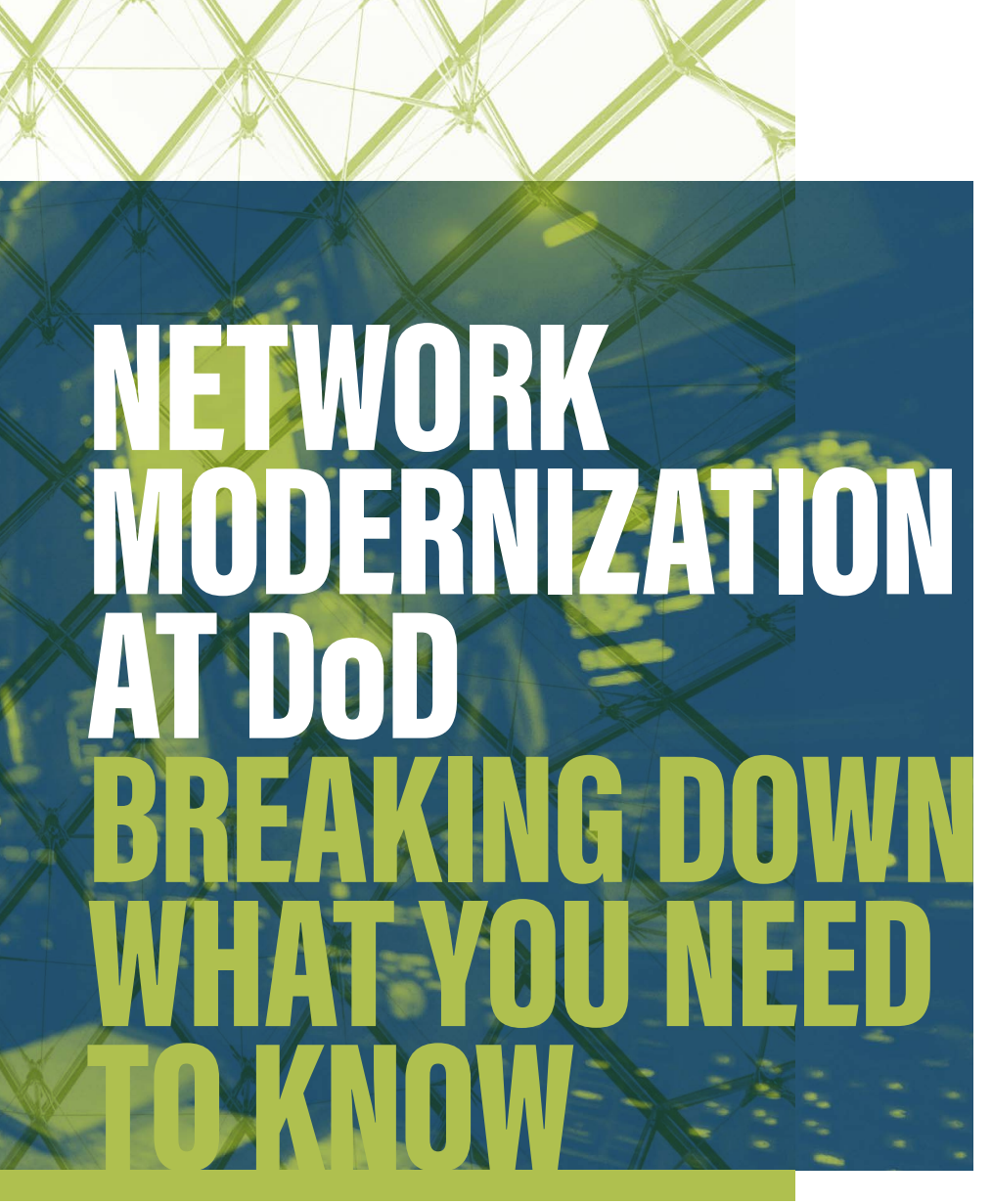


# NETWORK MODERNIZATION AT DoD

# BREAKING DOWN WHAT YOU NEED TO KNOW

GOVLOOP
POCKET GUIDE
2018


MODERN INFRAST
OFFERS A FOUNDA
FOR DoD TO ADOP
LATEST THREAT D
CAPABILITIES.


TRUCTURE
ATION
PT THE
DETECTION

# FOREWORD FROM CISCO

At Cisco we understand the critical role innovative technologies play in keeping our nation safe. That's why we're partnering with Department of Defense (DoD) leaders like you to drive IT modernization through proven solutions and services in cloud, collaboration, networking and security.

