Additional Information about the Joint Information Environment (JIE)

GAO Report to Congressional Committees, GAO-16-693, *"Joint Information Environment: DOD Needs to Strengthen Governance and Management*" (July 2016)

Introduction

The Government Accountability Office (GAO) evaluated the Defense Department's umbrella information technology vision, known as the Joint Information Environment (JIE), from July 2015 to March 2016, as a result of Senate Armed Services Committee Report, No. 113-176.[1] This evaluation focused on determining the extent to which the Department has effectively established scope, cost, and implementation planning for JIE, as well as the extent to which the Department is effectively executing and overseeing governance of JIE.[2]

GAO published its final report on July 14, 2016, and recommended overall that "…DoD…fully define JIE's scope and expected cost, and take steps to improve workforce and security planning."[3] The DoD Chief Information Officer (DoD CIO), the organization responsible for making the vision behind JIE a reality, interpreted this recommendation as an opportunity to help educate the GAO, other interested parties, and industry about this new style of IT.

Although the JIE approach may be somewhat atypical to DoD, *this flexible, somewhat fluid concept of IT through capabilities is consistent with industry best practices, particularly with expansive organizations with varied mission sets like DoD. Given the incredible pace of change in technology, DoD must adapt its approach as appropriate, and learn from industry partners*. As DoD thinks differently about the way in which it advances its IT infrastructure through JIE, the Department will need to work with parties like GAO to advance their thinking about these efforts. This is an initial contribution to what will be an ongoing conversation.

In this paper, DoD CIO offers additional information and context to help illuminate and explain some of the issues raised in the GAO's report. A comprehensive enterprise concept for the IT and cyber infrastructure for an organization of the size, scale, and scope of the Department is intrinsically complex and continual – this vision is what is widely known as JIE. DoD CIO values the GAO's passion and insights, and understands that IT is a complicated and rapidly changing field. GAO has provided DoD with countless valuable recommendations over the years, and many of them have helped improve the Department's processes and practices.

[1] S. Rpt. 113-176 accompanied S. 2410, *Carl Levin National Defense Authorization Act for Fiscal Year 2015,* available online: https://www.congress.gov/congressional-report/113th-congress/senate-report/176/1

[2] GAO Report to Congressional Committees, GAO-16-693, *Joint Information Environment: DOD Needs to Strengthen Governance and Management*, July 2016, available online: http://www.gao.gov/products/GAO-16-593

[3] *Id*

DoD CIO looks forward to working with GAO and other interested parties to successfully advance the Department's IT and cyber infrastructure. DoD CIO first outlined the scope of JIE three years ago. The approach has been refined over time, and it will continue to mature with the pace of technology and the dynamic threat environment. In addition, DoD CIO is currently developing an updated document that will outline the discrete elements of JIE. *This will be an evolving document. As DoD continues to move forward and learn more, its approach to JIE will continually progress and adapt to the complex environment of cyberspace*.

However, JIE is a vision, a concept that will be realized through the implementation of discrete capabilities that will result in the modernization of the Department's IT and cyber environment.

About the Defense Department IT Environment

DoD stands at a cross-road facing a future IT environment that is fast moving, connected, and highly contested. Technology advances rapidly. Adversaries are relentless with traditional and non-traditional methods – DoD is attacked every day in cyberspace. This connectivity impacts the computers and networks that the DoD military, civilian, and contractor workforce use every day, and the vital IT underpinnings of the military's planes, facilities, tanks, and more. *A seamless, transparent infrastructure that transforms data into actionable information and ensures dependable mission execution in the face of the persistent cyber threat is vital in this environment. This IT and cyber infrastructure is the strategic outcome of the JIE vision*.

If the DoD was a corporation, it would be at the top of the Fortune 100 – no organization has a broader mission or scope. Comprised of 1.3 million military personnel on active duty, and 742,000 civilian personnel – plus 826,000 who serve in the National Guard and Reserve forces – DoD is one of the nation's largest employers. It operates globally at several hundred thousand individual structures, with work streams that vary from acquisitions, to command and control, to global logistics, to health and medical care, to intelligence, to facilities management – each with a role in cybersecurity. As a snapshot, some of DoD's IT statistics include:

- DoD IT Budget: > $36B in fiscal year 2015
- Operational Systems: > 10,000
- Data Centers: About 1,700
- Servers: About 65,000
- Computers and IT Devices: > 7 million
- Commercial Mobile Devices: > 600,000

Through the vision for a secure, streamlined IT and cyber infrastructure known as JIE, DoD is pursuing specific IT capacity concepts. The implementation of these discrete elements under the JIE umbrella will result in the comprehensive enterprise modernization of the IT infrastructure that supports the DoD enterprise, for an organization the size, scale, and scope

of the Department. This effort alone is intrinsically complex and continual – but DoD must also keep all of its IT actively supporting its workforce while it is upgrading its IT backbone.

