



IC ITE: INDUSTRY PERSPECTIVES

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY ENTERPRISE TASK FORCE

SEPTEMBER 2014



ACKNOWLEDGEMENTS

INSA CHAIRMAN

Ambassador John Negroponte

INSA SENIOR INTELLIGENCE ADVISOR

The Honorable Charlie Allen

INSA SENIOR NATIONAL SECURITY ADVISOR

Ambassador Bob Joseph

INSA STAFF

Ambassador Joe DeTrani, *President*

Chuck Alsup, *Vice President for Policy*

Maureen McGovern, *Senior Fellow*

Ryan Pretzer, *Manager of Policy & Public Relations*

English Edwards, *Communications & Marketing Coordinator*

Daniel Allen, *Fellow*

Rick Dembinski, *Intern*

Kate Swofford, *Intern*

INSA CYBER COUNCIL LEADERSHIP

Terry Roberts, *TASC, INSA Cyber Council Co-Chair*

Ned Deets, *Carnegie Mellon University, Software Engineering Institute, INSA Cyber Council Co-Chair*

INSA IC ITE TASK FORCE CO-CHAIRS

Paige Atkins, *Virginia Tech Applied Research Corporation*

Nuhad Karaki, *Inceptre Corporation*

John Russack, *Northrop Grumman*

EDITORIAL REVIEW

Joe Mazzafrò, *Computer Sciences Corporation*

COPY EDITOR

Beth Finan

INSA IC ITE WRITING TEAM

Peggy Evans, *Evans Strategic Consulting (Lead)*

Nick Buck, *Buck Consulting Group*

Justin Christian, *Mercury Intelligence Systems*

Howard Clifford, *Hewlett-Packard Company*

Darius Farkondepay, *Sollertis Incorporated*

Larry A. Hultberg, *Accenture Federal Services*

Leigh Thompson, *TASC*

INSA IC ITE TASK FORCE PANEL PARTICIPANTS

Christopher L. Alligood, *PricewaterhouseCoopers*

Matt Carroll, *CSC*

Chris Codella, *IBM*

David DeVries, *Office of DoD CIO*

Brett Dody, *The SI Organization*

Ron Foudray, *Northrop Grumman*

Bernie Guerry, *General Dynamics*

Gus Hunt, *Operating Partner, LLR Partners; former CTO, CIA*

Jack Lautenschlager, *ManTech*

Keith Littlefield, *TASC*

Joseph W. Mahaffee, *Booz Allen Hamilton*

Kathy Pherson, *Pherson Associates*

David Porcaro, *CACI*

Alfred Rivera, *DISA*

Lewis Shepherd, *Microsoft Institute*

Jill Singer, *Deep Water Point, LLC*

Eric Warden, *Accenture Federal Services*

Michele Weslander Quaid, *Google*

Douglas Wreath, *AT&T*

IC ITE: INDUSTRY PERSPECTIVES

The Intelligence and National Security Alliance's (INSA) Cyber Council formed the Intelligence Community Information Technology Enterprise (IC ITE) Task Force in 2012 to engage Intelligence Community (IC) and Department of Defense (DOD) thought leaders, chief information officers (CIOs), industry executives, and academics on the technical and process challenges and opportunities associated with IC ITE. The goal of the IC ITE Task Force is to promote transparency and encourage a more meaningful and productive public-private dialogue and partnership, in order to ensure the successful implementation of IC ITE in support of all agency and IC entity missions.

The Office of the Director of National Intelligence (ODNI) IC ITE strategy focuses on enabling greater integration, information sharing, and information safeguarding across the IC through a common IT approach that substantially reduces costs. The IC ITE initiative focuses on achieving five strategic goals:

1. Fortify the Foundation
2. Deliver User-Focused Capabilities
3. Enable Efficient Business Operations
4. Establish Effective Governance and Oversight
5. Forge Strategic Partnerships

The first paper in this two-part INSA series on IC ITE, *IC ITE – [Doing In Common What is Commonly Done](#)*, focuses on the vision and perspectives of senior IC leaders and CIOs to help the community at large identify senior-level expectations that are driving changes in information technology (IT). It seeks to inform the defense industrial base (DIB), large and small businesses, and other partners on the direction and challenges of implementing IC ITE.

