Applications Stores, all agencies.

The IC ITE will be delivered in increments with Increment 1 (Initial Operating Capability, or - IOC) in FY13 and achievement of Full Operating Capability (FOC) planned in FY18. Increments for the IC ITE will include all activities required to plan for and implement IC ITE services, including scaling services across the IC enterprise, transitioning relevant legacy data and applications, and retiring legacy capabilities as appropriate. The initial IC ITE services focus on delivery of a common IC

desktop, common back office tools, broader and standardized access to analytic tools and applications, and data-centric computing using complementary government-developed and commercial cloud architectures. Development of Increment 1 began in 2012 and ultimately intends to deliver enterprise capabilities for the IC Cloud Environment, the IC Desktop Environment, and the IC Applications Mall services. Future increments propose to deliver additional ITE services and capabilities based on mission needs, and will further define/refine governance, cost recovery business models, and additional efficiency opportunities. In five years, the IC expects all agencies to be leveraging this shared services platform with each providing or paying for enterprise services. This baseline platform and new Community IT ecosystem is expected to enable and encourage innovation to occur and to spread rapidly.

Cost reductions in an increasingly austere budget have become a factor in forcing the IC to break down siloes and find ways to create savings based on economies of scale. In the future, it is unlikely IC members will be able to afford customized components designed specifically for one agency. There appears to be a growing consensus that although there may be some near-term degradation, common components and business processes are not only inevitable in a challenging budget environment, but the right thing to do to better integrate the IC. The IC will improve on consolidating appropriate business processes and supporting technologies to maximize benefits of an integrated environment. For example, agencies have run out of data storage space and are facing an avalanche of new data sources requiring storage and processing – hence the requirement for a more agile, shared cloud architecture used by the entire IC. Common implementations across the IC should drive efficiencies and best practices, allowing redirection of scarce resources (through those efficiencies) to focus on harder problems not currently addressed. Any initial cost savings may be reapplied to implement the IC ITE without additional investment dollars. Over time, any savings can be re-directed to core IC mission requirements.

The IC will lean heavily on industry to conduct R&D on enterprise solutions - COTs technology will likely predominate. Acquisition will be deliberate to provide some stability in enabling organized change. Outsourcing may be considered as long as vendors can meet service needs on a sustainable basis without sacrificing mission agility. Vendors depending on revenue streams from cost-prohibitive long-term license fees will likely find themselves disadvantaged as the IC ITE moves forward. Integrators who specialize in specific agencies may also be disadvantaged when the IC is seeking enterprise-wide solutions.

In addition to budget savings, the greatest impact is intended to be on the analyst. A common architecture will allow analysts to more easily query for data anywhere in the IC based on authorities and need-to-know. A key enabler will be improving reciprocity and the portability of clearances, to ensure we can fully utilize technology to improve intelligence analytics. It will allow a broader and deeper analysis of all data collected and processed by the IC than that currently available. Analytical transparency to critical data will be a major objective for the IC, allowing a seamless collaborative environment for the analyst and distributed analytics for automated contextual integration of data driven by the analyst's requirements. The IC ITE should be a key enabler for more effective multi-int analysis and ultimately for more distributed and shared multi-int intelligence.

Secure and appropriate access to people, data, and capabilities are paramount. The proposed foundation of the IC ITE is based on shared standards that include data tagging, access/identity management, and fungible data. This will require new models for analytical discovery with four states for an analyst to gain access to any data object: full access to the data object; no access to the data, but permission to see metadata; no ability to know the data object exists; and security alerting when an access attempt is made.

A basic assumption for the IC ITE is that the existing IC network security model is insufficient and is increasingly vulnerable in the face of aggressive and adaptable adversaries. It is inflexible in that the current model does not allow “discovery” boundaries to morph according to varying mission contexts. For example, the boundary for an analyst supporting a Special Forces mission in Afghanistan should be different for certain types of data than for an analyst supporting maritime awareness in the Pacific. The current model also limits our ability to leverage new IT platforms and frameworks such as the cloud or use of mobile devices. This new environment will require a shift in the security model from a Maginot-Line philosophy to a data-centric model. A defense-in-depth strategy is required, more focused on protecting critical data than the data repository.

