

The Foundation for DoD Innovation



GOVLOOP
E-BOOK
2019



Executive Summary

Data informs decision-makers, and these leaders need networks that can get it to them. Take the Defense Department (DoD), where split-second information can mean the difference between life and death for warfighters. More than ever, these personnel are demanding dependable networks for their missions.

Unfortunately, legacy IT isn't meeting the needs of modern warfighters. Legacy networks aren't just struggling to provide agencies with active, intelligent data; they're also keeping them from having full visibility into their enterprise's applications, data and network operations.

Clearly, agencies such as DoD need a new medium for their data to maneuver on. Unlike their legacy counterparts, modern networks must act out the intent of the agencies using them. Furthermore, they must recognize the ties between an agency's applications, data and users; more importantly, these systems must seamlessly link these relationships to their agency's operational, strategic and tactical decisions.

In "The Foundation For DoD Innovation," we'll explain how DoD and other agencies leverage the power of their networks as a critical asset for achieving their goals. We'll also detail how organizations such as DoD can leverage the existing investments in their networks to use new, innovative architectures and solutions that are commercially available today. Finally, we'll interview DoD thought leaders about how federal agencies can make the most intelligent decisions possible by harnessing human, machine and sensor information with modern networks.

Just as the Air Force needs the sky, the Navy the sea, and the Army the land, active, intelligent data needs the modern network. The way that organizations use data during their operations, however, has changed worldwide. This e-book describes what capabilities this new era demands of networks. Ultimately, we'll explore the qualities that modern networks need to become the backbone of any agency's mission.

Network Modernization at a Glance

What impact does network modernization have on government and DoD? How does it help you achieve your agency's mission, and how has it evolved? These stats will help set the context for why network modernization is more important than ever for DoD and governments at all levels.

\$36.1 billion

The amount of total IT spending DoD has budgeted for fiscal year 2020, with \$6.5 billion (or 18.1%) going toward major investments and \$29.6 billion (or 81.9%) going toward non-major investments.

163

The number of Infrastructure-as-a-Service (IaaS) cloud efforts DoD had in fiscal year 2017. IaaS clouds provide organizations with IT infrastructure.

13

The number of Platform-as-a-Service (PaaS) cloud efforts DoD had in fiscal year 2017. PaaS clouds provide organizations with a platform to develop, run and manage their applications on without having to build or maintain the underlying IT infrastructures.

40

The number of Software-as-a-Service (SaaS) cloud efforts DoD had in fiscal year 2017. SaaS clouds provide organizations with centrally hosted software that is licensed on a subscription basis.

136

The number of cloud efforts DoD had in fiscal year 2017 that did not have a reported model. DoD also had 20 cloud efforts in fiscal year 2017 that were some combination of IaaS, PaaS and SaaS services.

1,266

The number of data centers DoD had in August 2017, including 200 closed through that date and 258 additional closures planned through fiscal year 2018.

\$46.4 billion

The amount of DoD's IT budget in fiscal year 2019, a time when the agency is operating the world's largest and most complex set of networks.

36%

DoD closed or planned for closure this percentage of its data centers through fiscal year 2018 as of August 2017.

372

The number of cloud IT projects DoD had in fiscal year 2017, up from 78 in fiscal year 2016 and 60 in fiscal year 2015.

50

The number of cloud products DoD had in July 2019 that were authorized or in the process of being authorized by the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP establishes the processes and security requirements that cloud vendors must meet to sell their products and services to federal agencies.

\$37.9 billion

DoD's amount of total IT spending in fiscal year 2019, with \$6.7 billion (or 17.7%) going toward major investments and \$31.2 billion (or 82.3%) going toward non-major investments.

10,000

DoD had roughly this amount of operational systems in fiscal year 2019, plus thousands of data centers, tens of thousands of servers, millions of computers and IT devices, and hundreds of thousands of commercial mobile devices.

1.3 million

DoD employed this many active-duty military personnel in July 2019, plus 742,000 civilian personnel and 826,000 National Guard and Reserve forces.