The purpose of this second white paper is to explore the challenges faced by the IC and to present constructive ideas which can contribute to the successful implementation of a shared services IT model. INSA believes the ideas presented within this white paper can serve as a framework for continued public-private dialogue and cooperation.

Throughout 2013, INSA's IC ITE Task Force held four panel sessions to generate a productive dialogue and identify private technology sector best practices and lessons learned from large-scale technology and integration efforts associated with industry transitions to shared services and cloud-based architectures. The panel discussions centered on four topics that were originally identified by the IC ITE Task Force as key challenges for successful implementation:

- Governance model;
- Business model;
- Security and risk management; and
- Technology and innovation.

As a result of the dialogue during these panel discussions, the Task Force compiled the following observations based on best practices informed by private sector experience and adapted to the IC's environment, missions, assurance imperatives, and business practices. Consistent with several current IC ITE initiatives, the following areas were identified as having the most significant, potential impact on the successful implementation of IC ITE.

1. A transparent and metrics-driven governance process that supports the integration of IC ITE services and incorporates proven program management concepts should enable the timely decision making, effective day-to-day oversight, strong programmatic discipline, and accountability that are essential for success.
2. The development of a maturity model will aid in addressing how to optimally combine shared services across the enterprise with common standards that enable the continuous introduction of innovation enterprise wide.
3. Periodic written updates on progress to the workforce and to the industry partners posted to the DNI website would greatly improve transparency and promote acceptance. An integrated IC leadership-driven change and communication strategy enables communications that are consistent, transparent, coordinated, and user informed across all governance levels and agencies. Such efforts will help ensure that decisions coming down from leadership to implement the strategy incorporate the building of broad and effective awareness regarding the goals, schedule, processes, decisions, and status of IC ITE.
4. A well-prepared, motivated, high-performing workforce is as important as the technology that enables a transformational IT enterprise. Continued development of a workforce strategy to support IC ITE is critical and should include new skill sets needed to accommodate changing acquisition, security, and change management requirements.
5. Moving to a shared services model requires new funding and cost recovery models, a clear acquisition strategy, new procurement and contracting approaches, and new revenue models. Cross-functional teams can be leveraged to assess and recommend business model changes (including acquisition, contracting, and budgeting) to support the IC ITE effort and assist with the creation of new revenue models, such as working capital funds, to ensure sustainable funding.
6. Explicitly defining and publishing what proven and effective government-to-government (G2G) and government-to-industry (G2I) business models will be used in IC ITE is essential. Key areas for consideration include G2G provision of services, G2I contracting and budgeting models, and respective monetization strategies.
7. An architecture which focuses security more on the individual, providing the IC with needed protections while enabling broad access to shared data and applications by utilizing a data-centric security model including data tagging, identity management, and improved continuous monitoring techniques is at the heart of IC ITE.
8. Innovation and reduced barriers to entry are enabled by reducing the underlying complexity of the current IT infrastructure, increasing usage of open standards, leveraging innovation in the commercial sector more often, and establishing additional strategic partnerships while ensuring industry intellectual property (IP) protection.
9. A well-defined, centralized, and periodic method of updating and engaging between the Director of National Intelligence (DNI), Principal Deputy Director of National Intelligence (PDDNI), DNI CIO and the private sector could greatly aid adoption. The benefits of public-private partnerships will substantially enhance the chances of IC ITE's success by enabling the ODNI to receive regular updates, and to solicit and elicit feedback and lessons learned while continually engaging with the private sector to ensure that innovation and the benefits of private sector research and development are being utilized.



The ability of a shared services model to improve information sharing, promote innovation, and safeguard the security of information within the IC is now seen as a compelling objective.

