CONNECTING THE MISSION OF THE DEFENSE DEPARTMENT TO YOU
Table of Contents

009
HARNESSING THE POWER OF HYPERSCALE CLOUD

010
INITIATIVE 01: FORCE OF THE FUTURE

013
HOW LEADERSHIP IS TAKING SHAPE AT DoD

017
IMPROVING NETWORK AGILITY IN THE DoD

018
INITIATIVE 02: JOINT INFORMATION ENVIRONMENT

026
INITIATIVE 03: DEFENSE INNOVATION UNIT EXPERIMENTAL

031
SOFTWARE-DEFINED NETWORKING IN DoD

032
INITIATIVE 04: UNITED STATES CYBER COMMAND

036
CONCLUSION

Table of Contents
EXECUTIVE SUMMARY
The Trump administration appears poised to give the Pentagon as much as $54 billion in increased funding in FY 2018. At the same time, former Defense Secretary Ash Carter has urged his successor, Gen. James Mattis, to continue important initiatives for the future of the Defense Department.

These include programs like the Defense Innovation Unit Experimental (DIUx), which connects DoD with startups and commercial tech firms in Silicon Valley and regional hubs like Austin, Texas and Boston, Mass. Additionally, Carter emphasized the importance of continuing DoD’s information-sharing initiatives, like Joint Information Enterprise, as well as cyberstrategy with Cyber Command.

On the personnel side, Carter highlighted the importance of continuing to train and recruit for the best-equipped DoD workforce possible through reforms like those under Force of the Future.

These four initiatives are some of the most frequently discussed Defense Department reforms. But while they all have ambitious objectives, how do they affect the everyday DoD employee?

Whether they’re high-ranking military officers or civilian professionals, some who work at DoD may be wondering how these initiatives apply to the important work they do.

This guide will help. The following pages include high-level information for DoD employees who want to know more about important initiatives and how they connect to their work and the future of the Defense Department.

Additionally, this guide provides a survey of the GovLoop community of DoD employees and their thoughts and perceptions on these four particular initiatives. The results revealed that the majority of those surveyed do not understand how these initiatives pertain to their work but want to learn more.

By gaining a better understanding of these four initiatives, Defense employees can better grasp how they are affected, and navigate the future of DoD under a transitioning administration.
According to a recent survey of 877 federal employees conducted by the National Treasury Employees Union, nearly 81 percent said morale at their agencies was declining or getting worse. That means it’s more important than ever to help employees, whether military or civilian, feel connected to the missions of their agencies and government.
To get a pulse of the Defense Department community regarding the four major initiatives, GovLoop conducted a survey of 215 DoD personnel (Figure 1). While the collection of participants in this survey represents only a snapshot of the overall DoD workforce, the results offer insight on a few of the challenges facing DoD employees.

When asked what the biggest challenges were in individual departments, the top responses were budgetary constraints (69 percent), followed closely by lack of skilled professionals with relevant knowledge and experience (53 percent) (Figure 2).

Most respondents rated the importance of these topics to individual departments or agencies as important or extremely important (Figure 3).

While the topics discussed above tie directly into the four initiatives, there may be a problem drawing the connection for employees and communicating this throughout the workforce. According to our survey results, the majority of respondents had little to no familiarity with the initiatives and saw little to no relevance to their individual department missions and jobs. (Figures 4-5-6).
Figure 1: What role are you within the DoD?

Figure 2: What are the biggest challenges you face in your department? (Check all that apply)

Figure 3: Please rate the importance of each topic to the mission of your department or agency

Connecting the Mission of the Defense Department to You
The survey results made clear to GovLoop that DoD employees overall were looking to connect their jobs to new initiatives and better understand the future plans for DoD. So this guide is dedicated to breaking down the basics of Force of the Future, JIE, DIUx and CYBERCOM and looking into the future of each initiative. Each initiative is summarized with five fast facts, a budget breakdown of the initiative, a summary of how the initiative affects employees and a look ahead to the future.
Wish You Were Here.

When NASA needed a company to handle mission critical data from Mars - it turned to Amazon Web Services. Come see what AWS can do for your agency’s data.

aws.amazon.com/government-education
https://aws.amazon.com/nasa
HARNESSING THE POWER OF HYperscale CLOud

Cloud computing is growing as a popular technology option for government agencies. However, defense sector agencies have yet to harness its full power, leaving them unable to reap the benefits of cloud technology, such as improved mission effectiveness, cost savings and efficiency.

To understand how defense organizations can better harness the power of cloud, we spoke with Jennifer Chronis, General Manager of DoD, and Jim Caggy, Manager of DoD Solutions, at Amazon Web Services (AWS). AWS provides a hyperscale commercial cloud for government agencies, including defense organizations.

Chronis identified three primary challenges to successful cloud adoption in DoD: outdated acquisition procedures, perceived security concerns and cultural resistance.

When trying to procure the on-demand, scalable services of the cloud, finding the right solution is only half the battle. DoD contracting officials also must select the right acquisition approach which can differ from traditional IT procurement. Whereas traditional IT procurement requires agencies to make large upfront investments in hardware and capital expenditures, the cloud provides a pay-as-you-go model so agencies only buy the computing capacity they need, and use it only when it’s required. Caggy also cited the lack of DoD-wide acquisition vehicles for mission owners to access the cloud.

Perceived security concerns also create a barrier to cloud adoption. Not only do employees have misconceptions about security in the cloud, DoD’s strict and lengthy security protocols also present challenges.

Finally, for many senior leaders, moving to the cloud is a major shift from the way they currently manage IT. Not only are they managing an elastic technology, they’re also required to retrain the IT workforce and make the business case for the move to the cloud.

Hyperscale commercial cloud can help DoD agencies overcome these challenges to make the most of cloud solutions. AWS cloud has security built into it, taking many of the security concerns off the hands of IT administrators. It has an extensive range of federal security certifications, including FedRAMP and DoD SRG, and leverages the AWS partner ecosystem of security-focused partners.