To win future wars, DoD networks must provide uninterrupted access to intelligence and data that is gathered globally. They must then deliver that interpreted data easily and securely to our military personnel. This will empower them to better execute their missions both on and off the battlefield. But it will require simple, reliable network access from a variety of mobile devices anywhere in the world. This will have to be powered by new network virtualization and security technologies, like our Digital Network Architecture (DNA).

With DNA, you can enable advanced virtualization, security, analytics and automation across your entire network—from the combat cloud to the battlefield edge. DNA can help DoD achieve unlimited scalability and meet its IT modernization objectives for:

- Enhancing network performance, security and visibility
- Improving collaboration through trusted information sharing

- Achieving successful mission execution despite increasing cyberthreats
- Providing a secure, reliable and DoD-certified cloud environment that is more mission capable and less costly to operate
- Optimizing data center infrastructure by increasing resiliency, interoperability and security.

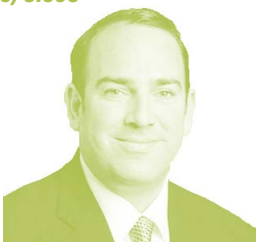
For IT modernization, DoD needs solutions that are mission-effective, cost-efficient, and most importantly, secure. With cybercriminals and nation-states increasing their attacks on our nation using malware, distributed denial-of-service (DDoS) attacks, and insider sabotage, we can help protect your mission critical networks and applications using our industry-leading cybersecurity that features:

- Next-generation firewalls with leading breach detection and mitigation
- Award-winning network access control to keep unauthorized users and devices from accessing restricted areas of your network
- Deeper visibility into your networks before, during and after an attack.

In this pocket guide we'll briefly discuss the DoD's current IT efforts, talk to industry experts, and present a few case studies to help you and your team better understand the benefits of IT modernization. Together, we can make smarter, more successful choices that better serve our military personnel and keep our nation safer. Welcome to the new era of cloud, collaboration, networking and security.

Welcome to the new era of defense.

*— Carl De Groote*
*Senior Director of DoD Sales in Federal Sales, Cisco*



# CONTENTS

# EXECUTIVE SUMMARY

*"Our current network is too complex, fragile, not sufficiently mobile nor expeditionary, and one that will not survive against current and future peer threats, or in contested environments. We find ourselves in a position now, within a new environment and facing new challenges, where our network is not user-friendly, intuitive or flexible enough to support our mission in the most effective manner and demands a heavy reliance on industry field service representatives to operate and sustain these systems."*

Lt. Gen. Bruce T. Crawford, the Army's Chief Information Officer, spoke those words in September 2017 in front of the House Armed Services Subcommittee on Tactical Air and Land Forces to make the point that the Army in particular and DoD as a whole face very real challenges as they look to modernize their legacy technology. DoD is known for silos, bureaucracy, set practices and a command-and-control mentality. To confront new threats with new tactics in real time, however, officials will have to reconsider the way it operates. Agility, collaboration, consolidation and informed decision-making will drive the Pentagon forward, and they must have the technology and modernized IT to do so.

Network modernization is more than a buzzword. It's the path forward — a real, mission-critical endeavor central to the goals of every federal agency. It is also one that, left ignored, will have huge ramifications. DoD networks need a major overhaul. Emerging technologies such as cloud computing, big data, the Internet of Things and mobility generate additional network traffic, straining legacy networks. The promise of these technologies cannot be fully realized without network modernization.

To help clarify how DoD can move into the future with its technology and networks, we've created this pocket guide. This new piece from GovLoop will give you an overview of network modernization at DoD, why it matters — both to DoD and to leaders at other federal agencies who can adapt these tactics and advice — strategies to carry it out, plus case studies and how-to's that will help you get where you need to be today.

# NETWORK MODERNIZATION & DoD THEN AND NOW

The approach to IT and network modernization has evolved thanks to legislation and realities about the use of technology at DoD and the federal government at large, and among citizens.

# STATISTICS

## 60%

DoD's internal goal is to close 60 percent of its data centers by fiscal year 2018

## $1.2B

Automation could save government up to 1.2 billion work hours and $41.1 billion annually

## $52B

Of the $52 billion in federal civilian IT spending planned for fiscal year 2017, about 71 percent ($37 billion) was classified as "legacy" IT spending

## 90%

Some agencies are spending 90 percent or more of their IT budgets on operations and maintenance:


Army Corps of Engineers:
96 percent of its
**$459.8 million budget**

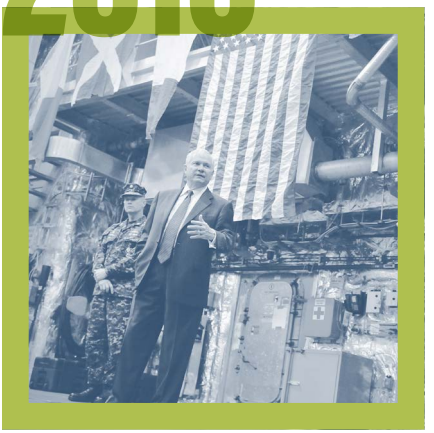

Nuclear Regulatory Commission:
93 percent of its
**$156.5 million budget**


Agriculture Department:
90 percent of its
**$3.2 billion budget**


Veteran's Administration:
88 percent of its
**$4.4 billion budget**

# IMPORTANT LANDMARKS

## 2010



Former Defense Secretary Robert Gates leads the charge to develop the foundation for the Joint Information Environment (JIE) framework — a secure environment comprised of shared IT infrastructure, enterprise services and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies.

## 2011

**October 7, 2011:** President Obama puts into effect "Executive Order 13587 — Structural Reform to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." The order stresses the importance of managing the people who have access to classified information and includes strategies to monitor what these people are doing with it, be it physical or electronic.

## 2015

**October 2015:** DoD releases its Cybersecurity Discipline Plan. The plan focuses on four key areas: strong authentication; device hardening; reducing the attack surface; and alignment to cybersecurity/computer network defense service providers.

## 2016

**October 2016:** DoD releases an information and cybersecurity roadmap that lays out plans for a departmentwide operating system, use of Common Access Cards, data center consolidation and migration to cloud services.

## 2017

**December 2017:** The American Technology Council releases its "Report to the President on Federal IT Modernization," which advises a strong focus on network modernization.

**December 2017:** As part of the 2018 National Defense Authorization Act, the Modernizing Government Technology Act becomes law. It creates working capital funds for IT projects at Chief Financial Officers Act agencies that don't already have them, in addition to a central modernization fund housed by the General Services Administration.

# TODAY'S LANDSCAPE OF NETWORK MODERNIZATION AT DoD

Outdated federal IT networks can't fully reap the extensive advantages of mobility, cloud, social networking and big data analytics technologies that are affecting so much of what the military does and needs to do. That deficiency limits the joint forces' ability to effectively and securely serve the men and women who serve them, and the citizens they protect.

Network modernization can help DoD take advantage of new, innovative technologies. The network is the backbone of everything you do in IT. Replacing older switches and routers with new, smart, intuitive versions immediately multiplies security, speed and efficiency to make other modernization steps easier. In fact, the network should be the first thing you modernize — but unfortunately often ends up being the last.

So why is network modernization more important today than ever to DoD? There are several reasons:

- It is the foundation for warfighting operations across air, land, sea and space domains, as well as is its own warfighting domain – cyber.
- It supports joint and coalition warfighting missions.
- It helps enable the DoD to gain benefits of modern security architectures to ensure a secure and resilient foundation from which to operate.
- Network modernization enhances and shortens the time to decision-making.
- It ensures a high-end, full spectrum-capable force in a multi-domain warfighting environment.

In this section, we will go over the current challenges presented by the network the military is operating on today and the initiatives and future vision that require network modernization at DoD. We'll also discuss the benefits the military will see by moving to a modernized network, and how they plan to get there.

# CURRENT DoD NETWORK CHALLENGES

The military, like any other organization, is always evolving. This means, however, that the network that was developed for previous warfare environments and that worked decades ago doesn't meet current needs, let alone future warfighting needs. Data storage, transport challenges, siloed departments and the absence of joint interoperability have all presented serious challenges to modernizing DoD's network. The military has turned to industry vendors to fill the gap and help them step up to the plate, but standard acquisition processes haven't kept up with a commercial innovation explosion, leaving the military at a disadvantage to adversaries.

Additionally, a recent Army study documented significant challenges to its network and network modernization across four broad areas: network governance, requirements, acquisition and innovation. In response to the study, the Army said, *"Today, our Army is not institutionally organized to deliver modern, critical capabilities to Soldiers and combat formations quickly. Our current modernization system is an Industrial Age model. It was sufficient for past threats, but insufficient to ensure future overmatch and rapid procurement of our modernization priorities. Our processes are staff-centric and often stovepiped, which inhibits integration within or across programs. Our requirements process is slow and overly bureaucratic. Our talent management process needs to adapt to ensure the right people develop the right capabilities for future battlefield success."*

Additionally, the Air Force has focused on network modernization as the next step in their success. "Looking at our adversaries, we are going to have to fight in a multi-domain way," Brig. Gen. Kevin Kennedy said at a Washington D.C. Armed Forces Communications and Electronics Association event. "The cyber domain is the key to integrating across all the other domains."