The 'Why' and 'How' of Network Modernization



In July 2019, Air Force Chief of Staff Gen. David L. Goldfein implored America's military to adopt a network that weaves together its multi-domain operations (MDO) to identify and defeat adversaries.

Goldfein said MDO would link land, sea, air, space, cybersecurity and information assets from the U.S. Armed Forces into one system. Initially, this network would gather massive amounts of data from each of these domains. From there, it would make all the information rapidly accessible, comprehensible and shareable for American warfighters. This networking would inform personnel, helping them quickly coordinate successful maneuvers.

"Victory in combat will depend less on individual capabilities and more on the integrated strengths of a connected network of weapons, sensors and analytic tools," [Goldfein said](#). "Where we are going, I believe, will change the character of modern warfare."

Goldfein added that the military's MDO network would be more agile, connected and resilient than its legacy version. The MDO network, he continued, would also rely more on artificial intelligence (AI) and machine learning to make faster, higher-quality decisions.

"People are on the loop, not in the loop," he said of the MDO system. "[Future decisions must] go beyond trade-offs between platforms, sensors and weapons ... and instead build integrated systems that allow us to close kill chains at speeds our adversaries can never counter."

AI involves machines imitating human cognitive functions such as problem-solving, while machine learning features computers using algorithms and statistics to perform tasks without explicit instructions. Both are emerging technologies that are widely considered crucial for tomorrow's warfare.

Regrettably, legacy networks such as those DoD and its military components use aren't capable of supporting MDO combat. These systems are costly, inflexible and impede innovation.

Let's examine how cloud can modernize networks and how this transformation impacts agency operations.

Reinventing Warfare With Modernized Networks

Whether it's DoD or civilian federal agencies, the problem with today's legacy IT networks is that they can't see the full scope of their enterprise's applications, data and operations.

With DoD, this network blindness has potentially lethal consequences. DoD's many civilian and military domains might be separated during the heat of battle; its manned and unmanned combat systems, meanwhile, might operate on separate decision loops. War has a thin margin between success and failure, and it's one that allows for few miscommunications.

Fortunately, cloud's scalability makes it capable of handling the dependencies between multiple applications, their data and the IT infrastructure supporting both. Overall, cloud can help agencies picture their entire enterprises; agencies that modernize their networks with cloud, meanwhile, can seamlessly link their operational, strategic and tactical decisions.

Active, intelligent data is the link between these various decision environments. Modernized networks take this information from humans, machines and sensors to enact their agency's intent. Intent-based networks help agencies make wiser, speedier decisions; they also support more frequent innovation agencywide.

For DoD, modernizing its network with cloud would assist with reinventing how offensive, maneuver and mass principles are exploited in combat. Modernized networks using intelligent, active data will:

- Alter the speed of decisions, generating cognitive superiority on the battlefield and adjusting offensive and defensive postures in near real time.
- Virtually and/or physically restrict an adversary's range of action by generating a new form of agility for carrying out simultaneous actions.
- Rapidly concentrate the effects of kinetic and non-kinetic force elements by generating new levels of synergy between both.

Transforming these principles, however, will require DoD to use a new foundation for its innovations.

Cloud can support these changes by unifying DoD's MDO data and hosting its emerging technologies. Let's examine how a modernized, cloud-based network looks at one of DoD's components.



The Future of Navy Networks With PaaS Cloud

Navy surface ships are incredibly complicated, with each one containing dozens of distinct systems such as propulsion and weaponry. Consequently, coordinating these disparate elements is one of the Navy's biggest challenges.

Take the USS Zumwalt (DDG 1000), a guided missile destroyer in one of the Navy's newest warship classes. Like older warships, the USS Zumwalt contains multiple networks, including alarms, fire suppression and steering. Unlike earlier warships, however, the USS Zumwalt's networks aren't disconnected silos.


Traditionally, many Navy networks are legacy systems separated from one another. Sensor networks, for instance, can't always exchange data with weapons networks. The resulting arrangement presents Navy crews with many problems – namely, they lack visibility into their vessel's full status. Furthermore, these legacy networks often operate in unrelated decision loops and can potentially cause confusion in pivotal moments.

