ICITE will improve information sharing and data security among intelligence agencies – especially those within the Intelligence Community Big Five. Cloud environments are opening other IC agencies and encryption and data tagging is making for secure information sharing.

With the Big Five offering service-provider support to the IC, the result should be increased efficiency, standardization and governance. Perhaps more importantly aggregate IT spending is expected to decrease by 25% over the next five years.
Contents

1. Introduction 4
2. Desktop Component Plays Major Role for ICITE 4
3. JIE Supports Unified IT Structure for DoD 5
4. Cross Domain Solution Delivers Key Security, Collaboration Capabilities 6
5. Getting ‘Faster, Smarter, Better’ through Protected Information Sharing 7
6. About Raytheon Cyber Products 8
Introduction
The history of cutting-edge innovation in U.S. intelligence goes back to the very beginnings of our nation: Continental Army Gen. George Washington made elaborate use of spy rings, secret methods and raw intelligence analytics. This led to campaigns to deceive the British, contributing greatly to the Yorktown victory and other battlefield successes.\(^1\)

Two centuries later, the Intelligence Community (IC) has set standards for technology deployment, the development of reconnaissance satellites for analysis of foreign missile systems during the Cuban Missile Crisis being just one example.\(^2\) With the dawning of the Digital Age, the IC has proactively pursued advancements in cloud computing, mobile solutions and data analytics, to name a few.

Despite these advancements, the IC cannot be described as ‘interconnected,’ at least not when it comes to IT systems. Instead, networks have operated as separate, siloed functions within the “Big Five” agencies accounting for most of the U.S. intelligence spend.\(^3\) Indeed, former DIA director Lt. Gen. Michael Flynn has described these silos as different “houses that we live in. DIA lives in an all-source house. NGA lives in the geospatial house. NSA lives in the [signals intelligence] house. The CIA lives in the all-source national intelligence house.” The biggest barrier to bringing together the “houses” has been the failure to establish a unified, enterprise-wide IT environment.\(^4\)

Today, however, the IC is addressing this same issue through an all-encompassing consolidation effort: the Intelligence Community Information Technology Enterprise (ICITE) project. As part of this undertaking, IC leadership will implement a shared suite of services and desktop applications called the IC Desktop Environment (DTE).

In this white paper, we summarize the ICITE and IC DTE objectives. We will describe a number of the IT solutions expected to play primary roles in the integration, consolidation and cost reduction. And we will explain how the IC will depend upon these solutions to maximize security assuredness, systems efficiencies, collaborative capabilities and cost savings.

Desktop Component Plays Major Role for ICITE
ICITE will improve information sharing and data security among intelligence agencies – especially those within the Big Five. Cloud environments are opening other IC agencies and encryption and data tagging is making for secure information sharing. With the Big Five offering service-provider support to the IC, the result should be increased efficiency, standardization and governance. Perhaps more importantly aggregate IT spending is expected to decrease by 25% over the next five years.

But beyond bottom line benefits, the IC is seeking greater visibility and awareness by:

- Establishing an architecture that eliminates stove pipes
- Ensuring seamless, secure collaboration on a need-to-know basis
- Aligning state-of-the-art IT with enterprise approaches to enhance mission performance
- Integrating common IT products while maintaining customer satisfaction

IC CIO Al Tarasiuk has cited the killing of Al-Qaeda leader Osama bin Laden as a model example of the collaborative possibilities within ICITE. “It took a lot of intelligence from various sources to pull that together,” Tarasiuk has said. “We’re working in a more integrated way than ever before, thus the need for more integrated systems and applications.”\(^5\)

In May, the project was described as having transitioned “from pilot to planning” after little over a year, involving about 2,500 users who migrated to a unified desktop structure with new applications.\(^6\) Subsequent steps include the migration of top secret/sensitive compartmentalized information from an agency into an ICITE environment; the launch of the CIA/NSA cloud; and the connection of local and wide area networks.\(^7\)

Lt. Gen. Flynn likens the process to the construction of an ideal neighborhood. “ICITE is going to build out the roads, the water pipes, the electricity, the telephone poles, the sewage system,” he has said, “all the things you typically find in a neighborhood that are the common access kinds of capabilities that people

---

2. [http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB54/#cw](http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB54/#cw)
want when they move into a neighborhood … Rather than each buying those applications separately, what we do is say, this fits your portfolio, you invest in that, and we’ll invest in these things. And then we look at how each other are investing, and that’s where the real cost savings are going to be. Before, we were all buying data and paying for data in different parts of the world – and paying for the same data multiple times over. And we can’t afford to do that.”

