THE JOINT INFORMATION ENVIRONMENT

THE IT FRAMEWORK FOR THE FUTURE


77

EXECUTIVE SUMMARY

In the midst of World War II, Phillip Johnston was looking for a way to support the Allied forces. As a veteran of World War I, he was too old for active duty, but he felt a moral obligation to be part of the war effort.

At the time, the military was looking to develop an undecipherable code to use in combat operations. Allied forces had been losing ground in the Pacific as Japanese intelligence operatives cracked their codes and obtained information via radio communication. Reading this news, Johnston got an idea. Having grown up on a Navajo Indian reservation, he was one of the few non-Native Americans who could speak Navajo fluently. He bet that enemy forces had gathered limited intelligence to decipher Navajo.

Johnston successfully persuaded the Marine Corps to conduct a pilot program to test how quickly Navajo speakers could transmit intelligence via a series of code words in Navajo. It was a success, so the military expanded the Navajo Code Talkers program, deploying teams in both the Pacific and European theatres. Johnston's bet paid off. Today, historians credit the Navajo Code Talkers as a key reason why the Allied forces were victorious.

The program reinforces the necessity of safely and securely transmitting intelligence during combat operations. But in today's digital world, intelligence flows not only through spoken language over a radio, but also across highly regulated and monitored information networks. To preserve and protect intelligence as it flows across these networks, the U.S. military needs a new approach.

That's why in December 2012 the Department of Defense (DoD) developed the Joint Information Environment (JIE) framework. JIE is an ambitious multiyear effort designed to realign, restructure and modernize the department's information technology networks. It will change the way DoD networks are constructed, operated and defended.

Since JIE is not a program of record, it is often hard to conceptualize. Simply put, JIE's ultimate goal is to converge all communications, computing and enterprise services into a single platform that can be leveraged for all DoD missions. To do that, JIE will:

- Remove barriers to information sharing.
- Promote collaboration and interoperability across DoD and mission partners.
- Enhance DoD security against cyberthreats and vulnerabilities.
- Simplify DoD IT infrastructure.

JIE is the department's attempt to remove barriers to collaboration while reducing the cyberthreat landscape. To put the complexity of JIE into perspective, consider some insights from "The Department of Defense Strategy for Operating in Cyber," which states that the DoD operates more than 15,000 networks and 7 million computing devices. Additionally, in a statement by Teresa Takai, former DoD chief information officer, to the House Armed Services Committee, she notes that the DoD IT environment must credential and connect 3.7 million people working inside and outside the department. This includes active-duty service members, reserves, the National Guard, and civilian and contractor support for base personnel.

These statistics only scrape the surface of the complexity of DoD's work to deploy the JIE framework, but the effort is worthwhile because it will help the military retain a strategic edge on the battlefield.

Our guide aims to provide you with the insights and knowledge you need to understand JIE. Specifically we'll cover:

- DoD's vision for the JIE framework.
- A JIE prep sheet and the Defense Information Systems Agency's role in deploying JIE.
- Insights on technical and policy challenges.
- Strategies to acquire the proper technology solutions.
- Next steps and future implications of JIE.

Whether it was the Navajo Code Talkers or current cyber professionals, securing information networks and preserving intelligence has always been a top concern of the U.S. government. With emerging technology, we have the opportunity to encourage collaboration, provide information quickly and accurately to those who need it, and keep it out of enemy hands. JIE is a step in this direction, and will transform how DoD operates. Our guide explores how.

Cover image: *Refueling over the Atlantic* (U.S. Air Force photo by Tech. Sgt. Paul Villanueva II/Released)
Opposite: *Sailors run on the flight deck.* (U.S. Navy photo by Mass Communication Specialist 2nd Class Tony D. Curtis/Released)

CONTENTS

The Necessity of Partnership Between Industry & Government..... 5

Your Joint Information Environment Prep Sheet 6

From the Foxhole to the Cubicle: Data Storage & JIE..... 9

Toward the JIE Framework: Key Policy & Technical Challenges..... 10

Creating Better, More Informed Decisions Through Streamlined Data..... 13

The Role of DISA in Evolving JIE..... 14

Case Study: JIE Success at Joint Base San Antonio, Texas..... 15

The Key to the Joint Information Environment: On-Demand Services..... 17

JIE Management..... 18

Impact on Workforce..... 19

Helping the Warfighter Maintain a Tactical Edge..... 21

Acquisition Strategy for DoD..... 22

About GovLoop..... 23

Acknowledgments..... 23

As the Information Technology landscape evolves, DLT Solutions continues to adapt and provide emerging technology solutions to our customers.

For more than 20 years DLT Solutions has been dedicated to solving public sector IT challenges. Guided by our relentless focus on these challenges, we have grown to be one of the nation's top providers of world-class IT Solutions. Here's why:

- We bring both deep subject matter expertise and in-depth knowledge of government-mandated requirements and initiative to each customer relationship.
- Leveraging our position as a leading, strategic partner with top IT companies, we develop best-fit solutions for our customers.
- Our sales staff and integration experts have the certifications and experience at helping customers at any level of any agency.
- We contribute to the development of new standards and policies to drive innovation in various technology areas.

DLT SOLUTIONS®

13861 SUNRISE VALLEY DRIVE, SUITE 400 | HERNDON, VA 20171 | www.dlt.com | 703.709.7172 | DLTSOLUTIONS

THE NECESSITY OF PARTNERSHIP BETWEEN INDUSTRY & GOVERNMENT

An interview with David Blankenhorn, vice president, engineering and chief cloud technologist, DLT Solutions, and Doug Martin, director, field sales, DLT Solutions.

Although the Joint Information Environment is not officially a program of record, the IT architecture will ultimately be deployed and put into practice by initiatives all across the DoD.

"The JIE is tremendously valuable if used, and in my mind long overdue," said David Blankenhorn, the vice president of engineering and chief cloud technologist at DLT Solutions, a value-added solutions provider to the public sector. But in meeting the ultimate vision of a shared and converged IT infrastructure, the DoD faces challenges.

"Anytime you have stove-piped systems, it is always difficult to get collective buy-in," said Blankenhorn. "From a top down DoD perspective, having something like the JIE is a no brainer, but having to translate the value down to the personnel out on specific missions or in the trenches, they may not be as concerned about the bigger picture. Their focus could be mission specific and accomplishing the task at hand."

Another challenge faced by the DoD, said Blankenhorn, is the sheer complexity of DoD networks. "The [DoD] is the largest computing environment in the world that JIE is looking to address," he explained. "There is a lot of inertia, one-offs and custom technology scattered all throughout the environment. So trying to bring that under a common architecture that can be secured, managed and maintained over time is not a trivial effort by any stretch of the imagination."

Although these challenges exist, Blakenhorn says they'll be worth overcoming to ultimately experience the core benefits of the JIE. "The primary benefit that I see from JIE is that we have the ability to securely get the right information to the right people, at the right time, on the right device in order to support the mission. That's really what JIE is about," said Blankenhorn.

Other benefits Blankenhorn says the JIE will offer include standardization, interoperability of systems, improved security, and reduced time to purchase and deploy IT.

DLT Solutions is helping the federal government build awareness about JIE, and the impact that the framework will have in meeting critical missions.

"We can help promote the JIE message, and build a groundswell of support," said Doug Martin, the director of field sales for DLT Solutions. "So when we go out and talk to customers during our day-to-day support, we can give a different perspective. We can talk about the benefits we see across the street, or across the country, at another military base, or insights on a DOD installation, and what JIE enhancements have done at a particular shop and how they can benefit a specific agency."

"The irony of the situation is that at DLT, we have spent a lot of time evangelizing across government about government programs, and JIE is a good example of that. We actually spend a lot of time educating people in the public sector about these programs," added Blankenhorn.

But to achieve deployment of the JIE framework, government and industry must work together. Fortunately, Blankenhorn and Martin believe there is already a healthy exchange of information between the DoD and industry, especially in terms of sharing IT roadmaps.