The Navy is tackling these problems, however, with its Next Generation Combat System. Using PaaS cloud architecture, this system will modernize Navy networks for future warfare. For starters, it will combine data from formerly separate warship components into one whole. Next, it will coordinate formerly disconnected domains such as communications and radar. Finally, it will pull manned and unmanned systems into the same decision loop. Eventually, humans and machines such as AI will collaborate in real time.

In 2019, the Navy decided that its roughly 200 surface ships would adopt the Next Generation Combat System. The Navy will also require all its component programs that need IT equipment to migrate to this cloud solution going forward.

This decision leaves the Navy well prepared for emerging technologies such as the internet of things (IoT). IoT networks contain various devices that can connect to exchange, share and store data. By preparing for technology developments such as these, the Navy is readying its networks for change in the years to come.





DLA Enterprise Infrastructure Services Director: We've 'aggressively tackled' IT Modernization

The Defense Logistics Agency (DLA) manages the global supply chain for the entire U.S. military. Operating in most states and 28 countries, DLA needs a reliable IT network to handle information about the roughly \$37 billion goods and services it provides annually.

Few know this better than Dempsey Hackett, the director of DLA's Enterprise Infrastructure Services. Hackett leads DLA's team of 600 IT infrastructure personnel, and he's also responsible for the agency's network telecommunications.

During an interview with GovLoop, Hackett explained how far DLA's network must reach to keep its operations running smoothly worldwide. Hackett also shared what other agencies can learn from DLA's network modernization moves.

This interview was lightly edited for length and clarity.

GovLoop: How does enterprise visibility into DLA's networks help citizens and warfighters?

Hackett: The largest benefit directly supports our warfighter customers by providing them with consolidating reporting that addresses all their interactions with our agency.

For example, a few years ago, we went through a significant modernization effort associated with our [enterprise resource planning] (ERP) solution to add in energy commodities. These commodities were being managed through legacy systems, but to provide our service

customers with complete reporting, we added in fuels, electricity and natural gas into the solution.

Another benefit is auditability. We're able to provide single reports to an auditor. In turn, they give taxpayers some reassurances that we're being good stewards of the resources provided to DLA.

There are additionally some benefits associated with data standardization. It's our ability to have more streamlined and effective processes by minimizing the number of legacy systems and moving as many as we can into a smaller number of enterprisewide systems.

What obstacles is legacy IT creating for DLA's mission of delivering logistical support to warfighters?

A lot of legacy IT is expensive to operate, can pose cybersecurity risks and can hinder innovation. It's an area that DLA has aggressively tackled through our application rationalization project.

In 2013, we had about 1,308 distinct DLA applications. Through that project, we've driven that number down to about 194 applications. We realize that number is still very large, and we're continuing to try driving it as low as possible.

Another problem with these legacy IT systems is many were hosted in our on-premise data centers. By having more applications in those, you get all the other requirements associated with them. It's things like making sure that the heating, ventilation and air conditioning (HVAC) systems and the uninterruptable power supplies and monitoring are up and running. It's not really DLA's core business.

What are some best practices for modernizing networks that you would recommend to other agencies?

It all starts with having buy-in from a senior leader. We've been fortunate here at DLA. Our

former and current CIOs had that vision of where they wanted to take the organization and what capabilities that they wanted to provide. They took that vision and then they shared it with other senior leaders to gain buy-in.

We also can't forget our end users and their representatives. We want to make sure that we have a lot of strategic communications which cater to the change management process. We realized that you must do this through multiple venues because not everyone reads those helpful IT emails. We reinforced those messages with town halls, and at some of our various sites tech councils, which are composed of IT-savvy end users. You educate them about the things that are coming up, including the benefits and the capabilities.

It's additionally important to make sure that we keep our union representation up to speed on the changes and impacts to the workforce. It's key to make sure that our users understand the changes that we're making, and so we try to communicate about them in the greatest number of venues.