INTRODUCTION

In anticipation of declining budgets, the Intelligence Community (IC) leadership directed implementation of a new, cloud-based, information technology (IT) architecture called IC ITE to incorporate commercially grounded enterprise architectures, approaches, and technologies across the IC with the intended benefits of enhanced efficiency and cost savings, as well as increased agility, security, productivity, and integration.¹

Preliminary evidence from industry suggests that shared services and cloud computing reduce long-term cost growth, but do not provide short-term cost savings.² Indeed, implementation requires redirection of IT resources to permit the early investment necessary to launch. However, the ability of such a model to improve information sharing, promote innovation, and safeguard the security of information within the IC is now seen as a compelling objective which justifies IC ITE as a critical enabler of IC mission success.

METHODOLOGY

In recent years, the private sector has been forced to address many of the same issues involved in IC ITE. The most recent spate of mergers and acquisitions in the U.S. business community has provided extensive opportunities to integrate disparate business cultures, infrastructures, data types, security practices, and workforces. Based on this vast experience, it is reasonable to postulate that there are likely considerable, surmountable challenges ahead in achieving the IC ITE goals. The IC ITE Task Force held four panel discussions in order to explore how industry might best aid the IC and to generate a dialogue that distills private sector best practices and lessons learned from large-scale technology and integration efforts associated with industry transitions to cloud-based architectures and open development. These four panel discussions focused on:

Governance

Governance is the structure through which leadership and management work. It specifies who is responsible for which decisions, processes, and services, and drives communication between service providers and service consumers.

Business Model

A business model describes the rationale of how an organization creates, delivers, and captures value.

Security and Risk Management

Information Assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data, and the systems and processes used for those purposes. IA includes protection of the integrity, availability, authenticity, non-repudiation, and confidentiality of user data while protecting information from unauthorized disclosure.

Technology and Innovation

Innovation involves introducing a new technology, solution, or process that results in some kind of measurable improvement.

These sessions were part of the Task Force's efforts to provide valuable information and insights to government agencies charged with implementing this crucial initiative. Panel members were from government, industry, and academia. Industry participation was enriched by including in the audience companies large and small that shared their experience, expertise, and questions.

INSIGHTS RESULTING FROM PANEL DISCUSSIONS

IC ITE REQUIRES STRONG GOVERNANCE FOR SUCCESS

The Director of National Intelligence (DNI) has focused much of his tenure on effective mission integration and partnership within the IC. IC ITE is the cornerstone to achieving that integration. In order to solidify adoption of information sharing and requisite collaborations, IC components will need to become less single agency-focused and accept more common solutions. The INSA panels concluded that the greatest risk faced by IC ITE, as with any organizational change, is resistant and entrenched cultures across a disaggregated federation of agencies. Industry experience suggests the path to breaking down resistance and changing the culture lies in strong governance. A strong governance model will detail responsibilities, assign them to the correct bodies (coupled with the authorities necessary to perform), allocate resources, provide accountability through benchmarks for measuring progress, and render all these elements transparent to the workforce, industry, and oversight organizations. This transparency will lead to better collaboration in resolving issues and, as a consequence, will build trust and confidence for both providers and end users. The INSA discussions reiterated the importance of accountability, sufficient funding, an integrated change and communications strategy, and guidelines for future workforce requirements.

Transparent and data-driven governance and oversight processes which have been critical to transitioning IT enterprises in the private sector are essential.³ Senior corporate leaders who established program management functions for similar transitions were able to make key decisions quickly, to communicate often and clearly, and to hold all levels of the organization accountable for meeting published timelines, milestones, metrics, and benchmarks on schedule. Resistance to change and cultural inertia were overcome by strong leadership, clear messaging, and strong enforcement. The challenge is one of integration by developing an ecosystem – a fabric that will be able to support future capabilities with agility. To this end, program management becomes the cornerstone to the path forward to define, implement, and sustain a single, standards-based, interoperable enterprise architecture and survivable infrastructure to accomplish mission objectives

66
Resistance to change and cultural inertia in the private sector were overcome by strong leadership, clear messaging and strong enforcement.

and drive efficiencies across the enterprise.⁴ Key to this approach is establishing a maturity model which would provide a structured way to assess progress of the implementation of shared services across the enterprise and address common standards to permit innovation within the enterprise.⁵ The most successful implementations balance standards and rigor with openness and flexibility to accommodate innovations at scale and changing user requirements.