"The senior leadership of DoD has shown it wants to learn from industry about what the future looks like in 12-18 months for IT advancements," said Martin. "I think what DoD can also do is to continue to share their requirements, to make sure the requirements map to each other. That way you can do a litmus test, and be sure industry and government are aligned."

He added: "The key really is that it is going to be critical for DoD and industry to continue to collaborate, and I think the last thing that anyone wants is have the JIE stagnant as technology capabilities increase, or as mission requirements evolve. It would be great to see in five years, when JIE has been deployed, a dynamic architecture that can leverage the latest advancements in technology."

For continued success of the JIE framework, government and industry must continue to work collectively and collaborate. This way both parties will know that as technology advances the JIE infrastructure will also be able to evolve to meet the needs and capabilities from a mission requirements and technology perspective.

Through collaboration between government and industry, DoD personnel can have the confidence they have an IT infrastructure able to meet the ultimate end state of JIE.

YOUR JOINT INFORMATION ENVIRONMENT PREP SHEET

The Joint Information Environment will change the way that DoD protects our country. The initiative's complexity is daunting, however, so we start our guide by breaking it down. We highly recommend you go through this section first before progressing further.

SO, WHAT IS JIE?

A good starting point is to review a statement to Congress by former DoD Chief Information Officer Teri Takai, which says:

"JIE will have federated networks that are built to common standards and configurations, and expanded use of shared IT infrastructure and enterprise services, which include thin clients, everything-over-IP, e-mail, and cloud services. The services will continue to operate and maintain their portion of the JIE, as well as provide mission-unique capabilities while incorporating shared IT transport services and common applications."

That quote can be broken down into six bite-size goals of JIE:

1. Realign, restructure and standardize DoD IT networks.
2. Improve the way DoD networks are constructed, operated and defended.
3. Provide better information access to all DoD stakeholders.
4. Improve how DoD protects data.
5. Reduce the cyberthreat landscape and provide more visibility of networks to combat and thwart cyberattacks before they happen.
6. Create a more responsive and agile information architecture to keep a tactical edge.

Why did the department embark on such an ambitious initiative? We explore more in our next section, but for now, we can point to four key drivers:

- **Modernize IT infrastructure:** A streamlined environment will help DoD agencies meet their complex missions more effectively by deploying world-class IT.
- **Decrease costs:** By moving to the cloud, reducing data centers and improving data management, the agency can minimize costs and better equip military and civilian personnel to make more informed decisions.
- **Optimize resources with limited budgets:** JIE consolidates systems into a single platform, helping streamline information and optimizing how stakeholders acquire and access data.
- **Reduce cyberthreat landscape:** Consolidated systems, better network awareness, and comprehensive identity management will enable DoD to preserve and protect networks more effectively with the JIE framework.

As you know, talking about government and technology involves scores of acronyms. We tried to write in plain language throughout this report, but in case you need a quick reference, check out our JIE glossary below.

Now that we've given you a quick overview of JIE, hopefully you're ready to dive a bit deeper. We'll move onto a brief history of JIE and how the program is changing the way DoD operates.

JIE GLOSSARY

ADM	Acquisition Decision Memorandum
CAC	Common Access Card
CANES	Consolidated Afloat Network and Enterprise Services
CCA	Clinger Cohen Act
CDES	Cross Domain Enterprise Service
CONUS	Continental United States
CYTAC	Cyberspace Training Advisory Council
DAB	Defense Acquisition Board
DCO	Defense Connect Online
DEE	Defense Enterprise Email
DEPS	Defense Enterprise Portal Service
DISR	DoD IT Standards and Profile Registry
FDCCI	Federal Data Center Consolidation Initiative
FEDRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
IA	Information Assurance
IDAM	Identity and Access Management
IOC	Initial Operational Capability
IPN	Installation Processing Node
JTSO	JIE Technical Synchronization Office
MAS	Mobile Application Store
MDM	Mobile Device Management
NDAA	National Defense Authorization Act
NICE	National Initiative for Cybersecurity Education
SSA	Single Security Architecture

HISTORY & CURRENT STATE OF JIE

JIE is an unbelievably ambitious yet necessary DoD initiative. Below, we share a few statistics about the size and scale of the department's IT shop, but here's some additional context: DoD hosts more than 6,000 locations, supports 40 agencies and manages about 3.7 million people with cyber identity credentials.

JIE dates back to about 2010, when former Defense Secretary Robert Gates led the charge to develop the foundation for the JIE framework. A January 2013 report by the Joint Chiefs of Staff described JIE as:

"A secure joint information environment comprised of shared information technology infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies. The JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs)."

JIE comes at an important time, as DoD leaders realize that our wars are not just being fought on the ground; they are also being waged across our networks. In the past decade, the department has spent an enormous amount of time and resources covering the world with bandwidth and computing resources to provide the DoD workforce with the tactical edge it needs against enemies. This not only provides much-needed intelligence to commanders on the ground, but also gives them the confidence that information and data are transmitted safely and securely.

As the battlefield has extended to a digital front, DoD must continue to improve the security and accessibility of data. Data accessibility is one of JIE's core components, and it aims to convert DoD from a network-centric to a data-centric model. Department leaders now understand that data is a strategic asset.

This is why Takai championed JIE during her tenure as DoD CIO. In a report to Congress, she identifies four ways JIE will help:

- "A standardized information and security architecture will improve how DoD operates and secures its networks on a global level. Users and systems will be able to trust their connection from end to end with the assurance that their activity will not be compromised."
- "The JIE's standard security architecture will enable cyber operators at every level to see the status of their networks for operations and security and enable commonality in how cyberthreats are countered. The department will know who is operating on its networks and what they are doing, and be able to attribute their actions with a high degree of confidence. This will minimize complexity for a synchronized cyber response, maximize operational efficiencies, and reduce risk."
- "Consolidation of data centers, operations centers and help desks will enable users and systems to have timely and secure access to the data and services needed to accomplish their assigned missions, regardless of their location."
- "A consistent DoD-wide IT architecture supports effective fielding of department capabilities in support of information sharing, as well as sustainment and integration of legacy systems."

These benefits help the agency work toward the ultimate objective of converging all communications, computing and enterprise services into a single platform that can be used for all DoD missions.

JIE will be created so that divisions will still have autonomy but abide by common standards and configurations to support collaboration. The hope is that JIE will transform the way that DoD uses new and legacy IT. It will reduce the complexity of DoD IT and improve management of users accessing DoD networks.

To get there, JIE requires additional technology components, which will seamlessly work together to create a unified, consolidated and efficient technology infrastructure.

In our next section, we break down some of the components and highlight the related technical and policy challenges.

"A secure joint information environment comprised of shared information technology infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies. The JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs)."

JIE/DOD STATS

These statistics trump the size and scope of any private-sector organization. Recognizing this complexity and the need to consolidate systems, DoD leaders needed a way to create a shared technology infrastructure, giving our nation's warfighters a tactical edge on the battlefield and reducing our cyberthreat landscape.

PERSONNEL

In fiscal year 2013, the department had...

1,400,000 active-duty

750,000 civilian

1,100,000 National Guard and reserve

5,500,000 family members and retirees

146 countries

TECHNOLOGY

Also in fiscal 2013, DoD operated...

10,000 operational systems

800 data centers

65,000 servers

7,000,000 computers

250,000 mobile devices

BUDGET

That year, IT represented a...

$37 BIL. investment

7 % of the total DoD budget

$20.8 BIL. in IT infrastructure

$3.4 BIL. for cybersecurity

We see a cloud where your data lives without limits.

Choose the right cloud solution that works for you.

Visit netapp.com/unboundcloud

UnboundCloud™
The new vision of cloud data management

NetApp®

ENABLING AN INTEGRATED ENVIRONMENT FROM THE FOXHOLE TO THE CUBICLE: DATA STORAGE & THE JIE

An interview with Dr. Gregory Gardner, chief architect, government and defense solutions, NetApp.

The Joint Information Environment (JIE), once deployed, will have far-reaching impacts on the way that the DoD shares critical information. But in order to capitalize on the benefits of the JIE framework, organizations must focus on their data storage practices, which have major implications on the ability of units and organizations to access information.