Finally, sometimes there's a balance between speed and ease of use with cybersecurity. There are times when you must make those tradeoffs. That's another area where we just need to make sure that we're communicating with our users

so that they fully understand the entire picture from all aspects. It includes their interactions with the system and the larger cybersecurity picture.

How do DLA's IT personnel help the rest of your agency's operations and workers using its networks?

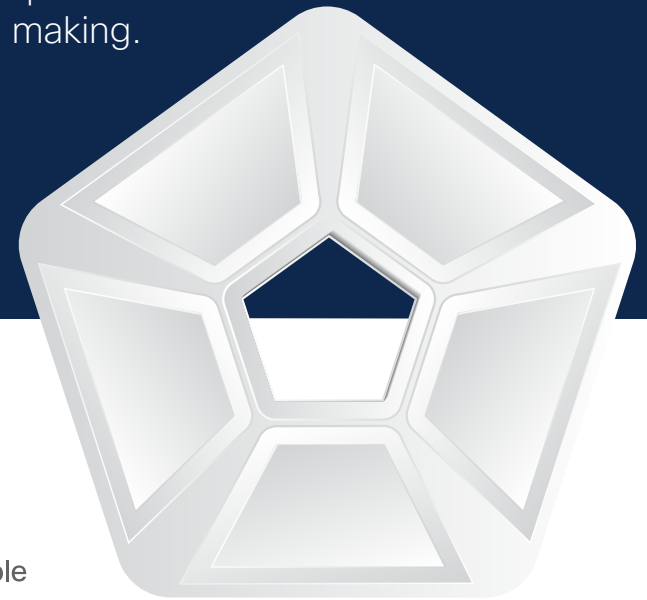
Within our IT organization, we consider ourselves enablers for DLA's overall logistics mission. The whole reason we're here is to support our agency, who can then in turn support the warfighter.

We have a 'whole of government' mission. For example, we support the Federal Emergency Management Agency [FEMA] in times of natural disasters. We have both DLA folks and even an IT contingency team that can deploy and set up communications in areas that have been devastated by various events.

DLA's director routinely reminds us that we have a global mission. We have folks in our agency across the entire world, and we've got IT folks out there supporting them to make sure that they can support our nation's only combat support logistics agency.

IT Modernization is now goal one for securing our nation

Why? Because the DoD is facing growing cyber threats, evolving mission landscapes and the need for faster, more accurate situational awareness for better decision making.



Tested and validated by Cisco for U.S. Defense.



Mission-grade networks

Your missions need strong, intuitive, and trusted networks—and a platform that never rests. **Get intuitive.**



DOD cyber resilience

Protect your data, from the flagpole to the cockpit. **Get secure.**



IoT +connected battlefield

The future of warfare depends on smart, highly secure and connected sensors/devices. **Optimize now.**



Collaboration for defense

Connect your teams to the people and resources you need, anywhere, anytime. **Secure communications.**

Dive deeper: Cisco.com/go/DoD



Modernizing Networks For Enterprise Visibility

An interview with Carl De Groot, Senior Director, U.S. Defense, Cisco

DoD calls itself “America’s largest employer,” and for good reason – in 2019, the agency employed 2.87 million people. Its workforce comprised primarily of military personnel totaling 2.15 million warfighters, an almost 3:1 ration to its 732,079 civilian workers.

With a work force of this size coupled with the magnitude and complexity of its mission, the DoD is working diligently to modernize its enterprise to support capabilities and requirements of the world’s most demanding work places. Modernization at this scale requires real time visibility to all assets both virtual and physical. This includes a comprehensive understanding of the dependencies between applications, their underlying infrastructure, and security posture. Without it, migration to new platforms such as the cloud is virtually impossible. And here’s the reality, the DOD like many other government agencies lack complete end to end visibility due to the ever-growing demands of a mobile workforce.