About the Joint Information Environment

From the business to the battlefield, the Department is focused on foundational changes that will modernize and integrate the DoD IT infrastructure to enhance its cybersecurity posture in a more enterprise, coordinated, secure, and cost-effective environment. *Through JIE, DoD has a flexible approach to advancing and integrating its IT infrastructure, because it is a portfolio of discrete IT capabilities that align disparate efforts across the DoD Components*. As an agile approach to improving the Department's IT and cyber capabilities that focuses on distinct elements that are each complex in their own right, JIE is not a program of record, as explained in established documents like the Financial Management Regulation[4]. One of these capabilities and a key foundation for other IT and cyber capabilities is the single security architecture, which is being implemented through the Joint Regional Security Stacks (JRSS).

This approach follows industry best practices. By exploiting proven technologies and game-changing approaches developed by industry, government, and academia, progress will continue to optimize DoD's IT and cyber infrastructures. In engaging with industry partners, the Department is emphasizing capabilities over specific technical solutions that often result in buying and promulgating legacy systems. *This approach is consistent with the Department's efforts to move toward capabilities and agreements with industry, rather than requirements*. JIE allows DoD this flexibility with a comprehensive approach to enterprise IT capabilities.

Through JIE, DoD is gaining efficiencies and improving operational effectiveness and security. The Department is improving the agility of its IT in discrete steps, and making technology and cost decisions that better align to the Department's needs. This is the best approach to lower overall risk and to procure the latest solutions. The flexibility JIE enables will make it more likely to succeed for DoD, and it will help the Department meet the pace of change in technology – but it may also appear contrary to those accustomed to more traditional approaches. JIE focuses on discrete IT modernization elements, such as normalizing network and transport, and standardizing IT security via the Joint Regional Security Stacks (JRSS).

Oversight of JIE

Governance and oversight mechanisms exist to streamline the various IT capabilities under the umbrella of JIE, and relationships and dependencies exist among them. As a result, together the DoD CIO, Joint Staff and USCYBERCOM established and implemented the JIE Executive Committee (EXCOM), tri-chaired at the Senior Executive Service/Flag

[4] DoD 7000.14-R, Volume 2B, Chapter 18, paragraph 180105.BE, Joint Information Environment, available online, http://comptroller.defense.gov/Portals/45/documents/fmr/Volume_02b.pdf

Officer/General Officer (SES/Flag/GO) level. The DoD CIO chartered the JIE EXCOM in the JIE Management Construct dated November 9, 2012. The JIE EXCOM comprises stakeholders across the Department to provide oversight and approval of capability requirements, solutions, funding, and scheduling. Some of the IT and cyber capabilities in the JIE portfolio are at a higher priority level than others, so the JIE EXCOM focuses on them.

Through this approach, JIE oversight is flexible enough to accommodate the incredible complexity associated with advancing IT across an organization of DoD's size, scale, and scope; as a program of record, this modernization effort would lose this flexibility. Most of the funding associated with JIE, such as funding for JRSS, is included in the Military Departments (MILDEPs) technology refresh dollars. None of the work associated with the IT modernization portfolio is developmental in nature. The initiatives are realignments and changes in scope based on successful approaches from one or more of the Military Services and DoD Agencies.

The governance of JIE cannot and will not stay stagnant. As the Department adapts its processes and technologies, DoD will also advance its governance of JIE. JIE is focused on a more enterprise approach to the governance of JIE, which couples centralized oversight with the ability to react and anticipate the unique needs of the Military Services.

Current Vision and Cost of JIE

A series of Joint Chiefs of Staff Tank and Deputy Secretary Management Action Group (DMAG) decisions in 2012 broadly laid out the vision of JIE. DoD CIO, via the JIE EXCOM, has further refined the priorities of those capabilities, consistent with the 2013 JIE implementation strategy. DoD first specified the vision of JIE in the DoD Chief Information Officer Guidance for Implementing JIE, signed September 2013. *Implementing the vision of JIE will lead to comprehensive IT modernization for DoD – not the other way around*.