GovLoop recently spoke with Dr. Gregory Gardner, the chief architect for defense and intelligence solutions at NetApp. Dr. Gardner provided expert analysis on the JIE framework, and discussed how NetApp is helping the DoD reach its desired JIE end state.

"The target objective of the JIE is a state that optimizes all of DoD's IT assets by converging communications, computing and enterprise services into a single joint platform, in a single security architecture," Dr. Gardner explained. "[NetApp] believes fundamentally that is the right thing to do, and we believe that NetApp's storage-focused solutions and services facilitate achievement of the JIE end state."

"We believe the way we are providing data storage to the DoD, enhanced by our storage management tools, is helping the Department achieve its mission. We are enabling the DoD to move aggressively toward its goal of establishing and operating within a Joint Information Environment."

One of the ways NetApp is helping the DoD advance toward its goals is by providing much of the data storage backbone for both tactical units and enterprise organizations. This enables the DoD to move, share, and protect data, so that information is available to decision makers and staffs across the globe quickly and securely.

"The Army uses the terminology, 'from the cubicle to the foxhole,'" explained Dr. Gardner. "That means sharing relevant data from the enterprise user who is sitting at the Pentagon, all the way to someone who is in a Battalion Task Force or serving on a Brigade Combat Team operating overseas. Both need efficient, effective, synchronized, and optimized information. NetApp provides the data storage operating system that underpins the development of that information."

"The NetApp storage operating system is the most widely used storage operating system in the world. Moreover, NetApp is the leading data storage provider to the Department of Defense," said Dr. Gardner.

The reason NetApp is so widely used is that its Storage Operating System, known as DataONTAP, provides a number of unique capabilities. NetApp has the ability to de-duplicate primary data which can reduce the amount of data stored by well over 50 percent. Additionally, NetApp uses a unique approach called thin provisioning.

"With thin provisioning, you can save about 33 percent of your data storage by proportioning just enough data so people can do what they need to do and not use more than they are allotted," said Dr. Gardner.

Another distinctive feature of the DataONTAP Operating System is that it provides the ability to quickly take snapshots of data and clone terabytes of data in just a few minutes.

"By using our snapshot technology, DoD users can backup and make changes to their data sets very quickly. This is part of what makes NetApp unique, facilitates our support to the DoD, and enables the Department to achieve its objectives," said Dr. Gardner.

NetApp also deploys what Dr. Gardner described as an agentless, heterogeneous tool called OnCommand Insight. OnCommand Insight does not reside on a single infrastructure and it works with any type of data storage technology.

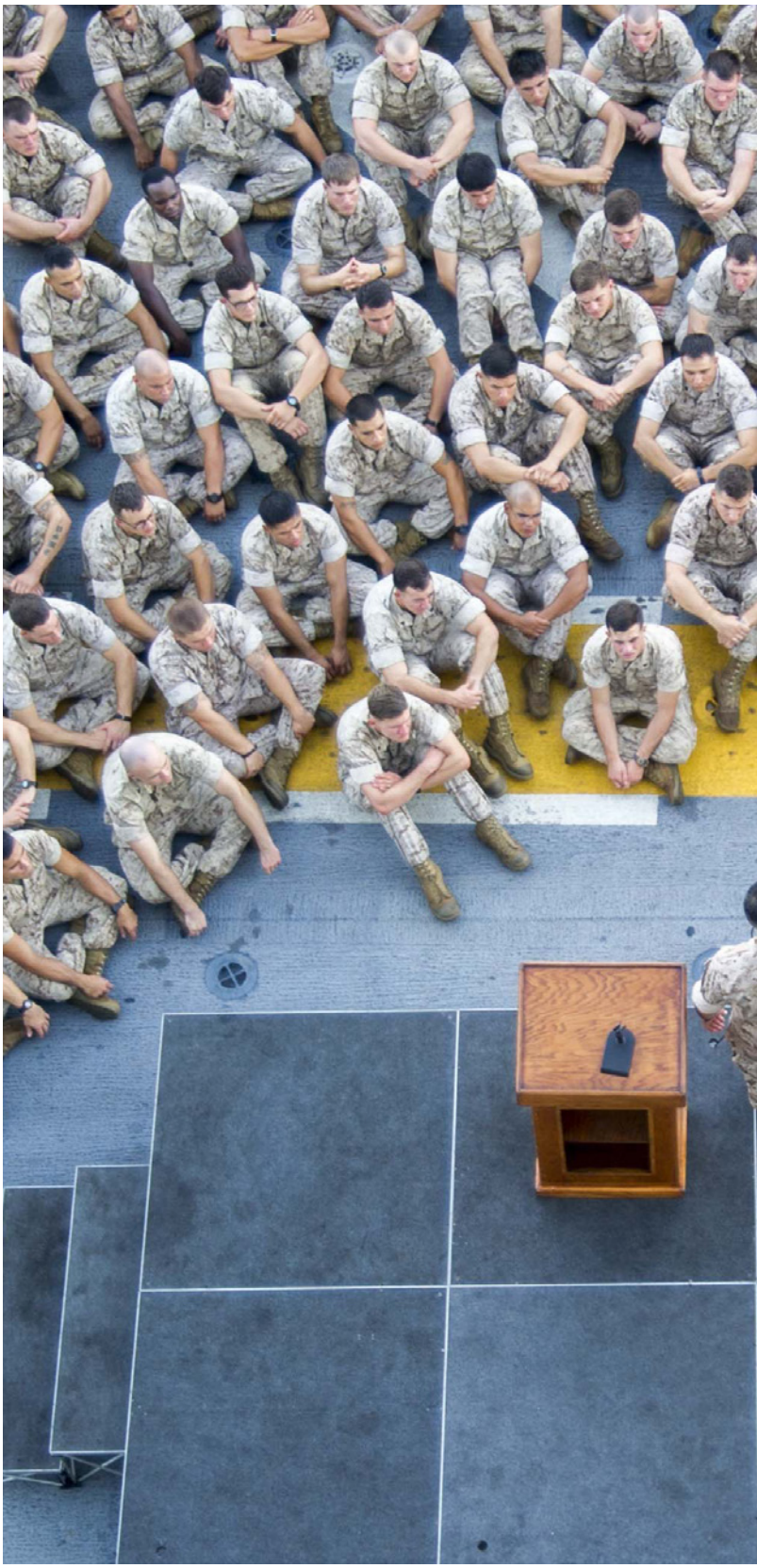
In addition to providing total visibility to all data stored on a network, OnCommand Insight also provides detailed data on all the routers and switches that are connected to the storage, as well as every virtual machine in the storage array. This provides the storage manager with exceptional information on how well storage is being used, what parts are idle, and what parts can be leveraged for other purposes. It also enables managers of storage arrays used by multiple users to see who is using how much storage and for what purposes. That information can be used to make different data storage investment decisions.

"We find that in data centers, the OnCommand Insight tool helps people manage their infrastructure much more effectively; it gives them a tool to allow them to blend technical understanding with business case analysis," said Dr. Gardner.

NetApp is already playing an essential role to help the DoD deploy the JIE framework, and it's one they take very seriously. "It is a significant responsibility. We are very proud to provide our DoD customers the best possible support as they execute their critical missions," concluded Dr. Gardner.

TOWARD THE JIE FRAMEWORK: KEY POLICY & TECHNICAL CHALLENGES

To achieve the ultimate goal of the JIE framework, DoD is moving toward an information-centric IT structure. In other words, JIE is consolidating systems to avoid the haphazard disbursement of networks, services and tools across DoD. By taking an enterprise approach, DoD workers will gain access to information and make better decisions in the field. This will give combat personnel an edge, but the shift toward enterprise services presents numerous policy and technical challenges for the department. We highlight them below.



MOBILITY

In May 2012, DoD released its mobile device strategy, highlighting a vision to evolve mobile capabilities departmentwide. It includes insights on policies, standards, app development and web-enabled IT for device support.