To help public sector agencies select the right acquisition approach, AWS offers a Cloud Buying Guide to walk customers through the steps they need to take to migrate to the cloud. The guide also helps customers leverage existing contract vehicles that have already been used in other parts of the federal government.

Finally, Chronis and Caggy addressed the culture challenge of cloud adoption, citing how important it is to educate and train customers. As cloud adoption increases, IT professionals will need to learn different strategies to operate in this new environment and skills they didn’t have in the past.

In addition to helping agencies confront these challenges, hyperscale cloud provides the agility and cost savings that defense organizations need.

Organizations can leverage hyperscale commercial cloud resources and deploy servers and IT resources in minutes, using only the technology they need at that moment. This prevents IT customers from “over-provisioning” resources to ensure they have enough capacity to handle what they need to do at peak opportunity. “By leveraging hyperscale commercial cloud, our customers only have to provision the amount of resources that they need, knowing they can scale up or scale down,” Caggy said.

Hyperscale cloud also allows customers to trade capital expense for variable expense. The variable expense is much lower than what they would be able to get on their own due to the economies of scale.

Chronis and Caggy also shared examples of how defense organizations are already reaping these rewards. For instance, after the U.S. Navy moved all of its public facing websites to AWS, they saved almost 60 percent over what it would have spent hosting on-premise. In addition, the Air Force Special Operations Command uses AWS to store data and makes it more readily available to post schedules and make them more open and available to those who need them.

In conclusion, Chronis highlighted the benefits AWS provides. From the rate and pace of innovation and the breadth of services to having the largest ecosystem in both customers and partners, AWS ranks high in its length of experience. “We really do believe that using hyperscale commercial cloud effectively becomes a mission enabler for DoD,” Chronis said.
Initiated under former Secretary of Defense Ash Carter, Force of the Future is an eclectic group of initiatives to maintain the DoD’s competitive edge in bringing in top talent to serve the nation. There are six links of the initiative, including maintaining DoD’s competitive edge, strengthening family benefits, improving the officer promotion system, attracting top civilian talent, expanding and enhancing military recruiting and reinvigorating the Reserve Officer Training Corps.
To address disproportionate geographic representation, Force of the Future includes a plan to use a Joint Advertising Marketing Research and Studies program. This program would help develop a new DoD-wide marketing campaign on the value of military service, build recognition of the DoD brand and grow propensity to serve.

In what was considered the most controversial policy proposal of the initiative, Carter called for permanent authority to allow experienced civilians in critical career fields, like IT or cybersecurity, to join the military as commissioned officers. While this was seen as a move to bring in necessary knowledge and expertise, critics questioned whether a civilian with only basic training could adapt as a military leader.

The secretary of a military department would be automatically authorized to approve an officer’s request to be temporarily excluded from consideration by a promotion board. This would allow officers to undertake activities to deepen expertise or pursue enrichment opportunities, without adverse impact on career advancement. For example, an officer up for promotion could ask to defer in order to first pursue a Ph.D. program.

Currently, civilian employees don’t receive any period of paid parental leave. In an effort to strengthen family benefits, Carter pushed for six weeks of paid parental leave that could be used within 12 months of a birth or adoption placement. But the proposal requires legislation to become effective. As for the Navy and all other military personnel, the second link provided for 12 weeks of paid leave for women and 14 days for men. Additionally, there would be an expansion of mandatory hours for on-base military child-care facilities. In an effort to improve recruiting efforts, one of the newest links called for the development of young women to serve in open combat and more effective recruitment of women, Hispanic and black youth.
Force of the Future proposes significant changes to expand promotion flexibility and potentially pave the way for experienced civilians to skip years of military service. This would allow civilians to immediately join the military’s upper ranks after boot camp.

While lateral entry and paid family leave would have some of the most significant impacts on employees, Force of the Future would certainly change the game in terms of talent management. One of the main proposals would require congressional approval to change the “up-or-out” system that limits the number of times an officer can be passed over for promotion before being forced to leave the military. Under Force of the Future, promotions would be based more on experience and performance rather than time in grade.

Carter envisioned the overhaul of the current lineal numbers system, where lineal numbers are usually assigned to officers based on seniority. Instead of having officers selected for promotion wait until a spot opens up in a higher rank, senior officers would be able to promote the highest performers on a merit-based system.

Under Force of the Future are several changes to current policies. First, there’s On-Campus Direct Hire Authority, which allows DoD recruiters to directly hire civilian employees from college campuses rather than having them go through the entire USAJOBS process. Then, there’s the Two-Way Talent Exchange with the private sector, which allows DoD civilians to spend up to six months in private industries to develop talent and knowledge.

One of the largest criticisms of Force of the Future was a problem articulating the exact cost. While many of the proposed reforms are low- or no-cost, others like graduate programs and sabbaticals would be more expensive. Estimated costs for sabbaticals and graduate programs were over $1 billion per year. The FY 2018 Defense budget, however, allot $142 billion on military personnel. This is a 3 percent increase from the previous administration.

Many thought Force of the Future was dead after President Trump was elected. But as of March 2017, the initiatives were being rehashed in the email chains of the Joint Chiefs of Staff, said Air Force Maj. Miriam Krieger, a special assistant to the Joint Chiefs of Staff.

“There’s value in the Force of the Future report. There is data, there are anecdotes, there are solution sets and framing constructs that people are finding useful. Now that some of the emotion has drained from the conversation, people are returning to it with a fresh eye and they’re recognizing the value added of that report,” Krieger said.
Leadership is tailored to an organization’s context, culture, climate and character. Defense Department leadership has evolved through a combination of discipline and training, military camaraderie and mission accomplishment.