As indicated, IC DTE is emerging as a major component of ICITE. The Joint Program Management Office (JPMO) is overseeing IC DTE, led by a team with personnel from DIA and NGA.

The IC DTE platform will allow users to remain in their native domain, while still connecting to an IC DTE domain for common services access. The singular IT architecture will enable tighter integration that still enables agency-specific/mission-specific capabilities. IT services will consolidate to a single network available IC-wide, greatly reducing operations and maintenance expenses. In addition, IC DTE will introduce new, collaborative software and a “mobile” desktop that users can log into and access from any IC agency.

IC DTE’s position strategy is to optimize a common desktop ecosystem for inter-agency communications and data sharing. At present, it is not expected to replace existing operating environments, mission-intended applications, data or other IT resources. “A key challenge is striking the balance between leveraging the state-of-the-art IT and enterprise approaches, while sustaining and enhancing mission ability, information sharing, information assurance and satisfaction of unique customer requirements,” (as stated in a white paper by the Intelligence and National Security Alliance).

**JIE Supports Unified IT Structure for DoD**

ICITE/IC DTE is not the only high-profile, consolidation-driven overhaul of government IT systems. For example, the Department of Defense (DoD) is implementing the Joint Information Environment (JIE). JIE will serve as a single, secure information sharing environment for the entire Armed Forces. Warfighters will gain never-before available access to IT networks connected out to the tactical edge, safeguarded through a single security architecture (SSA). Supported by a cloud-based, global identity management system, JIE will collapse boundaries via the SSA limiting overlapping roles. Through JIE’s Joint Regional Security Stack (JRSS) plan, hundreds of network security stacks will be replaced by little more than a dozen, significantly shrinking the attack surface. With the attack surface reduced, the teams will align with standardized controls to preserve network integrity.

Like ICITE/IC DTE, JIE intends to bring about a comprehensive consolidation. It will coalesce countless, individual networks at bases, camps and posts. It will eliminate separate IT infrastructures for separate units. Older, siloed data centers will be replaced by new core data centers with collective standards.

Authorized, military-community members will have “anywhere/anytime” access to the consolidated IT infrastructure, jettisoning duplicated services for the DoD. With a “data centric” approach to the cloud, the focus will be on data tagging, security and portability. As cloud/virtualization information sharing advancements play a lead role, cross domain solutions will allow users to securely obtain information when and where it is needed. Cross domain solutions enable warfighters, analysts and other members of the military community at different clearance levels to securely communicate and exchange data, documents, files, etc. in pursuit of their missions. In conjunction with consolidated infrastructure, the inclusion of cross domain technologies ensures seamless integration, information sharing and data protection, while reducing expenses.

To clarify, JIE will not create a single network for the entire military community. Each individual service will still run its own. But JIE will eliminate redundancies and is projected to save billions in the process.

The simultaneous forward movement of ICITE/IC DTE and JIE represents a sea change within the very culture of the DoD and IC. Both have reached the same conclusions about the urgency for totally secure and consolidated IT systems. This is a critical transition to make given the current era of asymmetrical warfare and increasingly complex global intelligence dynamics of the post 9/11 world. Only a fully integrated IT environment can bring the access, sharing, collaboration, agility and scalability required.

---


Cross Domain Solution Delivers Key Security, Collaboration Capabilities

Leadership has stressed that ICITE should leverage existing technologies as opposed to reinventing the wheel. Many members of the IC have already taken this direction, specifically through deployment of Raytheon’s Trusted Thin Client®. Trusted Thin Client is a Commercial-Off-The-Shelf (COTS) cross domain solution that provides authorized users immediate, secure, and simultaneous access to any number of permitted virtualized networks – regardless of the clearance levels involved – through a single device. From this single device, DoD/IC personnel communicate and collaborate on all allowable networks, maximizing efficiencies while efficiently executing mission strategies. The Trusted Thin Client model allows agencies to connect to internal networks as well as the shared networks within IC DTE and JIE as authorized. The Trusted Thin Client architecture permits administrators the seamless ability to add and remove networks as needed.

Users no longer require multiple machines or a switching mechanism – like a keyboard, video or mouse (KVM) switch – to look at information on one clearance level before switching to another level. Such cumbersome, time-consuming procedures were once necessary. Today, that is no longer the case. Users share vital, task-serving data in a completely secured environment, each classification protected “in its own universe.”