"The nature of the DoD workforce is mobile," the report said. "Its mission requires the provision of forces over air, land, and sea, across foreign borders, and into adverse conditions. Civilians and military personnel regularly rotate across organizations; leadership and field units regularly travel from place to place; and a growing number of teleworkers are beginning to operate from locations other than their primary officers. The mobile workforce's ability to access information and computing power can improve information sharing, communication, and action response time for greater mission effectiveness."

The JIE framework will eliminate barriers to access mobile applications. The Defense Information Systems Agency (DISA) has deployed an unclassified, enterprise-wide application store that delivers and updates apps without employees having to contact IT for support.

ENTERPRISE SERVICES

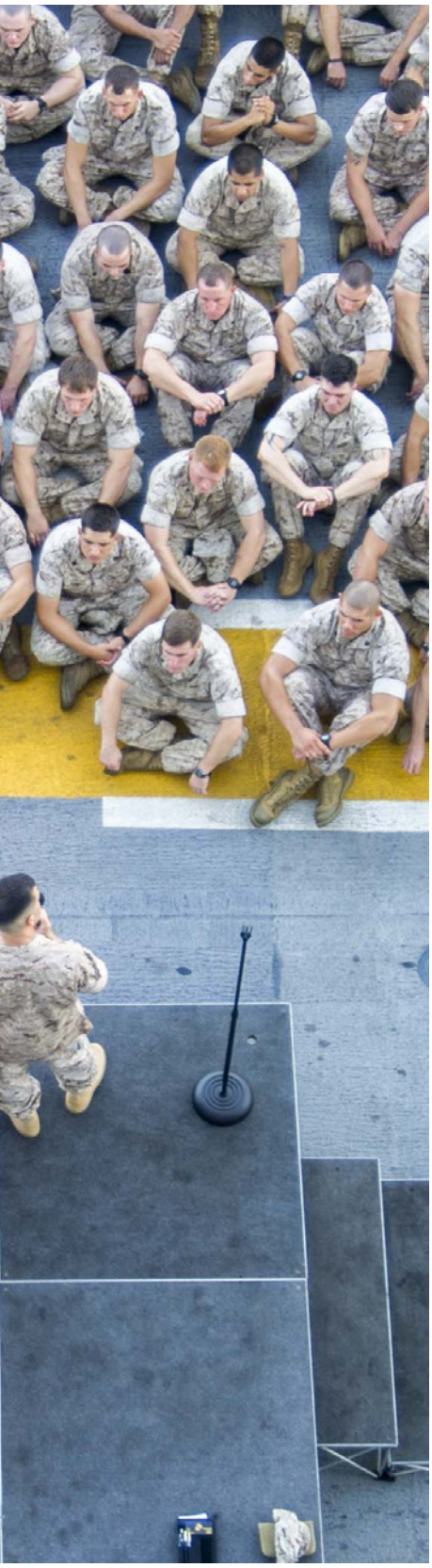
Enterprise services, which can include e-mail and file sharing, are essential to meeting JIE requirements. By providing shared enterprise services, department officials can reduce costs and mitigate the threat landscape, while providing services to personnel anywhere, anytime. This shared infrastructure is critical to JIE's success.

Providing enterprise services will be foundational to JIE. Enterprise services are necessary for the JIE framework. "Providing this consistent set of enterprise services will help ensure that Joint warfighters and their mission partners can discover, access, and use information assets to achieve mission success, no matter where the information resides," said a DoD report.

SINGLE SECURITY ARCHITECTURE

Establishing Single Security Architecture (SSA) will be imperative to the success of JIE. An SSA will help cyber operators gain valuable insights to their networks' status. It will also help create stronger responses to cyberattacks. With the standardized approach, DoD will be able to see who is using networks, spot abnormalities and provide better protection. A recent DoD report noted the benefits of deploying an SSA:

- Collapsing network security boundaries.
- Reducing the department's external attack surface.
- Enabling better containment and maneuvering in reaction to cyberattacks.
- Standardizing management, operational and technical security controls.



"The end result of establishing an SSA will be a set of capabilities that will enable DoD cyber forces to 'see, inspect, block, and collect' network traffic and provide the Joint warfighter with a trusted information environment," the same report stated.

NETWORK NORMALIZATION

With so many different networks and information infrastructures, collaboration becomes difficult at DoD. One of JIE's basic goals will be to normalize networks, which will provide an infrastructure to easily collaborate with internal and external stakeholders.

"Network normalization will reduce, standardize, and consolidate DoD's current system of disparate network, processing, and storage infrastructures, which currently are too diverse to protect and defend," a DoD report noted. "This incompatible, mixed environment also impedes internal and external collaboration and places warfighters and their support elements at the seams of integration."

CLOUD COMPUTING

For DoD, moving to the cloud is an essential component of JIE, but it still presents challenges such as management of thousands of pieces of hardware and software. The cloud is in many ways the glue of JIE, along with SSA and cyber initiatives. But cloud security has its issues. A DoD report highlights some:

- Achievement of real-time visibility into all cloud activities, where consumers do not have physical control over their systems.
- Implementation of continuous monitoring.
- Intrusion detection and alerts, as well as diagnosis and response.
- Agile acquisition of service and sustainment funding.
- Data migration and management.
- Reduction of network challenges for tactical-edge users.

DATA CENTER CONSOLIDATION

Consolidating DoD data centers is also essential, because it will improve the efficiency and efficacy of information networks. By consolidating data centers, the department will be closer to a standardized computing architecture. As part of the Federal Data Center Consolidation Initiative (FDCCI), DoD has been working to reduce its data centers from about 2,000 in fiscal 2014 to 100 by fiscal 2017. In addition, DoD is working to eliminate redundant applications and software by leveraging cloud technologies to share resources more effectively.

IDENTITY & ACCESS MANAGEMENT

With so many devices and personnel under DoD's control, knowing who is authorized and credentialed – a.k.a. Identity Access and Management (IdAM) – is essential for JIE. Some of the department's challenges include access control, authentication and directory services to seamlessly share contact information among units.

"The granting of access to authorized information to users on an automated basis will significantly reduce the intense manpower effort required today, while improving the control to and auditability of access to information across the network," a DoD report said. "The realization of a robust set of IdAM capabilities will provide the Joint warfighter and their supporting mission areas with secure, authorized access to all information and services required, regardless of location. In addition, it will increase commander confidence that their units have access to mission-essential information and services while maintaining the appropriate level of security for these information assets."

Although there have been obstacles, JIE has already seen some success in its deployment. DoD is moving full steam ahead with the framework. Our next section highlights how DISA will play an essential role in deploying the JIE framework.

> "Providing this consistent set of enterprise services will help ensure that Joint warfighters and their mission partners can discover, access, and use information assets to achieve mission success, no matter where the information resides."

solarwinds DLT SOLUTIONS®

IT Management & Monitoring **For Government** That's Powerful, Affordable & Easy-to-Use

SolarWinds® products are designed to solve the problems IT professionals face every day. With a continuously expanding product line, that can scale to meet your needs across your enterprise, we make the most cost effective, easy-to-use IT management software available, revolutionizing the way DoD and federal IT manage their operations.

SolarWinds eliminates complexity from every IT process imaginable, including:

- Network Management
- System Management
- Security Information & Event Management
- Database Performance

Our products are easy to buy, install, use, scale, and maintain, yet still provide the power to resolve any IT management problem.

No matter what your IT challenge is, we have a product that can quickly deliver results, whether it is **network operations**, **cyber security**, **data center consolidation**, **continuous monitoring**, **scaling to the enterprise**, or **compliance**, so you can do more with less.

IT Management & Monitoring Solutions for Government

Go to
SOLARWINDS.COM/FEDERAL
to Download Fully-Functional FREE Trials

Network • Application & Server • Log & Security • Virtualization • Storage
Help Desk • File Transfer • Database Management

877.946.3751 • federalsales@solarwinds.com • solarwinds@dlt.com • @SolarWinds_Gov

CREATING BETTER, MORE INFORMED DECISIONS THROUGH STREAMLINED ACCESS TO DATA

An interview with Chris LaPoint, vice president of product management, SolarWinds

The Joint Information Environment (JIE) promises to create a consolidated IT infrastructure across the DoD, helping to streamline access to data, provide access to computing resources, reduce costs, and improve the ability of DoD personnel to arrive at better, more informed decisions.