In addition, an integrated change and communication plan that enables communications across all governance levels and agencies regarding IC ITE are constant, transparent, coordinated, and involve input coming up from the user as well as decisions coming down from leadership. Change and communications plans should be designed, executed, and benchmarked at every level and constantly incorporate customer feedback. In order to manage expectations, communications plans should build awareness about the goals, schedule, process, decisions, resources, and status of IC ITE by making these transparent to the workforce and the industry that supports it.

Lastly, to ensure future success, guidelines for the workforce to support this effort must be continually developed. New skill sets to accomplish changing acquisition, security, and change management will need to be acquired. This new workforce requires expertise in areas such as service-level agreements (SLAs), revenue models, fee for management, agile methodologies, shared services models to include Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) implementations, as well as new cybersecurity capabilities. Increased training and incentives, strong emphasis on recruiting, rotating talent with industry, and collaboration with colleges and universities to develop the necessary curriculums all need to be addressed.

These challenges, along with managing current legacy systems while transitioning to IC ITE, speak

to the need for a strong governance agenda. A clear vision for implementation and execution can be instituted by establishing accountability, executing a strong change and communication strategy, and developing a workforce with the appropriate skill sets. Adherence to strong programmatic practices and evolving the governance model at all levels is crucial.

IC ITE NECESSITATES CHANGE TO THE BUSINESS MODEL

The IC is implementing a horizontally-integrated shared services model to support IC ITE. The primary benefits of shared services include reduced barriers to entry, greater innovation, reduced duplication, avoidance of cost growth, improved information sharing, as well as centralization of information assurance (IA) and enterprise management functions. With this approach, the Task Force projects that acquisitions will be grouped into infrastructure layers and application layers. Implementations will move toward IaaS and PaaS. Industry supported this approach during INSA panel discussions but noted that it is also necessary to adopt appropriate contracting and procurement approaches such as changes to the business model, including cost recovery model, contracting and procurement processes, and new monetization strategies.

The government should explicitly define what government-to-government (G2G) and government-to-industry (G2I) business models will be used in IC ITE. Achieving success requires clear and candid discussions with the industrial base regarding the impact IC ITE will have on the way software applications, mission capability and infrastructure will be funded, acquired, and integrated. Decisions regarding what programs companies pursue, how companies prepare for the market, and how finely they tune their offerings will have significant and long-term impact on the industrial base supporting our intelligence and national security communities.

Given this direct correlation, in conjunction with industry partners representing large- and small-business, software, hardware, and support services, the government should define key areas including: G2G provision of services, G2I contracting and budgeting models, and respective monetization strategies.

A different approach to the funding and cost recovery model will be required for shared services. The provision of services among government entities concerns such questions as how individual agencies will pay for functions provided by executive agents and what agency funding execution standards will be applied for cost accrual and recovery, as well as refresh. While historically the IC has not measured IT costs, relying instead on pricing IT infrastructure as a percentage of a system cost or through historical use, the IC ITE business model now should capture those costs. Accurate cost model accounting is essential, as fixed and variable costs must be projected for cost recovery and for appropriate pricing to IC customers under IaaS/PaaS. A working capital fund or other process may be included which will be prepaid or charged back. Consideration should be given to leveraging a cost recovery model such as the process used by the Diplomatic Telecommunications Service Program Office in providing network and communications services for U.S. government departments and agencies operating from U.S. diplomatic posts. Here, funding is split between appropriated funds, the fixed costs of doing business such as program office overhead, and fee-for-service funds, the costs related to the actual services utilized by the consumer.