This technology yields considerable cost savings for the DoD and IC. Previously, employees required multiple machines crowded within their work areas, generating excessive hardware, maintenance and energy expenses. Within DoD/IC agencies already using Trusted Thin Client such conditions are a distant memory. Users needing access to domains at different classification levels now get that access on a single device.

Trusted Thin Client is endpoint agnostic, which is another prime objective of ICITE and IC DTE. The focus is on protecting the data through redisplay technologies. With Trusted Thin Client, the nation’s most critical classified data is safeguarded through a trusted operating platform, strict controls and detailed auditing and logging. Data is maintained in the cloud rather than on an internal enterprise disk drive. This makes it impossible for hackers to attack, because no data exists in the traditional types of networks they try to compromise. Yet, for the user, there is no loss of functionality, thanks to seamless redisplay. Experientially, users access files and applications just as if they were using a traditional desktop computer.

The Impact of Trusted Thin Client

Trusted Thin Client is one of a number of cross domain products having impact for ICITE/IC DTE and JIE. In addition to increased security, other outcomes experienced by one agency supporting the Intelligence Community include:

- Value of Trusted Thin Client savings and other net benefits amounted to more than $7.7 million over three years, for overall 54% ROI.
- Computer requirements were streamlined from three machines per user to just one.
- Infrastructure savings came from a reduction in network needs (using one instead of four to six networking connections for each workspace). Including the elimination of some area networks and redundant network access switches.

A Broad Set of Solution Options

In addition, the following products are supporting ICITE to establish a fully secured environment with optimal efficiencies:

High Speed Guard – Provides rapid, flexible and secure transfer of structured and unstructured data.

Trusted Gateway System™ – Introduces a workflow tool to securely transfer files.

Trusted Print Delivery™ – Streamlines printing across domain boundaries while reducing hardware, maintenance and consumables.

WebShield – Allows users to leave data on any given network, for secure search and retrieval regardless of its resident network security level. WebShield users can access data from ICITE networks and other classified networks.
**Trusted Access Mobile** – Takes advantage of virtualization and secure redisplay to protect data at the source, eliminating the storage of data and applications on the mobile device (smartphone or tablet).

**Getting ‘Faster, Smarter, Better’ through Protected Information Sharing**

These developments represent a watershed era for the IC and DoD. With JIE and ICITE/IC DTE, IT operations will change forever. Intelligence officers, analysts, commanders and warfighters are newly empowered. They will access and share files and documents at speeds previously unimagined. They will collaborate when and where they need to, without the onerous logistical barriers. They will make actionable use of information far more rapidly, helping them execute mission decisions in real time. In terms of budgeting, leadership will have greater latitude to invest in impactful technological innovation given that the “new way” will require less hardware, oversight and power.

Perhaps most importantly, none of these innovations come with a cost of compromised information assurance. With Trusted Thin Client and cross domain solutions readily available, IC/DOD will freely obtain and share valuable data that stays “off limits” from our adversaries’ grasp. It will truly serve, as Lt. Gen. Flynn described it, as an ideal “neighborhood,” one in which once-siloed agencies get faster, smarter and better through a common IT systems framework. And, within the neighborhood, cross domain will ensure that each “house” remains protected.

---

**Use of Collaborative Technologies**

- **By 2016**, one-half of large organizations will have internal, collaborative networks to easily share information.

- **62% of workers** regularly need to collaborate with people in different time zones and geographies, such as the information sharing that transpires between a Pentagon analyst and a warfighter overseas.

- **The global cloud collaboration market will reach $5.9 billion by the end of 2018.**

- **Investment in collaboration/information-sharing tools is demonstrated to produce five-year ROI levels of 100%, and payback periods within 21 to 40 months.**

---

For additional information on how virtualization and cross domain technologies enable secure consolidation and efficient information sharing, please refer to these white papers:

- One DoD, One IT Environment: The Critical Role of Secure Information Sharing Solutions for JIE

- Implementing Trusted Thin Client Today: Realizing Cost Savings Through IT Efficiencies While Preparing Your Enterprise for Tomorrow

**About Raytheon Cyber Products**

Raytheon Cyber Products’ portfolio of cyber security solutions provides unprecedented visibility into the enterprise and utilizes advanced analytics to enable a new level of cyber risk management. Through continuous monitoring of endpoints, user activity and other key assets, real-time data is collected and analyzed so decisions can be made instead of merely reacting to alerts. With over twenty years of experience in developing and implementing products for some of the most sensitive and critical enterprise systems operating in the world today, customers trust solutions from Raytheon Cyber Products because they are scalable, secure, architecturally superior and cost effective.