The CIO respondents, while all extolling the benefits of the IC ITE, recognize that the greatest difficulties lie ahead as they get into the final details of the initiative. Most recognize that cultural predispositions of individual agencies, sometimes decades in the making, must be mitigated either through technology or budgetary persuasion. Progressing with IC ITE requires an honest understanding of the reality of legacy systems and how to move them toward a new architecture without breaking the bank or crippling operations. Most surveyed believed that technology would allow change to occur without significantly impacting mission or, as one CIO stated, “...building the airplane while flying.”

Strong IC Leadership Support and Consensus for the Effort – The Time is Now

Transformational change to an IT Shared Services model requires invested leadership.² The revolutionary shift that the IC is attempting can only occur with the commitment of the mission, CIO, CFO, HR, and policy leadership from the ODNI and each IC agency. This commitment is predicated on fully supporting a common vision and execution plan. Operational managers across the IC are also fully vested in the concept and are aware of the potential efficiencies and increased effectiveness from IC ITE, as well as potential disruptions in operations or mission degradation as consolidation proceeds. All IC CIOs felt that the time is right, with budget realities, current state of technologies, and a sense of urgency in the IC leadership all combining to create an optimal climate for positive change.

The IC CIO expects that ODNI and agency leaders will continue to provide full support for the extensive transition required of enterprise, business and mission systems, and cultures in order to implement the IT Enterprise as planned. Furthermore, change management must be driven from the top. The IC element heads have to actively drive the cultural, organizational, and policy changes required to implement the ITE. IC elements will be required to develop migration plans for transition of current operations and data to the IT Enterprise environment. A mutually agreed

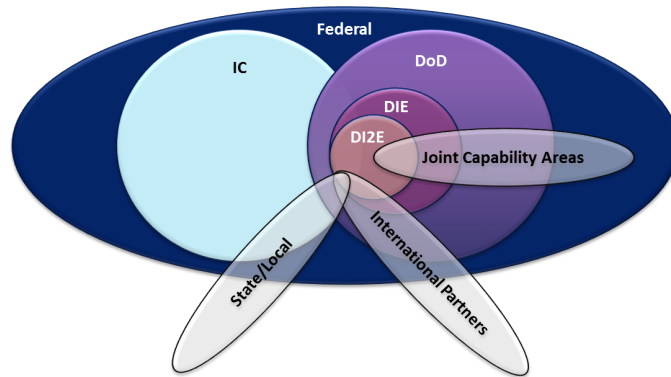
upon governance structure should enable the IC CIO to oversee Agency and capability integration into the ITE. Due to the complexity, scope, and aggressive timelines involved, the IC CIO intends to exercise an agile implementation approach, managing in three-month windows toward agreed-upon annual capability roadmaps and the five-year target architecture.

For this approach to work, the IC CIO believes that decision-making and governance of the IT shared services needs to be centralized rather than divided among the intelligence agencies. However, execution of those services (implementation and operations) will be largely decentralized. Faced with both challenging budgets and traditionally independent organizations, clear, committed, forceful leadership is an imperative to move forward. Having “apostles” at senior levels who support the effort for the IC IT enterprise increases the possibility of success.

DOD Shared Vision

In the computing and telecommunications arena, architectures and capabilities are related and connected which often means that key technical and mission decisions should not be made in a vacuum. Concurrent with the IC ITE, DoD is implementing the Joint Information Environment (JIE) framework, which is a secure joint information environment based on shared IT infrastructure, enterprise services, and a single security architecture. The goals of both JIE and IC ITE are ultimately the same - improved mission effectiveness and increased security while realizing IT efficiencies. While very similar to the IC ITE, JIE is DoD-centric, more decentralized, and addresses sensitive but unclassified and Secret-level networks. Ongoing JIE efforts using enforceable standards, specifications, and common tactics, techniques and procedures is a different way of working toward similar goals. The JIE is not a program of record, but is funded by DoD participants who join the environment out of desire for increased IT efficiencies. It is neither an enterprise (requiring common mission and leadership) nor an architecture (requiring tight management of implementation).