The Defense Information Systems Agency (DISA), which reports to the DoD CIO, established the Joint Technical Synchronization Office (JTSO) to develop the technical architectures to ensure that all of the capabilities under the JIE umbrella operate well together. JTSO is currently working through the third iteration of architecture development. Implementation has started on mature capabilities like JRSS and the foundational network modernization it includes. Application Rationalization and Desktop Virtualization remain goals related to JIE, and they are being implemented in smaller scale or as pilots, such as cloud computing. *This flexible approach allows the Department to take risks and fail small, addressing technical and policy issues through pilots*. The DoD CIO is in the process of completing an updated JIE document to better define the relationship, dependencies and maturity of capabilities under the JIE umbrella, with a goal of JIE EXCOM approval by December 2016. This scope will be a living document. As the Department continues to move forward and learn more, its approach to JIE will continually progress and adapt to the complex environment of cyberspace.

Schedule for JIE

JIE will result in IT modernization efforts with decentralized execution that allows for closer alignment with diverse warfighting priorities. As a result, JIE is focused on the near-term priority efforts outlined in the JIE Implementation Strategy. *Scheduling takes place as appropriate for these discrete IT and cyber capabilities that fall under the JIE umbrella. For example, JRSS is the most critical near-term element of the JIE portfolio*. Planning for JRSS, including budget and schedule, are discussed JRSS PMO briefings to the JIE EXCOM, which regularly include the JRSS schedule – including implementation of network upgrades, the stacks, and the migration schedule. In July 2016, the JIE EXCOM approved the JRSS Migration Planning Board Charter. The JRSS Migration Planning Board is chaired by the JRSS PMO, with membership from the Combatant Commands/Services/Agencies (CC/S/As). The JRSS Migration Planning Board will assess schedule variances and provide recommendations to the JIE EXCOM for approval. Additional information about JRSS is provided in the sections below. JRSS is realigning funds for the Military Services and DISA into a more simplified, integrated plan that addresses the need for standards and oversight, while allowing for unique Service mission needs.

DoD Oversight for JIE

DoD CIO is responsible for directing the implementation of the discrete items included in an internal DoD guidance document called the JIE Framework. *Accordingly, DoD CIO reorganized its staff to create the Deputy Chief Information Officer for Information Enterprise (DCIO IE), whose primary function is to plan, manage, and integrate the various IT modernization efforts that comprise JIE*. The Charter for the JIE Management Construct, dated November 2012, establishes the organizational and functional framework, defines roles and responsibilities, and specifies processes for implementing, governing and administering the JIE Strategy. As such, DoD CIO leads development, integration, and synchronization of JIE governance. The JIE EXCOM, chaired by the DoD CIO, USCYBERCOM, and the Joint Staff J6, sets the JIE direction, articulates goals and objectives, oversees the JIE Framework and maintains accountability.

Start and End Dates for JIE

JIE is not a program of record, so it is not conducted with the traditional program management "cradle to grave" mentality. As a result, the work toward moving DoD's IT to the JIE vision will not "end." *DoD is not and could not "end" work on JIE, because it is a vison of an end-state against an ever-changing IT landscape*. JIE is comprised of discrete IT and cyber capabilities, with the approach to better align the Department with how the IT industry tackles the pace of change and speed of technology. Traditional program management, with multi-year documentation and development efforts, cannot keep pace with the speed of today's IT.

For example, cloud technology and improved security technology have already influenced how DoD is approaching the Mission Partner Environment (MPE). *With a more flexible approach to overseeing discrete JIE capabilities, this adaptability is possible*. MPE is the Department's new approach for sharing both unclassified and mission secret information with its partners. Its intent is to migrate DoD from regional, such as Combined Enterprise Regional Exchange System (CENTRIXS), and physical instantiations to global and virtualized instantiations.

The Department continues to use tested commercial technologies and practices, which greatly reduces the risk to the Department. No longer is DoD building unique IT solutions, but instead is pivoting and actively pursuing solutions based on industry best practices and products. The flexibility enabled by JIE empowers DoD to take this approach to continuously advancing its IT and cyber infrastructure with no end date, because technological change will never end.

Cost Estimates for JIE

DoD must take a different approach to address its IT and cyber infrastructure capabilities. Rather than focusing on the total cost of JIE, DoD CIO has made IT efficiency a top priority, with an emphasis on reducing overall DoD IT spending. *While realigning existing IT program funding to pay for priority JIE initiatives, such as JRSS, the Department also has identified more than $1 billion in IT efficiency savings over the past year, allowing DoD to reallocate needed resources to support urgent weapon system requirements*. For example, by replacing hundreds of disparate security systems with the common JRSS Enterprise Service, the Army alone estimates over $500M in savings within the next five years. Implementing the vision of JIE and its specific discrete capabilities will cost less than what DoD spends today.