To help Federal enterprises address this ongoing challenge, next generation intent based networks help provide enterprise visibility. These platforms recognize the relationship between users, data, and applications seamlessly linking the strategic, operational, and tactical decision environments. The user is the “new firewall” who’s rights and privileges govern the applications and data they have access to. With policy enforced at a user

level, the network can now collect intelligence distributed throughout the battlespace – artificial, human or sensor - then aggregate, fuse and route information to create an ever-increasing advantage across various operations scenarios.

To understand how intuitive networks and platforms can boost an agency’s enterprise visibility, GovLoop spoke with Carl De Groot, Senior Director, U.S. Defense at Cisco. Cisco is a networking and telecommunications hardware provider specializing in enterprise visibility and modernization.

De Groot said that many agencies – including DoD – struggle to struggle to make data accessible across their enterprise. “Visibility is the No. 1 challenge,” he said. “The challenge is making data useable for agencies and understanding their environment.”

Visibility is especially critical to the DoD as its personnel needs a clear operational picture of their enterprise. Intuitive networks help agencies overcome this challenge by clearly illustrating a comprehensive view of all agency’s applications, data and operational systems. “In turn you build a more cognitive enterprise,” De Groot said. “It supports a more real-time operating environment.”

Intuitive networks and platforms are also flexible and scalable, making them ideal for emerging

technologies such as AI. Agencies that use the network to harness data can collect, analyze and share higher-quality information more easily.

Another advantage for agencies using intuitive platforms is that they can immediately adopt new applications, services and security measures as they’re introduced. For government agencies operating in a cloud smart environment, the network can save time installing, securing and upgrading their application infrastructure - cloud ready networks automate adoption of the latest platform enhancements as they become available.

“As a mediator, the network empowers the ability to connect and access data, to make it useable. You can share data more rapidly for better mission success.” -Carl De Groot

Providers such as Cisco, deliver cloud ready networks so agencies can immediately leverage commercial capabilities in the cloud, make data rapidly usable and support their missions with agile, adaptable toolsets. “The network remains more important than ever,” De Groot said. “Today’s network has to be highly useable and deliver a good user experience.”

Takeaway: Modernizing agencies’ networks with intuitive capabilities provide full visibility into their applications, data, operations and users.

Navy Cyber Security Division Director: 'We don't want stovepipes of information'



As one of warfare's newest arenas, cybersecurity is already changing military IT networks. These networks must keep data safe from the latest cyberthreats or risk exposing it to adversaries.

Enter people such as Rear Adm. Danelle Barrett, the Navy's Cyber Security Division Director, Office of the Chief of Naval Operations. Barrett – and other officials like her – work daily to keep the Navy's networks safe from harm. These networks not only help the Navy share crucial information over large distances, they also help its leaders make smarter decisions faster.

During an interview with GovLoop, Barrett described the Navy's cybersecurity challenges while modernizing its networks. Barrett also explained why modernizing these networks will drastically improve the Navy's future operations.

This interview was lightly edited for length and clarity.

GovLoop: How is the Navy's IT starting to complicate its mission as it ages in terms of network visibility?

Barrett: The Navy can't on a dime say, 'Well, I'm going to buy a new network and install it

tomorrow.' It's because we have ships all over the world, we have jurisdictions and we have, for example, legacy shore control systems. We've tried over the years to clinch together all these networks, because it's impossible to go in with a homogenized network tomorrow and just replace everything overnight. It's just not feasible. What we've tried to do, as best we can, is to make sure all these networks can share, talk and communicate.

However, sometimes different networks are funded and provided in different ways. Not

everybody modernizes at the same speed or gets their funding prioritized to modernize at the same speed.

The challenge becomes dealing with legacy infrastructure and state-of-the-art infrastructure. With legacy infrastructure, you're dealing with things that may no longer be supported by a vendor, and then you must have other measures put in place until those can be replaced.

Say the replacement is for a control system on a ship. Maybe the hardware associated with that piece of gear isn't going to get replaced on that ship until the ship is replaced. You're going to have to deal with that legacy infrastructure regardless.

How can modernizing its networks help the Navy innovate with emerging technologies such as AI and IoT?