"JIE is similar to a company merger or acquisition, and those are never simple," said Chris LaPoint the vice president of product management at SolarWinds. "The challenges are going to be similar with JIE – having to merge the systems and processes together for differing organizations and systems. With that comes contention around which organizations have the best infrastructures, applications and processes that should be chosen as the new standard."

Since the program is not officially on record, DoD leadership must continue to express the value of JIE and encourage full support of the framework. "JIE has to develop from all its key stakeholders that have a vested interest in making it happen, so implementation has to come from existing budgets. Finding the resources to make it happen and prioritizing those resources will be major challenges," said LaPoint.

LaPoint also identified that although obstacles exist, there are nevertheless massive benefits from the system – one of them being that the military will now be able to take a holistic view around security.

"Given the increase of cybersecurity threats both internal and external, having a common set of technologies and processes is really going to be helpful," LaPoint said. "There are a number of other benefits that have been called out by the key stakeholders and drivers of JIE, including things like improved network performance, cost savings with consolidation, and time savings. Once they are able to reach consensus and drive towards a consolidated infrastructure, I think it will save a lot of money around training and ongoing maintenance of the infrastructure."

"You are not talking about everyone having their own flavor of monitoring tools or own security tools, so you will hopefully be able to have a set of best practices that will be shared across all the participants in JIE," LaPoint added.

Some of those best practices are very similar to any kind of IT deployment, LaPoint added. "You can take a pragmatic approach here and look at the steps like you would take to any system deployment as it relates to IT management. That starts with assessing your environment and taking an inventory of what's out there, and then mapping that to the systems that you're trying to deploy," said LaPoint.

SolarWinds' first focus for their clients has always been making their products fast, easy to use and affordable. The same is true in the manner in which they are supporting JIE deployment.

"We have been focused on selling and providing IT solutions to practitioners – the people who ultimately have to use the tools – so they need to be able to get the system up and running quickly for easy use," said LaPoint. "IT professionals shouldn't need extensive training and professional services to deploy IT tools. The newest monitoring tools are built to be installed, configured and used with little or no training. Solutions should then also be affordable, especially with an initiative like JIE, which does not have specific funding allocated."

"Continuous monitoring has really been one of the key discussions we have been having with our federal customers for at least the last two years," LaPoint added. "Being able to combine IT operations with information security tools is key to achieving low-cost integrated NetOps capabilities that will help deliver both a high-performing and more secure JIE."

"Consider log management and log consolidation – that's an area where IT operations has a number of cases of using log data to troubleshoot performance and availability issues," said LaPoint.

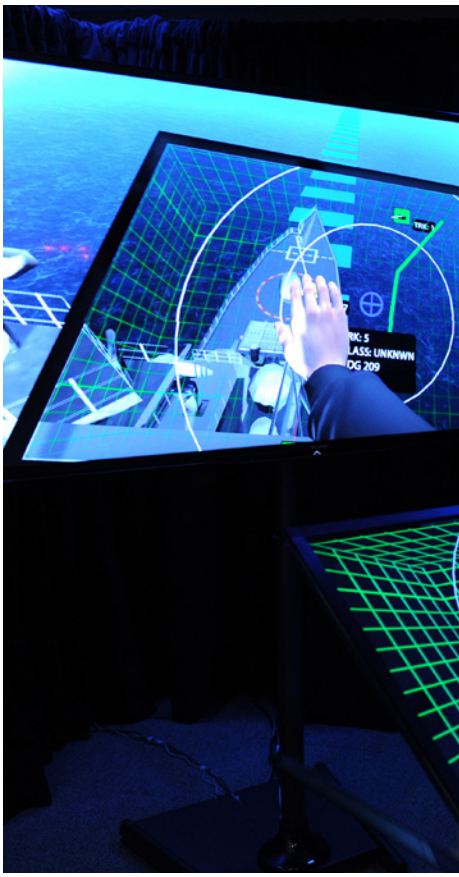
This log data can also be used to help solve security issues within the environment, so it makes sense for organizations to leverage the same tools.

"We've had a lot of success in getting the agencies to adopt that approach. With continuous monitoring, IT operations and InfoSec have a myriad of opportunities to work together – or as we guide our customers to do, collect once and report to many," said LaPoint.

With the help of SolarWinds, the DoD can accelerate adoption of the JIE framework, and help agencies streamline data to better protect their networks.

THE ROLE OF DISA IN EVOLVING JIE

There are three important factors to consider in deploying the JIE framework: governance, operations and technical synchronization. DISA has been granted authority to lead the technical synchronization component, and houses the JIE Technical Synchronization Office (JTSO). The office includes agency staff and representatives from military branches, the intelligence community and the National Guard.



DISA's strategic plan for 2014-19 calls for evolving JIE: "[We must] evolve a consolidated, collaborative, and secure joint information environment, enabling end-to-end information sharing and interdependent enterprise services across the department that are seamless, interoperable, efficient, and responsive to joint and coalition warfighter requirements."

DISA also provides key objectives to grow JIE. We share an excerpt below.

KEY OBJECTIVE 1.1

Implement and sustain an efficient, converged and consolidated IT infrastructure accessible by all means by any authorized user anywhere within DoD. To do this:

- Normalize networks with common standards with the intent to eliminate excess redundancy and legacy non-IP services to create an infrastructure of unified capabilities and everything-over-IP meshed transport.
- Standardize and consolidate computing infrastructure to maximize funding and offer better-valued services to mission partners through cloud broker-managed arrangements.
- Synchronize all efforts with JTSO to ensure proper execution of JIE increments.
- Establish JIE Core Data Centers leveraging the Defense Enterprise Computing Centers."

KEY OBJECTIVE 1.2

Develop Joint Enterprise Mission Assurance Solutions that expand and extend the security protections of the department's information assets focusing on solutions and capabilities while enabling authorized users to productively access needed information using any device and from anywhere in DoD. This means:

- Implement IdAM to enable secure access and eliminate anonymity from the network.
- Using SSA, harden the network infrastructure, enclave and host environments from cybersecurity threats by deploying the Joint Regional Security Stacks.
- Enable cybersecurity while focusing on enhanced mobility requirements of the enterprise."

KEY OBJECTIVE 1.3

Provide a portfolio of optimized and integrated enterprise service offerings that enable DoD-wide efficiencies and effectiveness, and improved responsiveness to dynamic joint and coalition mission partner needs.

- Employ a "DISA First" philosophy for piloting emerging enterprise services prior to expanding delivery beyond DISA boundaries.
- Expand delivery of enterprise services (i.e., milCloud, Defense Enterprise Email, the Defense Enterprise Portal Service and unified communications) to all services, agencies and activities
- Deliver foundational services (i.e., metadata registry, content delivery, identity management and joint user messaging) to provide a common core of infrastructure services that are critical to higher-level services, reusable components and applications.
- Establish a big data capability to handle the storage and analysis of data in excess of exabyte capacities.
- Establish an Airborne Intelligence, Surveillance and Reconnaissance Transport Service."

KEY OBJECTIVE 1.4

Promote rapid delivery and use of secure mobile capability, using commercial mobile technology to enable an agile deployment environment for new and innovative applications to support evolving warfighter requirements.