And for today’s DoD, navigating ever-evolving challenges — like cyberwarfare, the Internet of Things and big data — requires strong leadership that embodies such qualities. In an interview with GovLoop, Greg Gardner, a retired U.S. Army Colonel and Senior Fellow at George Washington University’s Center for Cyber/Homeland Security, discussed the important leadership lessons he’s learned through his experience; challenges that military and civilian employees must navigate and how he sees the future of the DoD playing out with the digital and data-driven world we live in.

As someone with over 30 years of government service and IT experience who is now working for a technology firm, Gardner uses what he’s learned to help DoD organizations adopt the best practices and insights that the private sector and the intelligence community have to offer. He previously served as Deputy Chief Information Officer [CIO] for the intelligence community, where he assisted the CIO in developing the information management systems that enable an agile intelligence enterprise.

During his final military assignment, Gardner developed the prototype of the Joint Protected Enterprise Network (JPEN) that enables force protection information to be securely shared among DoD organizations. What has been most helpful is keeping a pulse on his teams, the organizations he leads and private-sector innovation.

For Gardner, leadership is not just about being ahead of the digital world. Leadership is about listening. “The most important thing to be a good leader within the government and military space is the willingness to listen to others, particularly your subordinates,” he said. “You have to recognize that you aren’t the cornerstone on good ideas, but that you can find them throughout the organization.”

Specifically, Gardner highlighted the importance of not just listening to others but listening to the “rhythms” of the organization you’re leading. This means being in tune with what’s going on in the organization, what changes need to be made and what those changes drive in terms of outcomes. Listening also means being in tune with what’s happening in government, as well as the private sector.
FINDING THE FISHERMEN FOR BIG DATA

With DoD networks under constant attack, officials have been at pains to develop necessary defensive measures. One approach is to leverage big data and associated analytical capabilities, which can play a large role in defending against a vast array of attacks.

Harnessing big data and analytics is a significant challenge for people in all levels of government, but particularly in the military, Gardner said.

“The difficulty with data analytics lies in integrating different sources to get benefits from that data,” Gardner said. “You have the challenge of deciding what is useful and what’s not.” Leaders in the DoD are tasked with finding the right people to sift through and leverage the data they collect. One analogy Gardner used to summarize the challenge of data is water and fishermen. “Data as water is pooled in puddles, ponds, lakes or oceans, and you have to figure out how that data moves,” he said. “Think of streams and creeks as different data stores. If you really want to mine the data properly, you need a fishing guide to that certain body of water to help you learn how to ‘fish’ there.”

What will be especially challenging for the DoD workforce is operationalizing this analogy. Where can the Defense Department get these “fishermen” or data analysts?

For developing the best workforce, Gardner emphasized the importance of collaboration with the private sector. In fact, DoD has already started to adopt the same big data techniques used by businesses to mine databases and glean more information from different types of data.

Humans can analyze some of this information, but there’s more to be mined from the thousands of gigabytes being continuously generated.

Computer analysis can handle mundane tasks, freeing personnel to do tasks that better fit their talents. As DoD staffs train to be better data analysts or “fishermen,” leaders need to make sure they’re helping equip their staffs to monitor and understand inputs while computer analysis does the work of highlighting potential areas of interest.

COLLABORATION WITH INDUSTRY

The DoD’s mission is to provide U.S. security with up-to-date technology and industry innovation. Logically, leaders across the department should consider close collaboration with their private-industry counterparts.

Gardner praised the FY2016 National Defense Authorization Act for giving DoD authority to bring private-sector experts directly into the department. “That’s a good start,” he said. “The challenge for DoD is executing closer collaboration with the private sector. It is not easy, but as Secretary Mattis and his team face the challenges of a very uncertain world, they will need to evolve decision-making processes based more on digital products than the output of industrial systems. The private sector can help with that.”

While the role of private-sector collaboration with the DoD is complicated, particularly when it comes to acquisition rules, there are still many ways that leadership can work with industry. Again, listening plays a key role, but effective Defense leaders also find ways to bring their private-sector counterparts to the table and engage them in fruitful discussions.

“The DoD needs to have more discussions with industry, Gardner said. “Government leaders are often hesitant to talk to industry on specific details, while industry leaders can be afraid to open up for fear of abetting their competitors. But we need to have real substantive discussions between industry and government if we are to effectively grow our Defense capabilities.”
Finally, Gardner had three best practices for DoD leaders and employees alike to start applying in light of the digital economy, big data and collaboration with private-sector counterparts:

### LEADERSHIP BEST PRACTICES

**#1 LEARN EVERY DAY.**

Study data management and how it fits into your profession.

**#2 UNDERSTAND THE CHALLENGES OF THE DIGITAL FUTURE.**

Accept the increased pace of the digital future and remain abreast of current and emerging trends.

**#3 GET USED TO SPEED AND CHANGE.**

Agencies like the DoD need to be ready to modernize as quickly as the private sector.

Ultimately, leadership in the DoD means having an ear to the ground when it comes to the needs of their organizations as well as remaining in tune with what’s going on in the digital world. Harnessing big data and analytics will be vital to shaping the future of DoD. But by collaborating with private-sector counterparts and encouraging the growth of data analysts, the DoD can dominate its adversaries in the digital future.
Modernizing federal networks requires transformation. Federal agencies’ changing mission priorities require a shift in communication network architecture. But economic realities demand these network services in an environment of flat, or even shrinking budgets. Learn how agencies can meet these transformation challenges while balancing budgets and crucial mission needs. www.TransformingNetworks.com

Solutions that connect the federal government to the power of the digital world.
IMPROVING NETWORK AGILITY IN THE DoD

Shifting budget priorities force many agencies to balance the need to innovate with the cost of supporting outdated IT infrastructure. To achieve this balance, the DoD needs a simpler, seamlessly integrated network infrastructure to enable more agile configuration and increase mission response.