Unless my data's right and I can move it around the way I need to, applying AI and popping on IoT devices isn't going to work. We must have an infrastructure that's end-to-end across the enterprise. It's from the user through the cloud to whoever the other user is, or where a machine would be doing something with the

data on the other end. We must have that in place before we can even apply those emerging technologies. We want that backbone in place so that it's quickly adaptable to have things come on and off. The important piece of doing that is to make sure that we are using industry best practices. Using industry best practices, commercial cloud, industry tools and open standards is important to us. We don't want proprietary solutions, we don't want stovepipes of information, or stovepipes in the way we provision or provide network technology or data. We want to be able to jump to the next best thing as industry jumps; we want to move with them.

Why would modernizing the Navy's networks help it protect national security in terms of helping its personnel make decisions faster?

For both cybersecurity and national security, it's what you do with the information that's on the network that matters. For example, right now we have a lot of data out there that isn't necessarily correlated well to make the best operational decisions. I can use machines to do the heavy lifting for me to find combinations of data that human brains don't have the capacity for now, or that our networks don't allow visibility in.

This data's also secure so I can make an operational decision with confidence. I wouldn't say that that level is in a place where we'd like it to be today, which is why getting the foundation of our house right, with regards to data and transportation, is so critical.

A capable adversary from a national security perspective is not going to be loud and proud exfiltrating gigabytes of data. No, they're going to come in at the waterline and they're going to change your data just a little bit. That's what we want to avoid.

Modernizing the network, imposing data standardization and allowing for AI will help our operators improve our national security, and it'll improve our agility to move fast and to make decisions with confidence.

We're doing many things that are cutting-edge. While we would love to move faster, it's hard to move fast. The people who are going to have the information warfare advantage in the future are the people who can move fast with confidence in their information. We're building the infrastructure at the foundational level to allow us to do that.

Conclusion & Next Steps

Whether they're civilian or military, all federal agencies can modernize their networks by adopting PaaS cloud. These intuitive networks are nimble, secure and can support emerging technologies at a moment's notice.

Using DoD as an example, the following suggestions show other agencies how they can use PaaS clouds to modernize their networks for total enterprise visibility.

Don't Lose Sight of the Mission

Every agency has a unique mission that takes more than technology upgrades. DoD is no exception, and the agency can't stop protecting national security while modernizing its network. By focusing on this outcome before modernizing, DoD can ensure that its final network meets its needs. For starters, millions of warfighters will need DoD's network to inform their decision-making in real time. A network tailored to this capability can ensure that warfighters have the knowledge they need to keep America safe.

Map Out Cloud Migration

Legacy networks often have complicated IT infrastructures. Subsequently, understanding what these infrastructures look like and how they transport data can ready agencies for cloud. In DoD's case, the agency can determine which of its applications are siloed without cloud. It's a step that can help the agency re-architect old applications for cloud so the data they store is accessible and useable agencywide.

Don't Skip DevSecOps

DevSecOps is a product management strategy that combines development, operations and security personnel on the entire product process. The strategy saves energy, money and time by making sure all three segments align on product design and rollout. DevSecOps could prove

especially valuable for DoD. The agency routinely creates and launches apps that must balance security with accessibility and reliability for users in difficult operating environments.

Equip Emerging Technologies

DoD must frequently utilize new tools or risk falling behind its adversaries. PaaS clouds are a powerful remedy to this situation because they're easy to customize and scale. As platforms, PaaS clouds can readily support such emerging technologies as AI and IoT.

Connect Cloud to the Edge

The agility of PaaS clouds means that networks now extend farther than ever. IoT devices, meanwhile, are establishing networks where anyone has them. For DoD and other agencies, then, today's networks must constantly function reliably worldwide. These networks must also transfer data securely over wide distances or risk cybersecurity incidents. PaaS clouds can satisfy all these needs, however, meaning that agencies using them have truly limitless networks.



Thank you to Cisco for their support of this valuable resource for public sector professionals.



About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 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 the public sector.

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

govloop.com | [@govloop](https://twitter.com/govloop)