With over 70 percent of the IC under the departmental jurisdiction of DoD, IC ITE must—at a minimum—be directionally synchronized with the JIE. Ideally, DoD and IC will work together to de-conflict opposing perspectives on the path forward. DoD and the IC are both very large and complex organizations. Establishment of shared IT architectures within either organization is a Herculean task, requiring a huge investment of human capital. To date, implementation of their respective IT and telecommunications visions has consumed significant personnel and financial resources. This has limited the ability of both to coordinate their respective efforts to ensure complementary, mutually supportive efforts. However, there is a high degree of senior-level visibility which allows for the right interaction as necessary with an eye to ensuring the two communities are not diverging. To be mutually successful, efforts must be supported to improve existing intersecting governance—where multiple parties with vastly different missions, functions, and challenges must be aligned on critical issues.



Must Operate Across A Broad Spectrum: White House to the Foxhole	
TS Networks Dominate	SECRET, REL, UNCLAS & Open Networks Dominate
Fixed Facilities	Mix of Fixed, Temporary and Mobile Platforms
Stable MissionSet	Dynamic Mission Sets
Stable Communities of Interest	Dynamic Coalitions
Enduring Problem Sets	Mission-based Intelligence Problems
High Bandwidth/Reliable Comms	Mix of Comms (Reliable/Bandwidth Constrained) capabilities
Single Functional Agencies (i.e. HUMINT, SIGINT, GEOINT)	Multi-Functional Military Services, COCOMs & CSA'

Figure 2 IC and DoD: Unique Environments

Challenges and Opportunities

Defining Common IT

Establishing the Community definition of Common IT is moving ahead quickly with IOC of the first increment achieved March 2013. To move beyond the initial deployment, the IC — in concert with DoD — still has a long, complex journey ahead. Current Community IT standards are still in place for interagency exchange of information, not information sharing. Security standards still focus on the infrastructure—not the data layer—to prevent intrusion and attack. Governance continues to be cumbersome and cannot react with the agility needed to enable decisions and significantly move the plan forward when months count—and the ability to pilot and establish quick wins, fast effective changes, and if necessary, regroup from small failures, is key in light of the pace of these changes.

Moving from a customer-centric perspective, the IC’s IT leadership must come to consensus on the common IT service catalog, negotiate service level agreements with their customers, and fundamentally shift governance to a structure and supporting processes that enable IC ITE.

IT Shared Service Model

Current IT standards, architectures, and approaches do not scale in the face of the austere budget. “One of the common complaints we hear from the field, from theaters involved in operations, is that all these people bring all their own networks and architectures with them”, said Neill Tipton, Director of Information Sharing for the Undersecretary of Defense for Intelligence. “You sit at a headquarters and you’ve got NSA guys on their NSA net, the NGA guys on the NGA net, the CIA’s on its own network. They’re all doing the same mission, supporting the same commander and working at the same objectives. But their idea of sharing data is sending emails to each other across their different networks. When we can roll into a theater of operations and bring in a single network to provide intel support to that theater that will be success”.³

What is an IT shared service model?

Ask the question in the public sector and opinions vary. Some organizations define *true* shared services as the consolidation of IT functions from several departments or agencies into a single, stand-alone organizational entity whose only mission is to provide services as efficiently and effectively as possible.

Shared services frees up scarce resources to allow departments and agencies to focus on core business and customer needs while providing organizational flexibility to have IT structures independent of front-line activities and structures.

In a shared services model, the only function of the IT shared services organization is to run IT functions as effectively and efficiently as possible. IT shared services elevate the importance of administrative functions to the highest management levels.

The current mission objectives of both the IC and Defense Intelligence of timely processing, cross cueing, sharing, high end analytics and all-source knowledge delivery are unlikely to be met without employing an IT Shared Service model that allows the Community to “commonly do what is commonly done.” For example, Instant Messaging is used across the IC, but each agency does it using different tools, creating islands where sharing of valuable data or insights is the intent, but not always the reality. Even when the same basic tool is used, infrastructure differences (e.g., authentication, unconnected servers) prevent collaborative analysis and sharing across organizational boundaries. The IC will need to decide what the common IT services are, the architectures used to define and deploy the common IT services, and the cost model used to fund the common IT services.

Leveraging lessons learned from the Department of Defense Intelligence Information System (DoDIIS) model where DIA enables desktops for Combatant Commander Intelligence (J2) personnel worldwide, the IC may be able to move forward with the “quick wins” in its IT service transformation effort. Based on a common understanding of what is included and what is not, foundational decisions about an effective and affordable funding model can be better informed.