JIE is not a monolithic program of record with a centralized funding line. But cost assessments have taken place for the discrete elements of JIE, such as JRSS. As the Department's IT modernization efforts move forward, additional costs for future efforts also will be better understood. As progress continues on the JIE continuum, costs of its additional discrete elements will be similarly understood, and the DoD Components will be able to anticipate and realign their budgets to accomplish them. Any cost assessment for the entirety of JIE would be premature. It would be based on current technology instead of needed capabilities, and it would not provide the flexibility required to deliver the right solutions. DoD is not and could not "buy JIE" because it is a vison of an integrated, agile, responsive end-state, not a system. *A basic tenant of JIE is that it must be executed within available budget dollars. JIE's goal is to use industry best practices and new technology in order to save money for the Department*.

Joint Regional Security Stacks

JRSS addresses the immediate need to defend the cyber warfighting domain. It is a globally implemented, centrally managed suite of network security appliances that standardize and secure the current DoD IT environment and drive cost-effectiveness due to "sun-setting" local network security protections and duplicative network security infrastructures.

As JRSS enables global synchronized network operations, no single DoD Component will have to solve cybersecurity issues on their own. JRSS will allow the cyber and network defenders to better understand traffic flow by improving enterprise-wide visibility into network traffic. *This will allow for prompt detection of vulnerabilities to enable quicker, more effective responses to cyber threats. JRSS will also provide a baseline for more coherent, common network security capabilities for DoD's cyber defenders*, shrinking the attack surface to about fifty discrete points on the DoD Information Network, from the current level of more than one-thousand points on the classified and unclassified networks. JRSS also comprises several critical capabilities for DoD, including network modernization, initial implementation of a single security architecture, joint management of DoD IT security, and improvements to cybersecurity situational awareness through the Cyber Situational Awareness Analytic Capabilities.

Planning and Execution of JRSS

JRSS is DoD's near term priority for IT and cyber agility, and it is fielded as an Enterprise Service, as designated by DoD CIO in November 2015. As an Enterprise Service, JRSS transforms the network and its security, and significantly improves mission effectiveness for the Department by offering situational awareness visibility for all echelons. *JRSS aligns the DoD Components to a common capability, and allows them to align their individual funding lines for their individual network security system funding to the JRSS resource line*.

The DoD Components agreed to take an incremental approach to fielding JRSS, and are developing implementation plans to migrate to JRSS while decommissioning individual, legacy network security capabilities. In short, the U.S. Army began its migrations to the JRSS last summer, with the U.S. Air Force and the U.S. Navy migrating users this summer.

JRSS began as the U.S. Army's approach to improve its network security while reducing costs. The Army reprioritized funds in fiscal year 2013 to procure the fifteen stacks on the DoD unclassified network, and reprioritized funds in fiscal year 2014 for the implementation on the classified network. DISA became the Portfolio Manager and Executive Agent to procure the stacks for the Army. DoD CIO saw value in applying this approach across DoD to achieve even greater savings and improved network effectiveness and security across the Enterprise.

In fiscal year 2015, the Air Force reprioritized funds within their budget to enable the initial JRSS purchase to include capabilities comparable to its Air Force Network Gateway (AFNET GW) systems. The Air Force made a commitment to no longer tech refresh their AFNET GWs, but instead align funds to the JRSS Enterprise Service and decommission their AFNET GWs.

In the fall of 2014, the U.S. Navy and U.S. Marine Corps joined the partnership with the U.S. Army, U.S. Air Force, DISA, and DoD CIO, and nominated additional features to JRSS, which compares to their Enterprise Gateway network security systems and would be the catalyst for them to use the JRSS and decommission their Enterprise Gateway network security systems.

During the summer of 2015, DoD CIO led the coalition of the Military Departments, the Joint Staff, U.S. Cyber Command, DISA, and Defense Health Agency (DHA) to identify funds needed in a few areas for JRSS. The funds would be needed to implement JRSS globally; include comparable capabilities in JRSS that would allow the DoD Components to decommission their individual network security systems and instead use JRSS; and lifecycle cost for tech refresh, sustainment, and maintenance of JRSS for fiscal years 2017 to 2021. *The Military Departments and DISA realigned funds within their IT budgets to pay for JRSS procurement, fielding, deployment, sustainment, and tech refresh*.

At this point in time, no new funds were identified or used for the fiscal year 2017-2021 requirement. The Military Departments and DISA agreed not to procure, field, deploy, operate, and sustain individual systems for each DoD Component. With the designation of JRSS as an Enterprise Service, DoD CIO required separate identification of JRSS within the DoD Fiscal Year 2017 President's IT Budget submission, and the Military Services transferred funds to DISA for execution starting in fiscal year 2017-21. Beginning in fiscal year 2018, DISA will annually present the spend plan to the JIE EXCOM for endorsement, and the DoD Comptroller will issue a directive to move funds from the Military Departments to DISA for execution.