To improve network agility, defense agencies should consider multi-domain service orchestration (MDSO). MDSO is end-to-end service automation across multiple technology network segments – physical or virtual – and vendor domains. Traditionally, creating and deploying services across an entire network in multi-vendor environments is a manual process. It entails collaboration with a multitude of vendors and domain-specific element managers.

“The biggest issue DoD IT personnel face is the ability to roll out services on a timely basis,” Bob Kimball, Chief Technology Officer of Government Solutions at Ciena stated. “Various vendors offer proprietary management systems for defense networks that are extremely complex. And the more complex these networks are, the more they cost.”

Disparate management systems and subsequent data silos also pose a threat to national security. When networks aren’t configured properly between these disparate systems, it can create gaps and errors leading to more vulnerabilities to cyberattacks. “You need to consider the security elements and how they tie into connecting the different networks,” Jonathan Barton, Director of Advanced Technology Solutions at CenturyLink, added.

In an interview with GovLoop, Barton and Kimball discussed how the DoD could overcome their network challenges and improve agility through MDSO. They also shared how Ciena and CenturyLink – two vendors who work to simplify the process of converging networks – are partnering to provide MDSO capabilities.

Critical mission applications in the DoD rely on a trusted, reliable and secure network infrastructure. DoD’s Global Information Grid (GIG), for example, is a globally interconnected end-to-end set of information capabilities for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support staff. In GIG, a number of vendors, cyber networks, data resources, satellites and radio capabilities are at play.

A satellite can help warfighters in the field access critical information and communicate with their agency’s chief data center back at central command. But if that satellite is destroyed, the warfighters would need to switch communications over to a commercial satellite before the mission is completely disrupted. However, due to the multi-vendor environment, configuring the network to connect back to that data center is an intricate, time-intensive process as IT personnel are managing numerous proprietary networks that don’t communicate with each other.

“[MDSO] allows you to solve that problem,” Kimball said. “You can quickly reconfigure the cyber aspects of the network, get seamless communication capabilities and accomplish the mission despite any damage done.”

MDSO enables users to control a number of different technologies from a single system, allowing for more seamless network connectivity. “MDSO allows you to set boundaries in the network and control things fluidly,” Barton said. “You can have a domain in a certain region or geographic area and route any type of infrastructure, network appliance or firewall.”

Through MDSO, DoD users have the ability to view all their networks from a single orchestration system, or what Kimball and Barton described as a “single pane of glass.” “The advantages to that single pane are rapid service creation and having services available when and where needed,” Kimball added.

To help DoD agencies enhance their networks through MDSO, Ciena and CenturyLink solutions support open data standards where multivendor, diverse protocol, and multi-layer networks can automatically share information.

“CenturyLink is using the technology capabilities that Ciena brings into our assets to optimize network situational awareness and allow enterprise wide coordination of DoD network resources,” Barton said.

Ciena’s Blue Planet division supports MDSO capabilities. Blue Planet provides an open software layer that eliminates management silos and enables network operators to automate end-to-end service provisioning and orchestration. “CenturyLink is using Blue Planet capabilities to enable our service to deliver network function to organizations,” Barton said. “We can provide managed services in the network in real time.”

In multi-vendor environments, networks must be able to communicate quickly and seamlessly. No matter what the crisis, be it on the battlefield or in the office, MDSO allows for agile configuration and communication capabilities. With MDSO, the DoD can ensure that network disruption doesn’t derail its most critical missions.
Initiated in 2013, the Joint Information Environment (JIE) was conceived under the Defense Information Systems Agency (DISA). The program optimizes the use of the DoD’s IT assets by converging communications, computing and enterprise services into a single platform. This platform can be leveraged for all department missions, including cybersecurity and enhanced communications.
The initiative is expected to cut costs by consolidating redundant capabilities at the enterprise level. For example, transitioning the Army to DoD enterprise email alone is saving the service an estimated $100 million annually.

JIE is DoD’s joint enterprise solution. With increased interoperability, the initiative will facilitate more efficient collaboration between joint forces, the ability to provide joint cloud services and reduce the cost of managing IT infrastructure. Core enterprise services, which are at varying stages of implementation, include email and mobile services, intranets and enterprise portals.

JIE will be managed by several soon-to-be established entities, including the Global Enterprise Operations, which will oversee the entire enterprise, and Enterprise Operations Centers, which will have complete visibility into their own portions of the enterprise. The services will continue to maintain their local infrastructure as well as support tactical units and service-unique missions.

Single security architecture can reduce the cyberattack surface by enabling centralized configuration management, along with standardized security implementations. Additionally, consolidating services at data centers will more effectively secure the enterprise. Rather than trying to defend everything, security can be focused on the systems and data needed to support specific missions and capabilities.

Mobile devices will provide access to the DoD Information Networks (DoDIN), allowing warfighters to operate within the JIE when and where needed. DISA plans to develop an unclassified enterprise Mobile Application Store that will deliver, update and delete applications on mobile devices. This way, the user doesn’t have to return to the device for service. MAS will have both commercially available apps and those created for exclusive DoD use.
JIE would help DoD employees communicate and collaborate more effectively. Through Unified Capabilities under JIE, Defense employees would have access to a broad set of voice, video and data-sharing capabilities. Additionally, the Defense Enterprise Portal Service provides a scalable, cloud-based collaboration capability that enables mission partners to share information through independently managed community and mission-focused sites. Through JIE, DISA has the capability to grow DEPS capacity to support the entire DoD. This would offer users easier workflows, access to DoD address lists, document libraries, team sites and calendars, SharePoint lists, Intranet sites as well as real-time collaboration.