Shared services will promote new contracting and procurement processes between government and industry. The procurement approaches which will be used include consideration of capacity procurement and provisioning vs. "procure on demand/requirement," integration vs. development, and government make vs. buy; which approach is to be used and in what circumstances is something industry needs to clearly understand. New contracting strategies that support cross-segment integration, and preferred contract structures

based on type of work (specification performance vs. SLA vs. performance-based, and tools such as Broad Area Announcement with no expiration, rather than specific request for proposals [RFPs]) should become more widely used. New software procurement models and approaches should be created that comply with enterprise standards and vary depending on the type, criticality, and time frame of the requirement. When requirements are well defined but schedule is critical, a "spend" component could be utilized. Here the government defines requirements and pays industry to develop software using a government's PaaS. When needs are more open-ended and the schedule is flexible, a "revenue" model could be utilized. In this case, government provides overarching requirements and allows industry to develop on the government PaaS.

In addition, the findings of the INSA panel suggest IC ITE will require new revenue models for industry. Three major trends appear to indicate that the government intends to shift to PaaS in order to create the common agile platform necessary to support scalability and innovation which will enable an integrated user-centric architecture:

- Removing IT infrastructure revenue from industry's application development contracts;
- Moving away from monolithic software applications and toward modular development so that government programs can combine and customize capabilities from smaller, reusable services; and
- Opting for "pay for use" software costing, rather than a per-seat licensing approach.

These trends impact industry's revenue mix, overhead structure, and the way companies capitalize infrastructure. When the government formalizes an acquisition strategy that separates IaaS/PaaS programs from software development programs, industry will need to choose where in the stack they compete and will adapt to the revenue shift accordingly. New monetization strategies will need to be created. For example, a major point of confusion across the IC, by both government and industry partners, is in how applications in an "Apps Store" would be priced. Pricing options for application development in

an Apps Mall (PaaS) procurement environment, including industry revenue and profit models, intellectual property (IP) rights, and licensing strategies need to be addressed. Options include charging by user per year, charging per click of the application, and charging a base charge for the amount of time spent on the application with overages charged at a different rate. Each of these options provides its own uncertainties and in aggregate leaves industry with little ability to project costs or revenue. Industry's critical, recurring question is how businesses can plan – or even remain viable – in such an environment. The issue

of monetization needs to be resolved in order for industry to provide optimal support for IC ITE and contribute to the necessary cost savings.

IC ITE generates many fiscal and procedural challenges to the current business model. Addressing these challenges is an ongoing, long-term activity critical to the success of IC ITE. A sustainable cost recovery model, optimized budget, new contract and procurement processes, and predictable revenue streams are issues that all need to be resolved.

IC ITE REQUIRES A COMMON APPROACH TO SECURITY AND RISK MANAGEMENT

The INSA IC ITE panel sessions clearly articulated that a common approach for information security is essential for the successful adoption of shared services and cloud computing in support of any large enterprise. If individual agencies take an inconsistent approach in the areas of data tagging and identity management, the result will be a continuation of today's stovepipes that are incapable of interoperating with one another. IC ITE policies, procedures, and tools will support portability and consistency of individual accesses across the IC for the majority of data sets in order to provide seamless and secure enterprise solutions for trusted collaboration.⁶ While many information security functions are designed to prohibit certain data sets from being accessed, the ultimate objective is to enable enhanced, relevant intelligence production in real time whenever feasible. This happens through sharing information with authorized individuals and enabling processes for information discovery. As part of the information discovery process, individuals should be permitted different levels of discovery based on their individual attributes and the corresponding information they are attempting to access. This is divided into three basic use cases: (1) the individual can access the information; (2) the individual can discover the existence of the information but is not permitted to access it; or (3) the individual cannot access the information or know of its existence. Several factors including a data-centric security model, identity management procedures, data tagging, and improved automated monitoring techniques enable this common security framework approach.

In support of a defense in depth environment that supports its risk profile, the IC Chief Information Officer (CIO), in close coordination with security directors, is moving toward a security model where access to data is controlled based on the attributes of an individual or a particular system and away from a model that relies primarily on securing the perimeter through various network and database enclaves operating at different classification levels. A data-centric approach provides additional transparency and better overall control of information within a system. It also facilitates information sharing among authorized individuals, thus enabling stronger intelligence collection and analysis. In order to sustain a high degree of IA while still facilitating broad information sharing with authorized users, robust processes for identity management and data tagging along with enhanced auditing techniques to deter insider threats should be designed and employed.