Setting standards could also help mitigate the proliferation of “shadow” IT organizations and trust-breaking situations where a virtual architecture is blamed for poor performance of applications that have not been optimized for the environment. If early successes can be achieved, with associated savings, confidence should improve, providing a departure point from which to create solutions for other IT service transformations. Community CTO, CIO, CFO, and acquisition leaders would then need to work in concert to determine what other common IT services are possible and should be pursued.

Since the IC has never implemented enterprise IT capabilities on this scale before, it makes sense to examine, tailor, and integrate some industry best practices. CIOs and leadership teams in the private sector use a shared services decision matrix similar to the one shown in figure 3. Even with additional security concerns, a similar matrix—supplemented with objective assessment criteria—could be used to explore next steps for the IC.

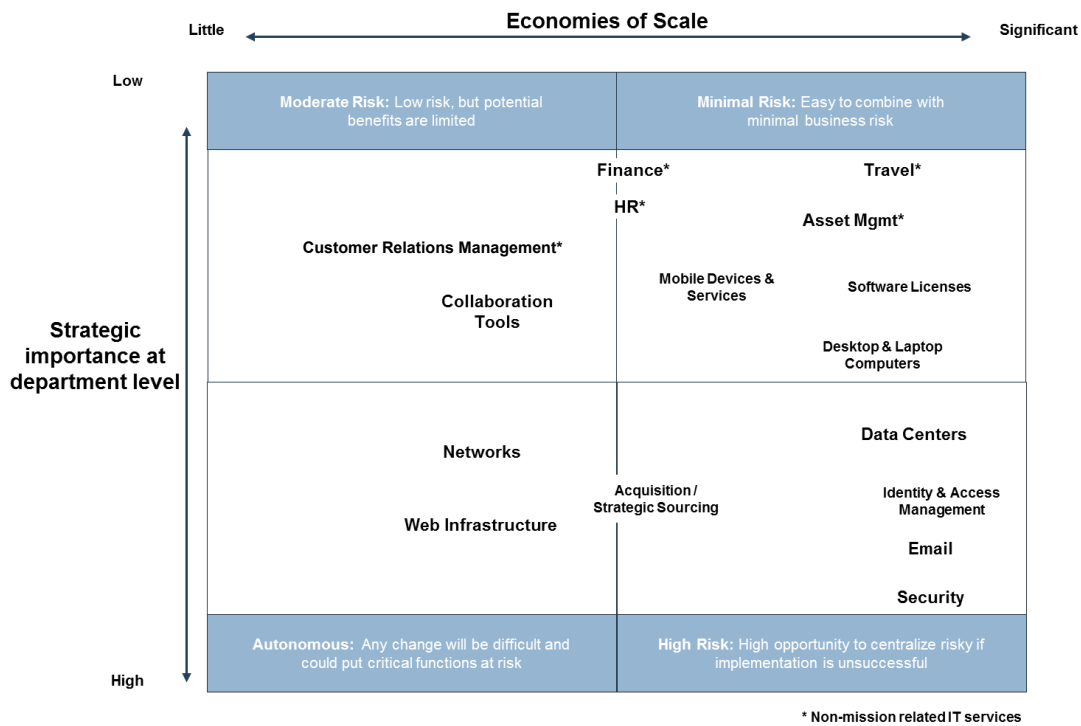


Figure 3. Example – Commercial Shared Services Decision Matrix

Decision criteria for leaders to use with regard to which IT Shared Services should be considered by the IC include:

- ✓ **Cost:** *Are the costs to maintain current or legacy systems high compared to benchmarks?*
- ✓ **Type of Process:** *Is the process highly transactional and does it follow standards across agencies?*

- ✓ **Standardization:** *Is there potential for additional standardization?*
- ✓ **Transaction Volume:** *Are the volumes of transactions high and warrant investment in automation?*
- ✓ **Complexity of Task:** *Are the tasks relatively simple and repetitive?*

Ideal IT functions for shared services should have low strategic impact on the organizations involved while achieving significant economies of scale. Under a shared services model, strategic IT functions, such as determining the types of next generation computers or decisions on changes to software applications, typically remain within agencies while transactional IT functions, like ordering, installing and maintaining hardware and software already in use, are migrated to Shared Service Centers. Tactical or operational functions are usually up for negotiation depending on the missions involved, identified executive agencies, and the uniqueness of particular applications that are needed to accomplish various missions. Mission critical IT should only be considered for a shared services implementation once an industrialized process and a solid foundation of success have been proven to mitigate risks. For example, it would be advisable to field test the deployment of desktop services in non-mission critical parts of the user organizations prior to attempting roll-outs to watch centers and other parts of the organization directly supporting ongoing operations.