According to the Defense Contract Management Agency (DCMA) Fiscal Year 2016 Budget Estimates report, the cost for JIE to make investments in IT equipment and "maintain some duplicate environments until transition is complete" was approximately $1.3 billion. Prior to unified capabilities under JIE, annual operations and maintenance at DISA were estimated to cost up to $500 million. In terms of savings, DISA-sponsored data center consolidation efforts have led to reduced Defense Enterprise Computing Center costs by $113.5 million annually for FY 2009-FY 2012.
LOOKING AHEAD

As of November 2016, DISA was preparing a $17.5 billion contract proposal for JIE. The RFP includes a plan for the enterprise contract, ENCORE III, which is a multiple-award contract to implement JIE. The agency plans to award 40 contracts – 20 for large businesses and 20 for small businesses. While a timeline remains unknown, ENCORE contracts typically last 10 years.

For personnel, JIE will help them access the necessary tools and resources to achieve their missions with easy access to a unified enterprise system from any location. It will also be essential to have talented civilian employees who are knowledgeable in cybersecurity working on the front lines. Many in the civilian workforce will also 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.

JIE is an expansive program that is changing the way the DoD operates. With its emphasis on protecting data and securing networks, JIE will enable all DoD personnel to better collaborate, make well-informed decisions and access world-class technology solutions.
In a recent program hosted by the Washington D.C. chapter of Armed Forces Communications and Electronics Association, **ACFEA Monthly Breakfast Program**, a panel of DoD leaders discussed how the DoD and military services are using big data. Additionally, they discussed the underlying technical challenges in acquiring, processing and analyzing big datasets, as well as how AI and data munging are helping.

The panel featured leaders from across DoD, including:

- **Tom Michelli**, Acting Principal Deputy, DoD
- **Margaret Palmieri**, Acting Director, Digital Warfare Office, U.S. Navy
- **Mark Kryzsko**, Deputy Director for Enterprise Information, Office of the Under Secretary of Defense for Acquisition Resources and Analysis, DoD
- **Jason Martin**, Services Directorate Executive, Implementation and Sustainment Center, Defense Information Systems Agency (DISA)

The diversity of Defense agencies on the panel alone demonstrated that big data is used to support a variety of missions and goals. For Michelli, his priority is using big data to drive efficiencies and cut costs for the department. For Kryzsko, big data is helping his teams support acquisition business processes, decide on more efficient programs and subsequent resourcing of those programs. Palmieri said the Navy is looking at ways to manage data more effectively to train sailors and help them access important information in real time. And as for Martin, DISA is focusing on its data centers and how big data can be optimized and integrated within joint enterprise systems.

As the Defense Department collects more information than ever, agencies across the board are seeing a number of benefits. Through artificial intelligence (AI) and data munging (compiling data into valuable portfolios) DoD is using big data to glean information and provide insights across a variety of domains – from intelligence to personnel readiness to logistics to cybersecurity.
The hardest part of big data is making good use of all the information that DoD collects. The panelists shared the many technical challenges they face when figuring out how to use massive amounts of data to improve services.

"[At DISA], our biggest challenge is requirements," Martin said. "We have to figure out what we need, what do we already have and how do we provide [better services]? That requires using common language, common datasets and leveraging the data to the service components."

Kryzsko had similar challenges and questions for using data to improve procurement processes. "We’re focusing on efficiency and effectiveness," he said. "How can we share that data and use it at the same time?"

MUNGING OF DATA

One way to start making sense of massive amounts of information is to munge the data. Data munging is the process of transforming and mapping data from one raw data form into another format with the intent of making it more valuable for analytics. Or, to put it into simpler terms, data munging is the cleaning up of datasets.

"The munging of data is complex," Kryzsko said. "It’s more than tools. Context also matters and we have to consider all the cultural perspectives. We need to think about datasets that are business-based and form technical partnerships with the private industry."

Data analysts will play an important role in data munging. "Tools are one component," Martin said. "But training and developing the data analyst is key to understanding situations."

We get the nuggets we need from the datasets and get the right pieces to the right people. Artificial intelligence helps us aggregate the data and apply different levels of classification.

THE ROLE OF ARTIFICIAL INTELLIGENCE

Another strategy that has been helpful in speeding up the analysis and classification of big data is AI. "AI is machine learning," Michelli said. "We get the nuggets we need from the datasets and get the right pieces to the right people. Artificial intelligence helps us aggregate the data and apply different levels of classification."

Machine learning has become a central focus in managing defense applications and data. In order to manage massive amounts of data from drone surveillance, Deputy Defense Secretary Bob Work recently announced the creation of the Algorithmic Warfare Cross Functional Team. The team, otherwise known as Project Maven, is charged with accelerating the Defense Department’s integration of big data and machine learning.

Managing the tsunami of incoming data and making it applicable to DoD missions and objectives pose significant challenges. But through innovative approaches like data munging and artificial intelligence, the DoD can develop a smarter, faster and stronger workforce.

"Our ultimate goal at DoD is to drive efficiency and effectiveness," Michelli said. The Defense Department is moving forward in developing more sophisticated enterprises and warfare tactics in the cyber, digital world we live in. As DoD makes progress, artificial intelligence paired with the ability to properly sort the data will play significant roles in achieving department missions and goals.
Solve for today, plan for tomorrow

Scalable, end-to-end IT monitoring and management software from solarwinds.com/federal
HOW NETWORK CONNECTIVITY CAN IMPROVE DoD IT

For defense agencies to fulfill mission-critical needs, their IT professionals need the right management and monitoring tools and processes. Branches like the Army, Navy, and Air Force can’t function properly without seamless communications, visibility, awareness, and security.

But DoD IT professionals face a number of challenges as technology becomes even more complex. Such challenges include budget and resource constraints, evolving security regulations and difficulty using increasingly complex IT products. How can DoD IT rise to meet these challenges while delivering mission-critical services?

The answer lies in comprehensive network visibility and connectivity. To learn more about the importance of comprehensive IT management tools and how network connectivity can help address DoD IT challenges, GovLoop spoke with Mav Turner, Senior Director of Product Management at SolarWinds. SolarWinds is an enterprise IT management software company.