Identity management procedures should use public key infrastructure (PKI) certificates for individuals and systems within the network, with common authentication and authorization services across the IC and all of its networks (i.e., NIPRNET, SIPRNET and JWICS). Emerging biometric capabilities should be considered to supplement PKI, but they must not be static (e.g., fingerprints and retina scans), as they have been proven to have vulnerabilities. The IC should coordinate closely with DOD to ensure that, where possible, approaches for identity management and access controls are designed to be interoperable.

Policies and tools for tagging data at the most granular level, preferably at the individual field level, should be provided. In order to marry the user to the data authorized for his use, data tagging appends additional metadata to information that

describes the classification, rules for sharing, and other identifying features of that information. Data tagging, where the tags correspond to attributes associated with specific individuals through their public key infrastructure certificates, enables fine-grained attribute-based access controls (ABAC). This approach also enables the IC to move beyond network-level or system-level security controls. If data is tagged and consistent authentication and authorization services are in place, access to information can be closely regulated. In addition to regulating information sharing, data tagging also enables data provenance, the process of tracking the lineage and usage of data within a system. Multiple tools are in use in the IC today but an enterprise-wide standard is a key dependency for effective implementation.

Furthermore, recent events have proven that increased emphasis must be placed on countering the insider threat. The IC has an opportunity to embed both enhanced access controls and enhanced auditing of user activity in the IC ITE architecture as it is developed to counter unauthorized access and identify improper user activity. As mobile and wireless access becomes more prevalent, security must become less coupled to the device or the physical location and more linked to the individual. The combination of data-centric security and ABAC will give the IC the flexibility it needs to develop a very rich set of controls based on the individual's role-based privileges combined with attributes about the data itself, such as criticality and provenance. This rich set of controls encompassing both the individual and data will vastly improve the IC's ability to safely share data without locking down the system or limiting innovation.

IC ITE ENABLES INNOVATION

A fertile, open IT environment that supports the development of new concepts and capabilities within the IC is part of the IC ITE vision. Innovation and mission effectiveness will thrive in an IC ITE environment that is simple to use, collaborative, and for which users are equipped with basic tools for information discovery. The INSA panel discussions stressed that in order to support innovation, IC ITE will need to reduce complexity in the underlying IT infrastructure. Technologies and

Automated processes and tools for auditing of user activity should be built in as central to the IC ITE architecture. Improved automation for assessing individual activity and detecting anomalies is critical to security, and should be seen as low hanging fruit for strengthening risk management. Auditability and tracking of data lineage, change history, and usage or data provenance, will enable improvements to data security, counterintelligence, and threat identification. These automated tools can be combined with other sources of information to create risk profiles and support counterintelligence investigations. These are the underpinning of change in policies to improve the overall security and risk management posture of the IC. Continuous monitoring changes the paradigm from a periodic security compliance check of systems, devices and applications, to a continuous view into compliance. This helps to identify risk and reduce vulnerabilities that today can be introduced when patching, security updates, and access controls are not maintained and updated in a timely manner. The National Institute of Standards and Technology (NIST) Risk Management Framework 800-137 is one example of a guideline that offers best practices for continuous monitoring and near real-time risk management.

Data-centric security and enhanced risk management will provide the IC with needed protections while enabling broad access to shared data and applications. By focusing security solutions on granting discovery and access to data to authenticated users, and then continually monitoring activity and compliance, the IC can realize its vision of broad sharing and innovation while appropriately identifying and managing security risk.

processes that enable simplicity and innovation should be cultivated and expanded, and barriers to innovation, such as closed architectures, be removed. Key enablers include the use of open standards to enable software developers, leveraging innovation in the commercial sector, judicious application rationalization, and establishing strategic partnerships while protecting industry IP.