Common IT Service Level Agreements

To realize the vision and work within the fiscal constraints for IC ITE, new architectures employing new IT standards should be used at an enterprise level. It would be beneficial if the types of IT standards for both common and unique services are similar; however, the actual IT standard for each group of IT services might differ. Ultimately, all members of the IC will need to agree on IT standards for common IT services—this includes agreement on standard levels of service to enable the Community at large to operate in this environment. As the Community continues to define what is common IT and creates their catalogue of services, IC ITE leaders will have to engage their stakeholders regarding the needed levels of service in order to help define baseline standards for these common IT services.

Obviously, establishment of acceptable Service Level Agreements (SLAs) will require that IC ITE leaders from across the Community work together closely and cooperatively. "Very specifically, we each jointly chair a standards committee that determines the standards we're going to use for data sharing, access control, identity and access management, all the points of intersection that are important for interoperability to be able to make sure our systems can read data across the divides, those are the real working-level details that are being worked jointly," according to IC CIO Al Tarasiuk. "It's the stuff that will endure after we're all long gone."⁴

Enterprise SLAs will set clear expectations for both providers and users. Service providers will have to be able to demonstrate their ability to meet the terms of these agreements. Building the confidence and trust to continue the transformation to shared services will only exist if IT providers can deliver on the promised services. Whether a fee-for-service or working capital model is chosen to fund shared services, consumers across the Community will likely be watching carefully to assure themselves that resources are being used prudently to meet broad customer needs.

To make selection easier and to speed service deployment, the IC is likely to standardize service definitions for IT shared services, especially cloud shared services. This approach provides three benefits: improved capacity planning, particularly if standard components are used; quicker service provisioning; and better buying forecasts which help to lower costs. Industry experience suggests that proactive service definition gives both customers and the service providers a common frame of reference to measure and monitor IT service performance. These definitions can help minimize service introduction delays or complaints due to issues because applications are not optimized for execution in a virtualized environment. A single entry point to request service, as well as managing trouble calls, enables enterprise level management of the service and, if done well, builds trust with the user community through consistency of service.

Culture

Moving to a shared architecture and IT shared services model will require significant cultural change in the IC, driven by the overarching need to share mission-related data.

By the very nature of organizations, culture pushes back on change and can get in the way of progress. Technology enablers can create platforms to enable and help facilitate the desired cultural changes on the mission side, while also fomenting complementary cultural changes in the IT organizations and workforces. As more clarity is achieved about the implementation details for IC ITE, greater differences between groups within the Community and apprehension about “how does this affect me” at the individual level will occur. Leaders in both the government and industry will need to engage in ongoing conversations with their employees to create a stronger collaborative culture among the IC members.

“Ultimately, your primary job as a leader is to nurture the culture your organization needs to have to get the job done.”

Amy Edmondson - Harvard Business School, 2009

Leaders across the board will have to constantly inform and reassure the workforce and other stakeholders about how the effort will enhance their ability to achieve the mission—and continually communicate the benefits and successes. As cultural barriers start to fall, standardization as part of shared services may raise concerns that individual initiative and creativity may be stifled. Balancing this dichotomy and creating a culture that understands and demonstrates these competing concepts where appropriate—a culture where people think and behave differently will require strong visionary leaders and, as one CIO believes, the shift will depend on the younger workforce to sustain the momentum for these changes. Effective communications with employees and making them part of creating the solutions should help enable progress.

Governance

Current IT governance models within the IC center around needing to control something that is limited and expensive rather than finding ways to take advantage of options that are less expensive and available. This model may block the implementation and proliferation of the newest and most effective technologies. One member of the IC stated, “There is a need for a new governance model which is more detailed and mature than what the IC currently has, in order to more effectively address different mission sets, priorities, and requirements being served by the enterprise.” Some of the governance questions that likely need to be addressed include:

- What are governance authorities, framework, and outreach?
- What issues can an agency “opt out” of?
- Where and how do customer requirements come into the cycle?
- How will commercial technologies and approaches be fairly and fully leveraged by all?