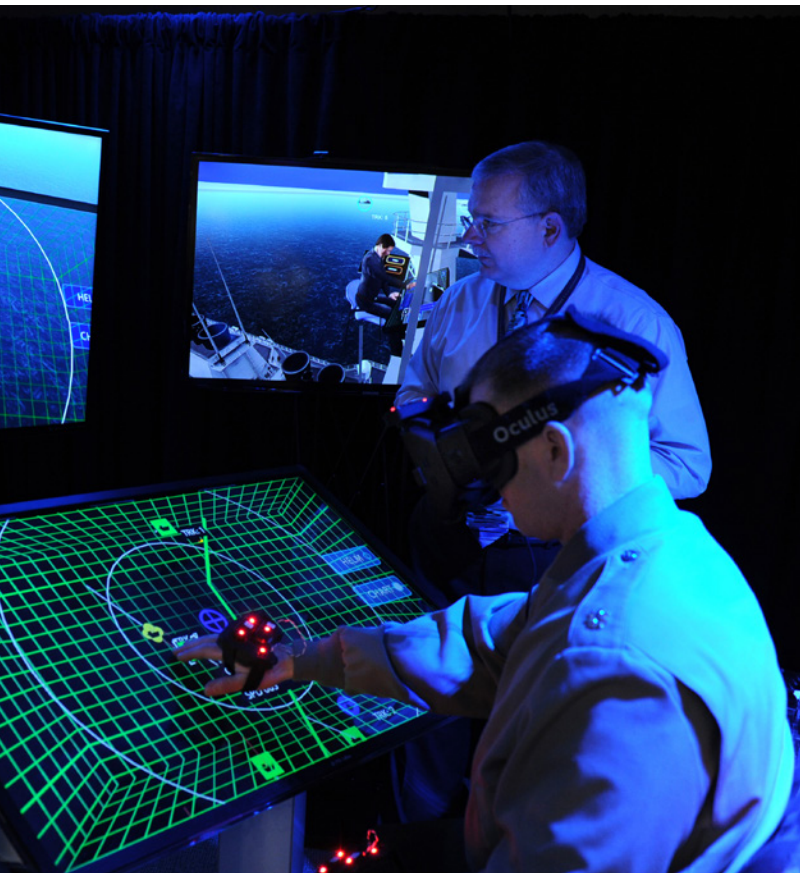
- Establish common infrastructure and services for unclassified and classified mobile solutions to enable the efficient application of mobile technologies to meet a wide range of DoD requirements.
- Establish security standards and a certification process sufficiently agile to keep pace with the rate of evolving mobile technologies.
- Provide a framework for management of applications to expand the capabilities available to users via mobile technology."

KEY OBJECTIVE 1.5

Provide a full array of electromagnetic spectrum services and capabilities ranging from short-notice, on-the-ground operational support at the forward edge to long-range planning.

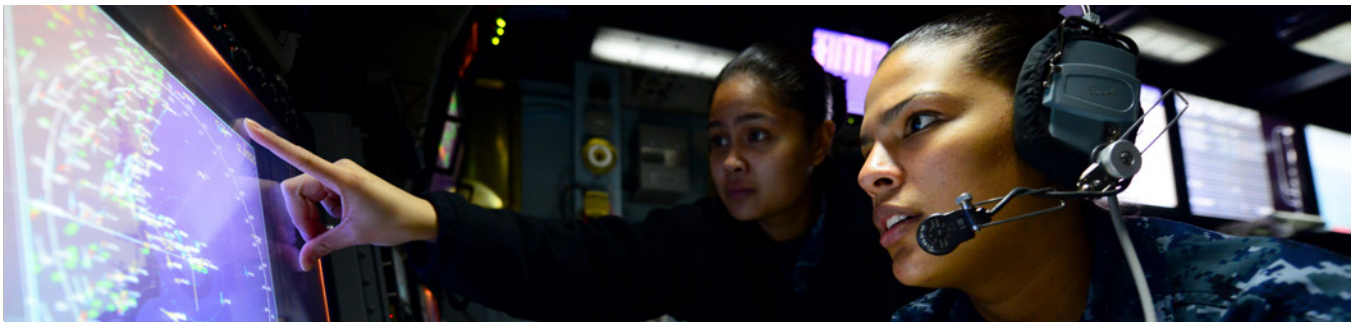
- Pursue national and international strategic objectives to ensure DoD's access to spectrum in support of warfighting capabilities with a view toward efficient, flexible and adaptive technology.
- Enhance quality and timeliness of operational spectrum management (SM) support for warfighting operations.
- Lead the development of comprehensive and integrated strategic and implementation plans, and an architecture to transform SM to support future cloud based operations and warfare.
- Perform SM and engineering analyses supporting national and international spectrum use initiatives to ensure DoD spectrum access.
- Implement, integrate and improve cloud-based SM services/capabilities and influence/facilitate the implementation of emerging spectrum technologies."

The impact of DISA has already been felt. In our next section, we explore a case study from Joint Base San Antonio, Texas, and how it has already made use of the JIE framework.



> "We see DISA as being that primary role for the integrator of how we bring the JIE into its operational capability for the warfighter" – Lt. Gen. Ronnie D. Hawkins Jr., Director, Defense Information Systems Agency, Fort Meade, Md, during DISA's Forecast to Industry Day in August 2013.

CASE STUDY: JIE SUCCESS AT JOINT BASE SAN ANTONIO, TEXAS



In September 2014, DoD took a step toward fully implementing JIE. In an Army press release, the department announced that the Air Force, Army and DISA achieved a big win for JIE at Joint Base San Antonio: now, data at the base moves across the same technology, rather than switching to different security points. This is the first time this has happened anywhere within DoD.

All online traffic from Lackland Air Force Base and Fort Sam Houston base — both in San Antonio — now flows through the Joint Regional Security Stack (JRSS). The new stack is expected to be fully operational by winter 2014 and network speed has already improved, the release stated.

"This is a tremendous step in terms of transitioning to a joint security architecture and making the Joint Information Environment a reality," said Mike Krieger, Army Deputy Chief Information Officer/G-6, in the release. "It also speaks to successful teaming by the Army, DISA and the Air Force and the Army's initial investment in this new joint capability."

JRSS will ultimately reduce DoD top-level security stacks from 1,000 to 50, noted the release. This helps achieve one of the main goals of the JIE: reducing the cyberthreat landscape to improve cyber efforts at a reduced cost.

"The JRSS Management Suite allows us to monitor and centrally control our security configurations," said Mark Orndorff, DISA's Mission Assurance Executive, in the release. "As new threats emerge, we can quickly assess the risk and more effectively mitigate identified risks across the enterprise."

As the program progresses, DISA will use the lessons learned in Texas for full-scale implementation across Army bases.

The Joint Base is one of many successful examples of JIE, which has also made substantial progress in Europe, Africa and the Pacific. The IT framework of the future is starting to become a reality for DoD.

MOVING YOUR AGENCY INTO THE CLOUD...

IT'S OUR BUSINESS.

ViON

Building your enterprise solutions

ViON Cloud Solutions has over a decade of experience making the cloud work for government agencies and world-class organizations. Our high-performance enterprise-class system combines the flexibility, efficiency, and power of the cloud with the safety of on-premise installation. Add that to our 24-7 customer care for a cloud-to-ground experience like no other in the industry today.

In partnership with

Hitachi Data Systems Federal Corporation

vion.com

THE KEY TO THE JOINT INFORMATION ENVIRONMENT: ON-DEMAND SERVICES

An interview with John Garing, vice president, ViON, and Richard Breakiron, senior director of cyber solutions, ViON

The Joint Information Environment (JIE) framework will build a modernized IT infrastructure at the DoD. It also aims to create federated networks built to common standards and configurations, which would allow the DoD to share infrastructure and enterprise services. These services could be everything from thin clients to email and cloud services.

The JIE framework will also reduce the cyber landscape and improve the way DoD protects networks and data. These services will provide the DoD access to computing, software or network services as needed, and on-demand. This will help to control costs and avoid purchasing costly IT infrastructure, while delivering both civilian and military personnel access to data to accomplish their missions.

But before achieving the desired end state of JIE, the DoD faces many obstacles and must deploy an advanced IT infrastructure, which includes providing an architecture to manage, secure and store data, delivering information through an on-demand model, in which DoD personnel can scale capacity as needed for services and leveraging a private cloud to securely move data and access applications.

Recently GovLoop spoke with industry experts from ViON, a company that works with the largest original equipment manufacturer (OEM) suppliers in the industry to design and implement custom IT solutions. They discussed how ViON is helping the DoD deploy the JIE framework with a flexible IT infrastructure.