Using open standards such as W3C (World Wide Web Consortium) and OGC (Open Geospatial Consortium), and DoDISS Apps Engine (DAE) within IC ITE to enable software developers should be considered where applicable. Such open standards permit leveraging other components within the IC and building interoperable processes that provide richer user experiences and enhanced intelligence collection and production. In addition to better interoperability, open standards could enable faster and more creative solutions by reducing barriers to entry for smaller, agile companies. It can promote more cost-effective use of capabilities developed for commercial use. Cost savings can also be achieved through economies of scale and the consolidation of various duplicative functions. New technologies can also enable improved IA within the IC.

The IC should seek to leverage commercial technologies to the greatest extent possible. Areas within the IC where innovation is lacking need to be identified and efforts should be focused on filling those gaps. Whenever possible, commercial or open source software products should be leveraged in order to enhance the state-of-the-art technology for the IC mission and to take advantage of the rapid worldwide advance in technology. Seamlessly integrating new commercially-developed technology solutions within IC ITE could provide a significant leap forward for the IC. Instead of falling further behind the technology curve, IC ITE can catapult the IC into the future of innovation, building on the capabilities that exist in the commercial sector and extending those capabilities to meet its needs.

The INSA panel discussions stressed the importance of being judicious regarding application rationalization. Porting legacy tools and processing functions constitutes a serious risk to implementation of the IC ITE architecture. Each instance should be considered from the standpoint of mission criticality, current and future costs, and projected functionality. End-to-end testing to ensure integration and operability is crucial. As big data consumes more and

more computing and storage resources, and advances in hardware and software occur, these legacy elements will become increasingly expensive to maintain and less able to take advantage of leaps in technology. Attempting to port all of today's mission application to IC ITE could exhaust too many resources to be feasible, and eliminating all legacy functions – starting from scratch – could result in mission degradation and decreased productivity.

The government will benefit tremendously from additional strategic partnerships with academia and industry. But when the IC's commercial and academic partners develop capabilities within IC ITE and then collaborate with others operating in this space, the mutually-beneficial business model is elusive. Commercial companies and academic researchers need some assurance that their IP will be protected and not consumed and reused by the government or stolen by a competitor. Furthermore, some have suggested that the DNI, Principal Deputy Director of National Intelligence (PDDNI), and DNI CIO should establish a more well defined, centralized, and periodic method of updating and engaging with the private sector. Public-private partnerships can greatly enhance the chances of IC ITE's success by enabling the DNI to receive regular updates, and to solicit and elicit feedback and lessons learned while continually engaging with the private sector to ensure that innovation, and the benefits of private sector research and development are being utilized.

By using an unclassified venue or requirement statement, the IC can dramatically increase its talent pool and reduce barriers to participation for small companies. While there is some risk associated with this approach, and some capability development will need to be restricted to classified environments, the overall mission benefits of performing software development in an open and unclassified environment will outweigh many of the associated risks.

In summary, the IC can improve innovation and technology insertion by more often using open standards, leveraging and continuously transitioning innovation in the commercial sector, judiciously utilizing legacy or proprietary systems, forming additional strategic partnerships while protecting industry IP, reducing barriers to participation by providing unclassified venues, and broader private-public partnerships.

CONCLUDING THOUGHTS

The IC believes that IC ITE will enable cost avoidance, mission effectiveness, and future technological agility.⁷ While implementation carries many manageable risks, the alternative of staying with primarily agency-centric, stove-piped, legacy IT architectures and capabilities is not a fiscally sustainable option. Technology is not the real challenge to a much needed IC ITE transition. Instead, the current cultural inertia and systemic aversion to risk, coupled with turf and budgetary concerns could prove to be the greatest roadblocks. Despite this, with strong IC leadership, detailed planning, sufficient resources, and increased transparency with public and private sector partners – these and future challenges can likely be overcome with decisive action, effective messaging, consistent enforcement, and accountability.