In addition to answering these questions, a senior IC official suggested that the Community needs to be more transparent so it—along with its industry partners—can plan and act efficiently. Governance will help get stakeholders to understand the accelerated pace of planning and execution. The new IT shared services model will require industry to work together to provide solutions in a teaming environment—among themselves and with the government. This means everyone will need to play by the same rules.

Consistent leadership and vision are going to be necessary for the IC to be successful in establishing an environment that results in timely, seamless, and secure information sharing between agencies, customers and individuals. Once shared services are in place, the governance for the delivery of the services must be migrated from the overall model to one owned by the provider and focused on the execution of its responsibilities. Experience elsewhere shows that an IT shared services model will require a robust governance approach focused not only on individual IC agencies, but also that incorporates the viewpoints and guidance of its stakeholders. Service delivery is paramount to the success of IT Shared Services and understanding customer requirements and monitoring the organization’s ability to meet those requirements is critical. This also enables an enterprise business model that drives strategic and operational investments and continuous improvement of the shared services.

Agency and capability integration into the ITE will be under the auspices of the IC CIO’s governance structure. This structure serves as the process and forum for raising and resolving ITE-related issues. Once the IC CIO Council recommendations have been vetted within ODNI (CFO, CTO, and Acquisition Seniors), then decisions can be sought from the DNI and his Deputies Committee and Executive Committee (DEXCOM/EXCOM), the IC’s senior authorities for decision-making, resourcing, and implementation.

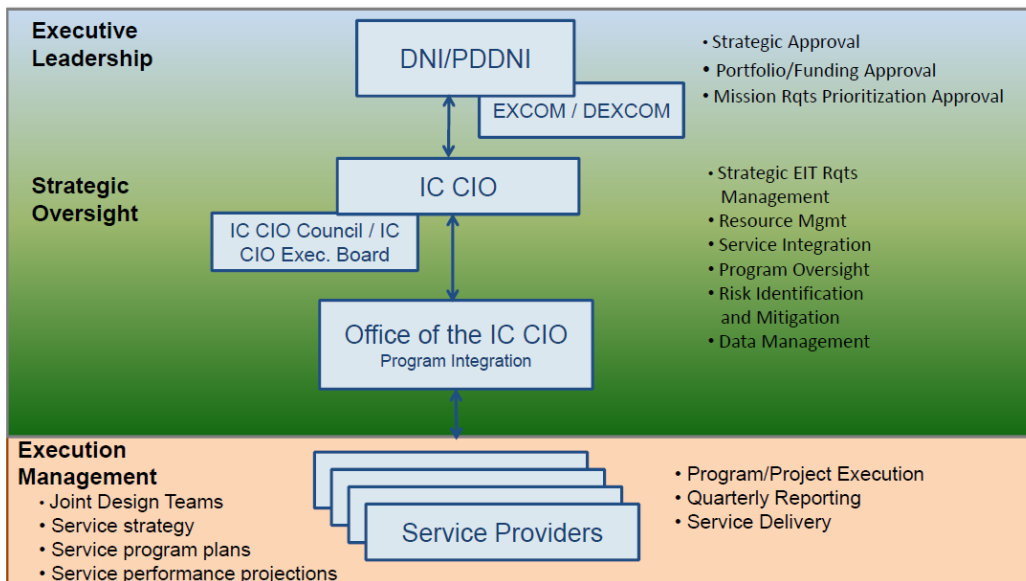


Figure 4 IC CIO Governance Structure

Security & Mission Assurance

What has historically kept the IC secure and reluctant to rethink the security of its IT systems may now be what exposes them to vulnerabilities. The Community must develop new security standards and move from system-level protection to protecting data as individual elements. Outdated controls used to secure data will not be adequate once data is more accessible across the Community. As the Community takes a fresh look at its architecture, the architecture insights can provide an opportunity to build in security from the outset based on best practices, a modern understanding of the threat, and sensible, proven risk management concepts.