"In every combat campaign, we always fight jointly," said Richard Breakiron, the senior director of cyber solutions at ViON. "We no longer fight as an Army, Air Force, Navy; critical to the joint fight is the management of information, so decision-makers can ensure soldiers, sailors, Marines and airmen are kept safe and out of harm's way."

Breakiron's statement underscores the importance of JIE, and how essential it is to create a converged IT framework to help meet the complex missions DoD personnel face.

One of the first objectives to creating the JIE framework is the ability invest in an agile IT infrastructure that can store, secure and manage data. "What ViON brings is storage on demand," said Breakiron. "Currently ViON does that as a service. For JIE, lots of investment is going to be needed, and the way around making a large investment decision is to go to industry and do it as a service. So rather than buying storage, you can say 'I don't know how much storage I need, but I want to start out and only pay for what I need every month.' Vendors now have the capability to do that for government."

By partnering with industry, the DoD can obtain access to cutting-edge IT, which can be deployed faster and more efficiently than if it the DoD attempted to purchase, deploy and then modernize solutions.

ViON also stresses the importance of the ability to provide information on-demand to end-users. "ViON has been a pioneer in the on-demand services delivery," said John Garing, the vice president of ViON. "We can take the lessons we have learned from contracts with DISA and use those on-demand models to take away the worry of over provisioning and having to buy infrastructure, and rather, provide services like compute, storage and network on-demand."

The importance of on-demand services highlights how the nature of the DoD's work has evolved, and why an agile and flexible IT infrastructure is essential. With frequently changing mission requirements, the DoD must be able to provide an IT environment that can quickly adapt to users needs.

"You can't build something that people aren't going to use," Garing said. With on-demand services, the DoD can offer solutions to what personnel are demanding, providing the necessary IT framework to achieve the goals of the JIE.

An additional piece of the JIE is the delivery model for information. Certainly, one core component of on-demand services will be cloud computing. "The cloud is a model of various flavors and various technologies, that simply provides a place for people to discover information, share and collaborate in its fundamental nature," said Garing.

Through ViON's private cloud offerings, DoD can create and acquire a private cloud based on their business needs and built to JIE standards. ViON offers technical expertise in the design, installation, configuration and maintenance of data center technology for a private cloud. With ViON's help, organizations can deploy custom on-demand services, which will empower everyone at the DoD to have access to the right tools to meet complex missions.

JIE MANAGEMENT

To help fully deploy JIE, the DoD CIO created a "JIE Management Construct Charter." The environment consists of several working groups and committees. At the top is the JIE Executive Committee, jointly led by the DoD CIO, Joint Staff and the U.S. Cyber Command's CIO. It sets the environment's direction, establishes goals and objectives, provides oversight, and maintains accountability, according to a recent DoD report.

Additionally, the committee provides strategic leadership and direction to several JIE working groups. A DoD report identified each:

JIE PLANNING & COORDINATION CELL (PCC)

Jointly led by the DoD CIO, Joint Staff and the USCYBERCOM CIO, PCC is responsible for synchronizing DoD components' actions to realize an integrated departmentwide implementation of JIE. PCC maintains an Integrated Master Schedule; tracks implementation plans; coordinates activities among governance, operations, and JTSO; and manages implementation issue resolution and execution.

JIE OPERATIONS SPONSOR GROUP

Led by USCYBERCOM, the group develops, integrates and synchronizes operational tasks and procedures in support of JIE that are integrated with existing department-level procedures. The group works closely with the JIE theater-level execution sponsors and coordinates and leads the development of operational concept of operations, tactics, techniques and procedures (TTPs), and standard operating procedures. It also identifies and makes recommendations on budgetary priorities necessary to support JIE operations, in coordination with Combatant Command Integrated Priority Lists and cyber component inputs.

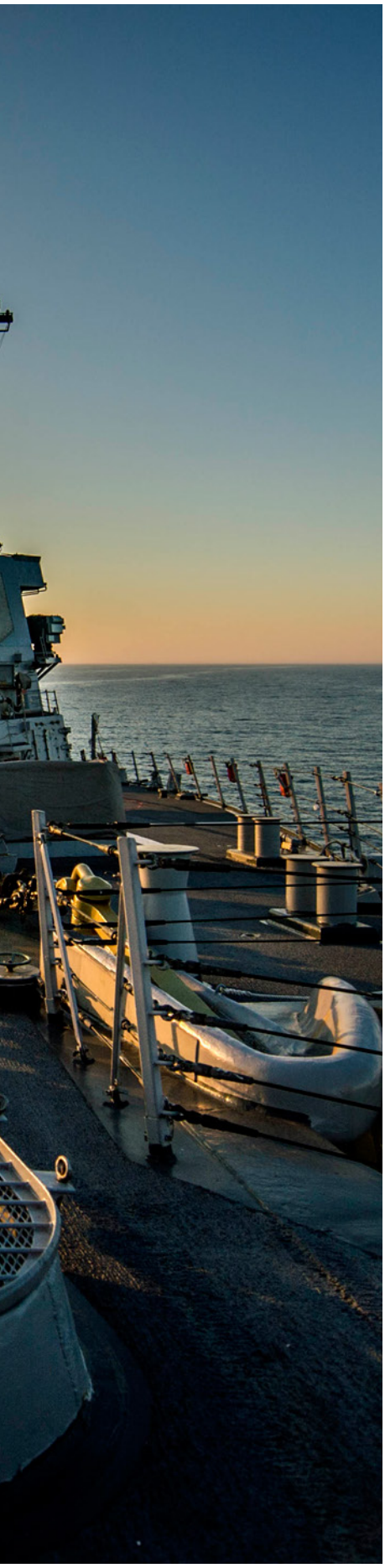
JIE JTSO

Led by DISA, this office serves as the technical and implementation lead for JIE and provides engineering and architecture direction. It works to realize an integrated, DoD-wide implementation of JIE by developing, integrating and synchronizing the JIE technical plans, programs and capabilities. JTSO leads the development of DoD technical specifications, designs and standards to enable JIE; assesses maturity of JIE capabilities based on tests of systems, services and products, and combatant commands, services, and agencies operational assessments of JIE TTPs at exercises; manages the technical portion of the department's JIE Plan of Actions and Milestones; and ensures that JIE security architecture development is designed to secure the infrastructure, provide access and allow cross-environment data sharing.

JIE GOVERNANCE GROUP

Led by the DoD CIO, the group is designed to align JIE to the department's requirements, budgeting and acquisition processes. It is responsible for policy compliance, capability validation, resourcing, program objective memos and budget decisions. It also provides the overarching plans, guidance and policy that inform requirements approval and is responsible for the development of the JIE Enterprise Architecture."

Although the management structure is important to consider, JIE is also affecting the DoD workforce. Next, we explore how it will impact both civilian and military personnel.



IMPACT ON WORKFORCE

The JIE framework will change the training requirements and necessary skills for the cyber workforce.

> To deploy the JIE framework, DoD will have to create highly skilled managers who are able to communicate across DoD, while understanding the complexity of operations. To accomplish this, DoD will need to provide training, certification and development opportunities.

TRAINING NEEDS

DoD is creating common training standards for personnel to take over classroom, online and on-range activities. But because one of JIE's goals is to reduce the cyberthreat landscape, DoD must work to attract, retain and train talented cyber professionals.

CIVILIAN SIDE

As JIE evolves, it will be essential to have talented civilian employees working on its front lines. To attract top talent, DoD faces obstacles in providing competitive salaries and benefits. What's more, many teams are already understaffed but cannot fill gaps because of weak budgets. Nonetheless, working for DoD provides an unrivaled experience in terms of projects and contributions to civil service.

Additionally, many in the civilian workforce will need to adapt to changes from JIE. For instance, acquisition professionals must learn to quickly acquire solutions and design contracts in ways that current procurement procedures are not designed to handle.