The findings of the INSA interviews and panel discussions bear repeating here. The following areas were identified as having the most significant potential impact on the successful implementation of IC ITE:

1. A transparent and metrics-driven governance process that supports the integration of IC ITE services and incorporates proven program management concepts should enable the timely decision making, effective day-to-day oversight, strong programmatic discipline, and accountability that are essential for success.
2. The development of a maturity model will aid in addressing how to optimally combine shared services across the enterprise with common standards that enable the continuous introduction of innovation enterprise wide.
3. Periodic written updates on progress to the workforce and to the industry partners posted to the DNI website would greatly improve transparency and promote understanding and acceptance. An integrated IC leadership-driven change and communication strategy enables communications that are consistent, transparent, coordinated, and user informed across all governance levels and agencies. Such efforts will help ensure that decisions coming down from leadership to implement the strategy incorporate the building of broad and effective awareness regarding the goals, schedule, processes, decisions, and status of IC ITE.
4. A well-prepared, motivated, high-performing workforce is as important as the technology that enables a transformational IT enterprise. Continued development of a workforce strategy to support IC ITE is critical and should include new skill sets needed to accommodate changing acquisition, security, and change management requirements.



The IC believes that IC ITE will enable cost avoidance, mission effectiveness, and future technological agility.

5. Moving to a shared services model requires new funding and cost recovery models, a clear acquisition strategy, new procurement and contracting approaches, and new revenue models. Cross-functional teams can be leveraged to assess and recommend business model changes (including acquisition, contracting, and budgeting) to support the IC ITE effort and assist with the creation of new revenue models, such as working capital funds to ensure sustainable funding.
6. Explicitly defining what proven and effective G2G and G2I business models will be used in IC ITE is essential. Key areas for consideration include: G2G provision of services, G2I contracting and budgeting models, and respective monetization strategies.
7. An architecture which focuses security more on the individual, providing the IC with needed protections while enabling broad access to shared data and applications by utilizing a data-centric security model including data tagging, identity management, and improved continuous monitoring techniques is at the heart of IC ITE.
8. Innovation and reduced barriers to entry are enabled by reducing the underlying complexity of the current IT infrastructure, increasing usage of open standards, leveraging innovation in the commercial sector more often, and establishing additional strategic partnerships while ensuring industry IP protection.
9. A well-defined, centralized, and periodic method of updating and engaging between the DNI and PDDNI, DNI CIO and the private sector could greatly aid adoption. The benefits of public-private partnerships will substantially enhance the chances of IC ITE's success by enabling the ODNI to receive regular updates, and to solicit and elicit feedback and lessons learned while continually engaging with the private sector to ensure that innovation and the benefits of private sector research and development are being utilized.

IC ITE offers clear cost, performance, and mission benefits to the IC. Industry has demonstrated its interest, capacity, and readiness to effectively support this transition. Through transparent planning, strong communication, adherence to best practices, reasonable pricing strategies, and updated acquisition practices, the IC can successfully make this transition over the next five years.

ENDNOTES

¹ Operating as an enterprise will enable data to be linked – connections can be made people to people, people to data and data to data..<http://www.dni.gov/files/documents/IC%20ITE%20Fact%20Sheet.pdf>.

² Konkel, Frank. "Daring Deal." 9 July 2014. <http://www.govexec.com/magazine/features/2014/07/daring-deal/88207/>.

³ CIO website, Office of the Director of National Intelligence, (accessed 5 Jan 2014). <http://www.dni.gov/index.php/about/organization/chief-information-officer-what-we-do>.

⁴ Ibid

⁵ A maturity model allows an organization to have its methods and processes assessed according to best practice against a set of clear external benchmarks.

⁶ CIO Website, op. cit.

⁷ CIO website, op. cit.

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.





INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ABOUT THE INSA IC ITE TASK FORCE

The **INSA Intelligence Community Information Technology Enterprise (IC ITE) Task Force** engages Intelligence Community and Department of Defense thought leaders, CIOs, industry executives and academics to explore the challenges and opportunities in the IC IT environment.

The Task Force seeks to provide a framework for understanding the opportunities and challenges of implementing the Intelligence Community Information Technology Enterprise within budget. Its goal is to provide transparency on the process, in order to better enable partnership and ensure the successful implementation of the IC IT Enterprise.

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.



INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

BUILDING A STRONGER INTELLIGENCE COMMUNITY
901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org