The IC CIOs are well aware that the Community needs to determine how to deploy data security to minimize the two unrecoverable errors in IC IT: 1) Loss of data, which once leaked can never be “unleaked” and 2) loss of data that results in loss of life. These mission assurance imperatives call for data centric security for both mission and business data. “Fine-grained, attribute-based access control is critical to enable sharing of information in the face of the kind of cyber-attacks that we are now experiencing. I think it is the only way to fundamentally know who you're sharing with. You have to associate the attributes of a system or a person with the attributes of data. I think at the end of the day, it will give our data stewards across the enterprise a better sense of where their information is going and that it's under control. Today, many data stewards release information without really knowing who's seeing it or what they're doing with it.”⁴

The IC will have to determine how to describe data at the source combined with an enterprise identity management system to enable proper protection and dissemination. The intelligence agencies will have to work in parallel with the Defense Intelligence Information Environment (DI2E) to enable the sharing of not only information, but in the future, services and applications.³ It is important for the IC to establish a common model for enterprise security in a distributed, heterogeneous environment – including operations with mission-specific foreign partners.

Managers understand that the current Intelligence IT workforce can help the community determine what technologies will best handle the new data sharing demands. This means IT personnel will need to move off of the transactional work they currently conduct to more meaningful and difficult tasks within the IC. Technologies already exist to enable data sharing and analytics in a secure way. According to one senior IC official, the Community can leverage the excellent work already being done by individual agencies to deliver these capabilities.

Workforce Skills

The government spends a huge portion of its IT budget on infrastructure operations and maintenance (O&M). But new paradigms, such as cloud architectures, should diminish the associated O&M costs while shifting the costs to “higher end” challenges. The current IT workforce should be capable of implementing and supporting the early transition to a shared services solution for IT. However, a reinvestment of a portion of the savings will likely be needed to develop new skills as the implementation evolves. There will probably be less emphasis on system administrators and narrowly focused subject matter experts. To execute the plan for IC ITE, there will need to be more focus on a government IT workforce comprised of generalists who have a greater blend of skills to manage the increasingly complex systems and an agile contractor workforce that has the expertise to fully implement the program.

The skills needed to operate in the evolving cyber world are different than before and will continue to change rapidly. Concerted actions to close the skill gap will require the government, industry (which can comprise over 60 percent of the IT workforce), and academia to work together to develop innovative solutions in much the same way the workforce is being asked to rise to the technology implementation challenges. There is a significant demand—and minimal supply—for data scientists, software and system architects, and IT assurance and operational experts. There will also likely be a growing need for more experts in the areas focused on data – data management, data analytics and data security.

The Role of Industry and Academia

Successful implementation of the IC ITE will depend on cultural, procedural and organizational shifts not only in government, but also in industry and academia. Without defense and commercial industry, as well as academia, the objectives of IC ITE and the building of an integrated, collaborative community will be difficult to achieve. Fundamental changes to sales approaches, business models, and staffing and education will be required.

Both industry and academia have a long history of partnership with the IC and are paying close attention to the impending changes associated with the IC IT Enterprise. History and logic suggest they want to effectively support the effort, while trying to anticipate how the changes impact their current and future work, focus and deliverables. Their roles will need to be clarified as the IC IT effort progresses. The IC CIOs, for their part, are actively involved in outreach efforts with industry and academia to ensure they are cognizant of the “way forward,” to include multiple interactive forums such as IC/Industry Day partnership meetings and publications such as this INSA paper. As suggested earlier, consistent communications and leadership will be critical.

The IC CIOs universally acknowledged that industry/academia will need to change their business/sales models presently supporting the IC IT communities. Traditionally, a company imbedded themselves in an IC element for numerous years while providing a holistic approach to all IT support. However, they often had difficulty working across agency boundaries. Under this new IT vision, the IC is moving away from the previous model of a major acquisition, large-scale integration model for IT services. The new model emphasizes flexibility, teaming with other industrial partners, and working together to provide enterprise IT solutions to the entire community. A single company providing a single solution to a single agency is probably not a viable concept moving forward. To compete and contribute in this environment, industry/academia will have to start thinking in terms of an enterprise approach that includes evolving business models and partnerships in this new open-eco-system.