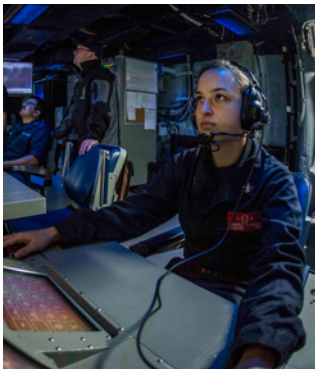
MILITARY PERSONNEL

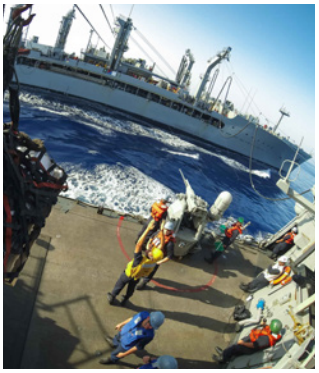
JIE will help military personnel better access the necessary tools and resources to achieve their missions. JIE is being created in response to new workforce demands and the necessity to combat a new age of cyber crimes. With the improvements to information management and security, JIE will ultimately create a leaner and more efficient workforce, able to meet mission needs in new ways.

CYBER WORKFORCE DEVELOPMENT

The cyber workforce must continue to be improved for JIE to be a successful project. "To allow for easy identification of like skill sets across the Components and with other federal agencies, industry, and post-secondary educational institutions, the Department must develop a set of workforce standards that align with the National Initiative for Cybersecurity Education (NICE), Cybersecurity Workforce Framework," according to a recent DoD report.

With more professionals equipped to combat attacks, DoD can improve joint operations and communications across teams, and define unified and standardized competencies and job descriptions for cyber professionals.





HELPING THE WARFIGHTER MAINTAIN A TACTICAL EDGE

An interview with Mark Wiggins, director of business development, DoD, at Juniper Networks

To improve the way resources are shared across networks at the DoD, the agency is implementing a unified command, control, communications and computing environment. Known as the Joint Information Environment (JIE), it will provide enterprise services and capabilities to DoD personnel. The JIE will be based on open standards and architectures, enabling more efficient use of cloud, storage and simplified data center infrastructures.

Juniper Networks, a company committed to network innovation, is helping the DoD to fully implement the JIE. Their technology supports the DoD with data center security, access control and hosted computing infrastructures, all available as certified products on the DoD Approved Products List (APL). The APL is a list of approved equipment that can be deployed on DoD networks. Prior to deploying any tool, the APL must be consulted to purchase an information technology solution.

To help us understand how Juniper can help deploy the JIE framework, we spoke with Mark Wiggins, Director of Business Development, DoD, at Juniper Networks. He provided insights on the challenges moving forward with JIE, and how Juniper can help overcome some common obstacles.

"One major challenge is piecing together the legacy components and leveraging the new capacity currently being built," said Wiggins. "What does modernization mean from an operational and policy standpoint? How is big data going to be analyzed to alert the cyber workforce of a potential problem? Those questions seem to be some of the challenges facing DoD leadership."

As DoD services become virtualized through the JIE initiative, workflows, operations and strategies all must be adjusted accordingly. As the unified environment is deployed, the DoD must continue to identify applications and services that will be transitioned to cloud and core data centers. As applications are virtualized, the DoD will be able to support mission outcomes in new ways, giving DoD personnel access to information more quickly, thereby helping them achieve their mission objectives.

Through the JIE framework, Juniper can support the DoD's task of providing access to information on any device, any time, under any circumstance, all to support DoD personnel during complex and often changing missions.

The JIE will also present many additional benefits for agencies and the DoD. "There is a consolidation of services and removal of duplication, that provides increased IT efficiencies," said Wiggins. "DoD will be able to leverage bulk buys, taking advantage of economies of scale from a discounting perspective from vendors. New IT deployed will enable greater situational awareness into the network. Ultimately, the modernization efforts will enable improved network operations for command and control for cybersecurity protection. Now cyber warriors will have insights and situational awareness into what is happening within the DoD."

For JIE success, Wiggins recommends that the DoD should think about strategies to flatten networks. "With innovative technology, leveraging Juniper, you can flatten the network to cut latency down in traversing the network from point A to point B," he explained.

"As a result you are able to have more dynamic cyber policies and changes to the network. As data centers are being consolidated, you are able to have more active management, scalability and dynamic allocation of resources based on what needs to occur to support mission success."

With JIE's unified approach to communications and technology, DoD will support on-demand access to IT services for mission support. The JIE will enable military units to gain access to information on demand. Once implemented, the JIE construct will provide the IT infrastructure needed to give the warfighter on the ground the tools needed to maintain a tactical advantage.

As Wiggins noted, scalability with the cloud is going to be critical to the success of JIE. With the scalability, organizations can deploy a pay-as-you go model to control costs. Although the cloud will lead to new insights and situational awareness, one critical element to consider is the identity management component of the cloud.

"If you have access into the cloud, you should only be able to go so far based on credentials, instead of having the keys to the kingdom," said Wiggins. "Identity management is very important for access based on your security clearance or mission sets, and is another key component within the scalability and cloud architecture."

Using the JIE, the DoD is moving closer to create a unified command, control, communications and computing environment. With Juniper Networks providing the IT backbone of JIE, the warfighter can maintain a tactical edge on the battlefield, and preserve the safety and integrity of confidential information.

ACQUISITION STRATEGY FOR DOD

We've noted before that JIE is not a program of record, and therefore, not an acquisition program. "This is an IT modernization effort that will consolidate, standardize, and optimize the design and architecture of the DoD's networks," stated a DoD report. The same report also reminds us of the need to move toward commodity IT throughout the department. This means deploying services such as cloud-based applications for storage, virtual machines or webhosting. One good example of this is the DoD's current cloud broker model, which helped expedite the adoption of cloud services.

JIE's desired end state of an integrated platform will eliminate disparate IT networks and architectures. A DoD report identified what will be core components of the JIE network stack, including:

- Network and computing services.
- Computers and mobility devices.
- Standard software loads on the computers and servers.
- Core machine-to-machine services, such as messaging.
- Global load balancing.

To fully realize the JIE framework, DoD must be able to rapidly and efficiently adopt the necessary IT components. One of the major issues that will also occur with JIE is achieving compliance. JIE will have to comply with the JIE Enterprise Architecture, defined by the DoD CIO. Compliance monitoring will be conducted annually and enforced by Milestone Decision Authorities and Investment Decision Authorities at the department.

With all these new solutions deployed to standardize and integrate services, security must be top-of-mind for officials.

"The program must integrate cybersecurity across all of this, from operating system configuration, to access controls, to perimeter defenses, to cyber intrusion detection and diagnosis. DoD will speed up the development, testing, and cybersecurity compliance of programs and systems by standardizing software development environments and integrating test and security evaluation capabilities that match the production platform. Programs will deliver faster and will inherit better cybersecurity," a DoD report stated.

By acquiring these new IT solutions and thinking about security from the start, DoD is well on the way to having the technical backbone to deploy a JIE framework.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 140,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

GovLoop
1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421
Fax: (202) 407-7501

www.govloop.com
Twitter: @GovLoop

ACKNOWLEDGMENTS

Thank you to DLT Solutions, Juniper, NetApp, Solarwinds & ViON for their support of this valuable resource for public-sector professionals.

AUTHORS:

Patrick Fiorenza, GovLoop's senior research analyst

DESIGNERS:

Jeff Ribeira, GovLoop's senior interactive designer,

Tommy Bowen, GovLoop's junior designer.

EDITOR:

Catherine Andrews, GovLoop's director of content

ATTRIBUTIONS

Thank you to the US Navy Official Flickr Feed for photography used throughout this guide. All image attributions and original sources can be found by clicking on any image in the guide.

JIE is an expansive program that is changing the way DoD operates. With its emphasis on protecting data and securing networks, JIE will enable all DoD personnel to make better decisions and access world-class technology solutions. As technology continues to evolve at unprecedented speeds, the JIE framework will enable rapid adoption of emerging technology and empower warfighters during mission-critical operations.

GOVLOOP
1101 15TH ST NW, SUITE 900
WASHINGTON, DC 20005
PHONE: (202) 407-7421 | FAX: (202) 407-7501
WWW.GOVLOOP.COM