“One of the big differences for DoD is their mission-oriented nature,” Turner said. “Their entire IT infrastructure is required for the mission, but must also be portable when the mission requires it. Due to the nature of IT deployment and how critical those capabilities are, a small mistake can have a big impact on the mission. In some cases, it can even be fatal for warfighters.”

That’s why it’s especially important for DoD agencies to seek the right tools and processes for ensuring network connectivity. Turner emphasized that visibility across your networks is one of the first key elements to delivering network connectivity. “You need to have that single pane of glass across all IT infrastructure,” he said. “This way, you can quickly identify problems in your networks and address them before they impact service.”

At the same time, networks must be manageable and easy to use for any level of IT expertise. “Individual management is key,” Turner said. “While technology’s getting more complex, a user should just be able to log into a screen and not have to figure out what all the blinking lights mean.”

Lastly, security is critical to network connectivity. An agency as large as DoD must be especially protective of its networks to ensure the safety of warfighters. “Security needs to be built into your alert management, automation and visibility components,” Turner said.

One recent example of DoD leveraging better network connectivity is the Warfighter Information Network-Tactical (WIN-T). WIN-T is the Army’s common tactical communications network backbone. It enables soldiers operating in remote and challenging terrain to maintain voice, video, and data communications.

WIN-T has deployed a range of SolarWinds network management, monitoring and troubleshooting tools, including Network Configuration Manager, Network Performance Monitor, NetFlow Traffic Analyzer, VoIP & Network Quality Manager, and Engineer’s Toolset. WIN-T selected SolarWinds because the solution met the program’s technical mission requirement and was more affordable.

WIN-T leaders strive to upgrade network operations and management in an effort to simplify operations. The network team needed call detail records of their VoIP calls in order to comply with Army Training and Doctrine Command. SolarWinds responded to support this requirement by developing a solution for aggregating CDRs, partnering with WIN-T to define and test the solution.

Automated network tools analyze network traffic, discover and map devices, manage and back up configurations, and monitor network communication and quality. These systems can immediately notify IT staffs of any issues before they become a problem. Additionally, the network tools are able to run on a variety of IT infrastructures.

“One recent IT trend we’re seeing is about 98 percent of public sector organizations have migrated some critical applications and infrastructure to the cloud,” Turner said. “Yet almost a third had to bring some back on-premises because of performance, security, and other challenges.”

Tools like those in SolarWinds’ network management suite offer what Turner described as a “sweet spot” in these hybrid environments. “These tools can improve the success of deployments by providing that hybrid IT single pane of glass. Users can see how their networks are doing on-premises, in the cloud, and can measure how those applications are performing before they even migrate,” said Turner.

While DoD IT will continue to face the challenges of increasingly complex technology, it is imperative that they ensure communications, visibility, awareness, and security—especially for warfighters. With the right network management suite, IT professionals, regardless of level of expertise, can deliver these results. Additionally, network connectivity tools are easy to use in any cloud or on-premises environment so that IT staffs and DoD professionals alike can meet their mission objectives.

How Network Connectivity Can Improve DoD IT
Established in 2015 by Carter, DIUx is an innovation initiative within DoD. It is meant to “increase DoD’s access to commercial technology, with the ultimate goal of accelerating innovation into the hands of the men and women in uniform.”
### FAST FACTS

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DIUx 2.0</strong></td>
<td><strong>NEW PARTNERS AND MODELS</strong></td>
<td><strong>NOT JUST R&amp;D</strong></td>
<td><strong>BUDGET IN FLUX</strong></td>
<td><strong>DIUx GUIDEBOOK</strong></td>
</tr>
</tbody>
</table>

**DIUx** was established as a conventional acquisitions shop that was three steps away from the top of DoD’s organizational structure. That meant any decision faced the same traditional barriers to acquisition – lengthy approval processes requiring sign-off from multiple parties. In May 2016, Carter announced an overhaul of DIUx after less than a year of operation. The plan included new leadership under entrepreneur Raj Shah and an organizational change that has Shah reporting directly to the Defense Secretary as a managing director.

So far, DIUx is seeing success in getting technology into DoD faster. In April 2017, Shah reported that 22 out of 25 contracts facilitated by DIUx were with “non-traditional Defense partners.” Twenty-one of those contracts were completed using “other transactions” (OT) authority, which expedited processing. The average time to completion of those projects was only 78 days, compared with the months – or even years – it takes to complete a traditional Defense acquisition.

While it’s easy to think of DIUx as another branch of DoD’s research and development efforts, DIUx leaders are adamant that they are more focused on changing the culture of innovation and acquisitions than actually developing new tech.

Last year, the House Armed Services Committee attempted to zero out the budget for DIUx. After OMB and the White House pushed back, the 2017 National Defense Authorization Act (NDAA) took a more tepid step at cutting funds by 20 percent. The act requires a more fleshed-out plan of DIUx growth, effectiveness and spending be presented to Congress before the full budget is released.

A **99-page e-book** titled “Fast, Flexible, and Collaborative: The Commercial Solutions Opening and DIUx’s Approach to Other Transactions for Prototype Projects” was recently published to help spread best practices and lessons learned from the initiative’s first two years of operation. It’s also meant to encourage other DoD components to adopt a similar acquisition style.
DIUx’s budget is comparatively small, with only about $30 million earmarked for the program in 2016. According to Shah’s calculation, DIUx has signed 25 contracts worth about $48 million within the large DoD budget. Nevertheless, spending seems to be on the rise, with more than half of those contracts signed in the last quarter of 2016 alone.

Moreover, it’s important to realize that DIUx’s purchasing power isn’t really in the budget. Rather, it’s in its ability to revise transaction authorities and procurement vehicles – allowing other components of DoD to spend their budgets more efficiently.

**BUDGET BREAKDOWN OF DIUx**

DIUx’s budget is comparatively small, with only about $30 million earmarked for the program in 2016. According to Shah’s calculation, DIUx has signed 25 contracts worth about $48 million within the large DoD budget.