Industry and academia, working with the government via new Private-Public Partnership vehicles and approaches, must continue to explore new educational and training methods to close the growing skills gaps. An interviewee commented, “The shift will require worker retraining and may cause displacement. Vendors will need to change hiring and execution strategies.” The future will entail a shift from system administrators to the need to hire more engineers, mathematicians, and experts in security, data management, and data protection. Defining these professions and associated training and education standards will also require a close collaboration between government, industry, and academia.

Last, but not least, the IC CIOs agree that industry and academia will play critical roles in providing innovative technologies, solutions and approaches to enable IC ITE implementation. Key challenges include the need for real-time situational/infrastructure awareness, secure mobility, agility, and the ability to access appropriate data and applications from wherever personnel are located around the globe. Operationally, effective trouble-ticketing and crisis response will be paramount. Sustainable acquisition models will be required to ensure that operational capabilities are available to the enterprise users, while also reaping the expected IT efficiencies of this strategy.

As the government looks at new ways of doing business to reflect the buying power at the IC enterprise level rather than individual agencies, and refocuses from monolithic, stand-alone systems to a network of capabilities that provide data across the Community, it should become increasingly apparent to industry that it is time to change their approach to doing business in this market. If IT services and solutions will be managed as an enterprise—with an expected reduction in 20-25 percent of the overhead—and the ability to fund efforts across the current organizational boundaries becomes the norm, existing vendor approaches to selling and contracting in this business space will fundamentally change, impacting everything from licensing agreements to account management and revenue models.

Concluding Thoughts

The DNI clearly believes that the vision and plan for IC ITE is foundational to the enablement of efficient data gathering, processing, analytics, and sharing. The overall strategy for IC ITE proposes to leverage new approaches to technology and community management which will continue to

break down organizational and mission barriers, and produce resource savings that can be reinvested in increasingly complex IC missions and global challenges. While not the entire solution, the use of common cutting-edge IT will help the IC shift toward an online collaborative environment built on shared trust and a shared purpose. In other words, successful implementation of the IC ITE is the foundation of meaningful intelligence integration and critical in achieving the overall efficiencies required to accomplish the demanding national intelligence mission in an increasingly challenging resource environment.

Getting to full operational capacity will be a long journey, and the optimism that the IC CIOs reflected in their interviews for this report will likely encounter significant challenges and setbacks along the way. Implementation is clearly in the early stages. Realizing the full value of shared services is years away. But, as Al Tarasiuk stated, "We have no choice but to move in this direction. The budget situation was the impetus that put us over the top to move in this direction. This has been tried before, but the culture has already resisted and the budget has been growing for many years. But the reality now is that none of our agencies is going to have enough money to deal with the kind of requirements we have, especially when you look at big data, mass analytics and things like that. No agency will be able to handle the volumes and the intensity of the data that's coming in. The only way we can do this and be effective is to do this together..."

This paper only begins to address the many challenges and opportunities related to IC ITE implementation. IC officials appear to recognize that reshaping outdated governance models, establishing an IC enterprise of common IT services, including a catalog of services and service level agreements, and seeking out and implementing new security strategies for the data layer are among the pressing challenges that must be confronted. These are further complicated by the accelerating pace of IT innovation in the private sector, which quickly outpaces Federal acquisition models and cycles and often leaves the IC implementing "yesterday's technology today."

That said, the fact that the IC seems to be collectively willing to take this risk is reason for optimism. Follow-on papers will explore these challenges in more depth and look into how industry and academia have addressed them in their own enterprises, and how the lessons they have learned might be applied.

Sources

1. Intelligence Community Information Technology Enterprise Strategy 2012 – 2017. Available at <http://www.dni.gov/files/documents/IC ITE Strategy.pdf>
2. *Accenture*. "Driving High Performance in Government: Maximizing the Value of Public-Sector Shared Services," 2005
3. Serbu, Jared. *FederalNewsRadio.com*. "Intel CIOs finding common ground in shared services" October 21, 2011. Downloaded: 12/6/2012
4. Serbu, Jared. *FederalNewsRadio.com*. "DoD, Intelligence Community Tune In, Turn Off IT System" October 11, 2012. Downloaded: 12/7/2012
5. Interviews with IC and DoD Seniors – Lonnie Anderson, David Bottom, Dave Devries, Gus Hunt, Dawn Meyerriecks, Grant Schneider, Jill Singer, Al Tarasiuk