The implementation of JRSS has been complicated and nuanced, and it has differed across the DoD Components. *JRSS is only one key capability under the JIE umbrella, and it demonstrates how DoD is following industry best practices to advance its IT and cyber infrastructure for the entire Department – not only for individual DoD Components*. The implementation of JRSS is only one of many examples that illustrate why categorizing all of JIE as a program of record would not add value to such a comprehensive enterprise approach to improving the resilience, security, and agility of the DoD IT and cyber infrastructure.

DoD IT/Cyber Workforce

JIE is a comprehensive enterprise approach to the IT and cyber infrastructure for an organization of DoD's size, scale, and scope. As a result, various initiatives across the

Department to advance its cyber and IT workforce and ensure its success in a future IT environment that is fast moving, connected, and highly contested all are applicable to JIE.

Congress recently enacted a law that outlines the requirements for a federal-wide cyber workforce coding initiative that will affect both DoD civilian and military cyber personnel.[5] It will help the Federal Government to code IT, cybersecurity, and other cyber-related functions. This requires an examination of all cyber positions and identification of work roles and tasks associated with each job. The Department will use the resulting data to enhance management of the DoD cyber workforce, to include developing qualification requirements for each work role. This, in turn, will inform identification of the type of personnel and specific skills required to support enterprise operations and services and the governance capabilities needed to oversee a more agile IT architecture through JIE, and continue looking to tomorrow's DoD IT environment. Coding of the federal civilian cyber workforce is to be completed by December 2017, and coding of the military cyber workforce by December 2018, as required by law.

DoD is also actively implementing the excepted service hiring authorities for its cyber workforce as recently authorized by Congress.[6] *The new DoD Cyber Excepted Service capabilities will provide more agile management processes and improve DoD's ability to recruit and retain cyber talent*, including personnel who perform traditional IT, cybersecurity, cyber mission-focused effects and cyber-focused intelligence functions, and those who perform related support functions like acquisition, training, human resources, and policy and planning.

Security Assessments

At the direction of the DoD CIO, the DoD's NIPRNet / SIPRNet Cyber Security Architecture Review (NSCSAR) is being conducted by DoD CIO, the National Security Agency (NSA), and DISA in coordination with other DoD Components. *NSCSAR makes recommendations about where cybersecurity capabilities are best positioned in the architecture to provide the greatest operational effect, and its assessments will be delivered incrementally*.

In addition, DoD has also implemented a Cybersecurity Scorecard that is reported monthly to the Secretary of Defense to monitor cyber basics and improvements in establishing a common security baseline. *This Scorecard tracks compliance with ten of the most significant issues identified in the DoD Cybersecurity Discipline Implementation Plan*. They include removing obsolete operating systems, and upgrading to a modern operating system with advanced security features (e.g., Windows 10). It also tracks patch compliance and configuration compliance across DoD, and ensuring Internet-facing web servers are in demilitarized zones.

[5] Sections 301-305 of Public Law (PL) 114-113, the "Federal Cybersecurity Workforce Assessment Act of 2015," available online: https://www.congress.gov/bill/114th-congress/house-bill/2029/text
[6] Section 1107 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92), available online: https://www.congress.gov/bill/114th-congress/senate-bill/1356/text

Closing Considerations

The pace of change in the threat environment, coupled with the pace at which industry develops new products that can bring new capabilities to the Warfighter requires DoD to take this new, perhaps unfamiliar, approach to improving its IT infrastructure. No longer can DoD afford to do traditional, "business as usual" acquisitions when it comes to IT modernization. Rapidly evolving threats within the cyber terrain requires the Department to strengthen and secure its infrastructure just as quickly. It also calls for DoD to invest existing IT-programmed funds directly into capabilities for the warfighter to see results immediately and bringing in new capabilities faster, leveraging proven commercial tools and practices for critical missions.

This remarkable pace of change in the DoD IT and cyber environment – both the threats and opportunities it introduces – requires DoD to advance by following successful industry best practices. The Department's approach to implementing the discrete JIE capabilities parallels these industry best practices. It empowers DoD to improve the security, resilience, agility, and transparency of an infrastructure of an unparalleled scale with flexibility, while enabling the ability to take smaller risks with individual efforts – failing small and recovering quickly. This is not how DoD has done business in the past. GAO has provided DoD with countless valuable recommendations over the years, *and as the Department thinks differently about the way in which it modernizes its IT infrastructure through JIE, DoD looks forward to helping GAO and other interested parties – including itself – think differently about the new style of IT*.