**CONTRACTS**

25

**HOW DIUx AFFECTS EMPLOYEES**

Ideally, DIUx will help DoD employees – especially warfighters – get new and better technology faster. As DIUX’s Chief Science Officer Dr. Bernadetta Johnson explained, “One of the ways we can move faster … is to look at the commercial market. Ask, ‘What’s already out there now that is almost what we want, perhaps exactly what we want?’ That’s one way we can more rapidly transition things into the hands of the warfighter.”

The initiative identifies relevant technology that could aid U.S. military operations by soliciting solution briefs from private-sector developers. If a solution is selected, a more detailed proposal is fast-tracked under OT awards to the departments that could deploy them in real-life settings. Those departments work with DIUx to initiate a pilot test of the solution, allowing personnel to start using the tools as quickly as possible.

For DoD personnel, that means they can expect to acquire niche solutions more quickly, with less bureaucratic hassle when they use DIUx. But it’s not just frontline employees who will see the results of DIUx. Procurement professionals should also see the immediate impact of the innovation initiative.
In addition to creating new contracting vehicles for contracting officers to use in their own endeavors, DIUx is also providing training and the aforementioned 99-page guidebook. Shah said they’re educating acquisitions personnel to use new models, but also helping officers find more efficient ways to work within the existing FAR. Those training efforts are part of the greater goal of DIUx – to change the culture of procurement, rather than just acquiring a few tools.

The future of DIUx is uncertain, with Congress particularly questioning its value to DoD. Other critics have called out the fact that, despite its mission to introduce innovative tech into DoD, the group has primarily engaged with well-established industry leaders in contracting.

Nevertheless, Shah said the group has been advised by the Defense Department to move “at full speed.” Moreover, contracts continue to accrue through the program, even though the program isn’t currently accepting new solutions briefs.

It seems that DoD is committed to making acquisition more flexible and efficient, but the jury is still out on whether DIUx will be the way it does that.
Imagine your applications delivered, from any cloud.

Is your legacy Application Delivery Controller ready to support the digital transformation?

Network *wherever* you are.

Learn more at [citrixgbc.com](https://citrixgbc.com)
SOFTWARE-DEFINED NETWORKING IN DoD

DoD networks are undergoing major transformations due to the advancement of cloud, mobility and datacenter consolidation. Yet such transformation is putting serious strain on DoD IT staffs to respond with adequate network solutions — resulting in loss of productivity and mission agility. To compound these challenges, DoD agencies must also consider how they can modernize security for all their data, applications and endpoints on older legacy systems.

Moving to software-defined networking (SDN) can help defense agencies address these challenges all while improving mission responsiveness and decreasing costs. To learn more about how a software-defined approach can advance DoD networks, GovLoop sat down with Faisal Iqbal, Senior Director of U.S. Public Sector Sales at Citrix, a software company that provides server, application and desktop virtualization, networking, software-as-a-software and cloud computing technologies.

"Most IT shops are not built to be adaptive to trends like cloud and mobility," Iqbal said. "But this significantly impacts how DoD delivers its mission. That's why it's important to tear away from older systems and modernize to new ones. SDN helps virtualize many important functions while improving security and driving down costs.”

SDN also provides programmability and agility to government networks, enabling defense agencies to keep pace with user demands. In many DoD datacenters, traditional hardware network appliances perform a single function on-premise and are costly to refresh. In contrast, a SDN approach offers the same key network functions as hardware appliances, as well as the flexibility to migrate those functions across platforms both in the datacenter and in the cloud.

Today, DoD is starting to explore SDN solutions. Iqbal shared some tactics on how the department could do this effectively. "It's all about how the end-user consumes applications and data", he said. "The end user shouldn't care about networks. He/She cares if the application is easy to use, secure, available and performs well. The end game of deploying SDN is to ensure apps and services can be delivered to users as quickly, efficiently and securely as possible while ensuring a high-quality experience.”

Another important consideration is security. With cyberattacks becoming more application-centric, securing network infrastructure alone no longer provides adequate protection. A SDN approach ensures security is "native to the network" allowing concepts such as zero trust networks to become prevalent.

Equally important is addressing core backend functions, like switching and routing. These functions are usually hardware-centric in DoD networks, meaning the evolution to new capabilities requires a hardware refresh and when an application is migrated to cloud, the agency also has to buy a new set of capabilities for the cloud.

"Instead of repeating the vicious hardware refresh cycle, you need to take a step back and look at the whole picture," Iqbal said. "With an SDN approach, your ability to deploy apps and achieve high-level performance and functionality is the same on any infrastructure - be it on premise or in the cloud. This is especially true for App-centric Network Services beyond routing and switching such as App HA, SSL Proxy, App Firewall, DDOS Protection, and advanced analytics.”

To ensure agencies get leverage out of their next gen SDN architecture, Iqbal recommends ensuring their Application Delivery Controller platform is based on agnostic delivery infrastructure, like Citrix’s Netscaler. "This type of platform can take any application — regardless of where it lives - whether in a cloud, on premise or in a container and allow it to be delivered with high availability, security and strong performance across any network,” Iqbal said. "The agnostic part is key, as this allows agencies’ on-prem training, configuration and infrastructure investment to be leveraged for their network of the future without having to relearn technology or re-buy capabilities for the cloud.”

A software-defined platform agnostic App Delivery Controller offers agencies the ability to:

- Deliver any application securely regardless of form factor: on-prem, hybrid cloud or container.
- Provide App assurance, analytics and security for all mobile, web and windows based applications.
- Improve application performance for mobile, remote and branch users.
- Ensure network resilience for mission continuity.

DoD will continue to navigate significant challenges that come with cloud, datacenter consolidation, mobility and security. But software-defined networking helps defense agencies better secure their networks while having the flexibility to provide applications in any environment - be it the cloud or on-premise. Using a platform agnostic delivery infrastructure can help DoD IT leverage the best of SDN without having to invest in new and costly technologies. Ultimately, whether in the trenches of a battlefield or a datacenter, DoD users can better meet their mission objectives through SDN.
On June 23, 2009, the Secretary of Defense directed the leader of U.S. Strategic Command (USSTRATCOM) to establish a sub-unified facility, United States Cyber Command (CYBERCOM). CYBERCOM plans, coordinates, integrates and conducts activities to direct the operations and security of DoD information networks as well as cyberspace operations.
Wheelchair

NEW LINE
OF COMBAT

Last year, the Obama administration directed CYBERCOM for the first time to mount computer
network attacks alongside more traditional weapons. Specifically, these “cyberbombs” have been used on ISIS computer networks. Before, CYBERCOM was focused largely on Russia, China, Iran and North Korea – where cyberattacks on the U.S. most frequently originate. The goal of the new campaign is to disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions, like paying its fighters.

OPERATION-
ALIZING
CYBERSPACE

Cyberspace is a new warfighting domain, meaning CYBERCOM is expected to defend DoD networks, systems and information in addition to defending the nation against cyberattacks. Keys to operationalizing cyberspace include creating defensible networks, achieving and maintaining shared situational awareness, building cyber forces that are trained and ready and developing a command and control system that is agile, quick and integrated.

ORGANIZA-
TIONAL
STRUCTURE

CYBERCOM is currently a sub-
unified combatant command under USSTRATCOM. Its service elements include Army Cyber Command, Fleet Cyber Command, Air Force Cyber Command and Marine Forces Cyber Command.

DUAL-HATTED
COMMAND

Right now, the National Security Agency (NSA) and CYBERCOM share a leader. Adm. Mike Rogers is both director of the NSA and commander of the cyber unit. There has been much discussion, however, about separating CYBERCOM from the NSA to become a full-
fledged combatant command, and the separation seems imminent. While open to the possibility, Rogers said the benefit of the “dual-hatted” nature is CYBERCOM’s proximity to NSA’s elite hacking teams.

3 FOCUS AREAS

The main focus areas of the command are to defend the Defense Department Information Network (DoDIN), provide support to combatant commanders for execution of their missions around the world and strengthen our nation’s ability to withstand and respond to cyberattacks.
In order to promote CYBERCOM, Rogers is asking for a 16 percent increase in its budget. This would mean CYBERCOM needs a budget of $647 million. Money would be spent “building out” the command’s cyber fighting units, called Cyber Mission Forces, and other cyber-specific capabilities, Rogers said. The 6,200-strong CMF is on track to be fully operational by Oct. 1 next year, he said.

$647M
BUDGET NEEDED

6,200
CYBER MISSION FORCES
With the impending elevation of the status of CYBERCOM, there will be significant rearranging of leadership within the DoD. There is also a need to attract top talent to the agency’s cyber workforce.

What this means for DoD employees is that cybersecurity awareness as well as skillsets are a must. In 2016, the Defense Department began initial steps to create a new civilian cyber workforce outside the structures of the traditional civil service system, giving the department more flexibility to hire, fire and pay employees in critical cybersecurity positions. This initiative, called Cyber Excepted Service, sought to ask around 3,000 current employees to move from the traditional civil service system to one that offers fewer job protections but might also boost their pay and promotion prospects.

The legislation includes provisions that permit direct commissions of cyber personnel to be officers, similar to arrangements made for doctors and lawyers; expand an existing private-sector jobs exchange program for IT personnel to include cybersecurity personnel; and add a training requirement for human resources personnel to ensure they are aware of these new hiring flexibilities.

Additionally, there has been an intense focus on personnel manning the 6,200-person, 133-team force for CYBERCOM’s Mission Force. That’s why as of February 2016, DoD set up the Capabilities Development Group (CDG) at CYBERCOM. Its main mission now is development and fielding of what they call the Military Cyber Operations Platform (MCOP), Keith Jarrin, Executive Director of the CGD, said. MCOP is intended to be a “sum of portfolios that we manage” for cyber warriors, said Jarrin.

LOOKING AHEAD

Under the Trump administration, CYBERCOM is likely to be promoted out of its “dual-hat” status from under NSA and into its own command. Recently, the House proposed its fiscal 2017 Defense authorization bill, which calls for Cyber Command to be recognized as a unified combatant command.

The program would be elevated to function directly without Strategic Command or the NSA being involved, making it one of 10 such command centers empowered to carry out global defense missions. While the Senate was hesitant about this separation, Air Force Gen. John Hyten told the Senate Armed Services Committee that he and Rogers submitted their plan to the Trump administration calling for elevation of CYBERCOM sooner rather than later.

HOW CYBERCOM AFFECTS EMPLOYEES
As the Trump administration prepares to increase the Defense budget, it’s more important than ever to ensure the Defense workforce, both military and civilian sectors, remains engaged and motivated. In order to do so, employees need to understand the rationale behind important initiatives being discussed that could have significant impacts on them, including: Force of the Future, Joint Information Enterprise, Department Innovation Unit Experimental and Cyber Command.

By obtaining a better understanding of these four initiatives, the DoD community can better cope with changes. At the same time, employees can also better navigate their roles and individual departments and missions. Ultimately, a more informed workforce makes for a stronger Defense Department and a stronger nation overall.

CONCLUSION
THANK YOU TO AMAZON WEB SERVICES, CENTURYLINK, CIENA, CITRIX, DLT AND SOLARWINDS FOR THEIR SUPPORT OF THIS VALUABLE RESOURCE FOR PUBLIC-SECTOR PROFESSIONALS.

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 250,000 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.

www.govloop.com | @GovLoop

AUTHORS

Francesca El-Attrash, Staff Writer
Hannah Moss, Senior Editor and Project Manager

DESIGNERS

Kaitlyn Baker, Lead Graphic Designer
Marçal Prats, Design Fellow