Many of the joint forces have evolved as multiple stovepiped mission command systems and networks with various, duplicative and non-integrated IT programs. This has yielded inadequate integration across the mission areas, and poorly conceived network architectures, resulting in inefficiency and ineffective integration of readiness priorities.

These challenges to network modernization are significant, but DoD acknowledges them and is looking for ways forward. So what's next?

# GOALS OF A MODERN DoD

## In 2016, DoD unveiled its roadmap for modernizing its IT and networks, including the following eight goals:

**1**

Executing capability initiatives toward the JIE vision: A modernized IT enterprise with enhanced network performance that is more secure and visible throughout.

**2**

Improving collaboration with mission partners and industry: Positive synergies in processes, technologies, and intellectual capital are mutually beneficial to DoD and its partners.

**3**

Ensuring successful mission execution in the face of a persistent cyberthreat: Provide mission dependability in the face of a capable cyber adversary.

**4**

Providing a cloud computing environment: DoD operations are supported with a new less complex, more agile and defensible IT environment that is more mission capable and less costly to operate. This increases mobility, virtualization, and integration of virtual services into DoD strategic environments.

**5**

Optimizing DoD's data center infrastructure: Optimized DoD computing infrastructure provides greater operational and technical resilience, improves interoperability and effectiveness, increases capability delivery, prioritizes secure capabilities, and reduces costs.

**6**

Exploiting the power of trusted information sharing: Enhanced support to decision-making processes — through secure access to DoD information and application of common data standards — improves collaboration both across the DoD enterprise and with external mission partners.

**7**

Providing a resilient communications and network infrastructure: Modernized DoD communications infrastructure and increased maneuverability within the electromagnetic spectrum provide greater operational and technical resilience, improved plug-and-play and effectiveness, faster capability delivery, prioritized secure capabilities, and reduced costs.

**8**

Improving transparency, oversight and execution of DoD IT investments: Strengthen DoD CIO's support to the Secretary in all matters regarding IT investments. Ensure that DoD IT investments are mission effective, cost efficient, and secure.

***You can view the whole roadmap here.***

# WHAT NETWORK MODERNIZATION CAN DO FOR DoD

## The future of infrastructure at DoD has at its foundation a software-driven, automated and intelligent network. Here are the ways in which a modernized network can help the department overcome its challenges and meet its goals for future warfighting capabilities.

**Automation:** Automation does three things for DoD:

1. Enhances services' agility through analytics, security and application experience
2. Allows for the creation of entire local- and wireless-area network architectures, plus underlay and overlay networks with ease of point-and-click through the DNA-C appliance and associated networking gear and software
3. And allows for network virtualization, tying in wired, wireless and IoT endpoints.

It also enables workers to spend less time on manual tasks so they can focus on mission-critical projects.

**Software-defined networking:** Software-defined networking (SDN) provides a new architecture for the network, an architecture that brings the application and networking layers closer together. It is a shift in technology that changes the networking landscape by providing greater automation and orchestration of the network fabric, and by allowing dynamic, application-led configuration of networks and services. SDN allows the network to respond to requests from an application in real time, based on the current state and condition on the network. It is this agility that will transform networks as DoD knows them.

**Cloud computing:** The cloud enables modernization without the need to "rip and replace" on-premises systems. In many cases, you can replicate and even enhance the functionality of a legacy system by subscribing to it as a service via the cloud. The cloud also offers a secure environment and compliance with the Federal Risk Authorization and Management Program, assuring that a cloud offering meets federal requirements.

**Cybersecurity:** Although network modernization and digital transformation are expanding DoD's online attack surface, they also can improve cybersecurity. Technology is evolving rapidly to counter these threats. A security-driven network refresh to replace outdated equipment can help eliminate vulnerabilities and mitigate risks, and also allow the joint forces to take advantage of the efficiencies and functionality of new technology to improve both their cost savings and productivity.

**Analytics and AI:** As the network environment scales, it will become exceedingly difficult to effectively manage it and ensure the prescribed service levels. The network is inherently difficult to manage today, and once cloud computing and IoT are fully adopted, the complexity will be overwhelming. Solutions will need to incorporate artificial intelligence and machine learning to analyze the vast amounts of data generated from the network and take the appropriate action.

Investing in a modern, digital-ready network provides solid returns that make good business sense. Organizations often put themselves at risk while struggling to do more with less. Modernizing your network and investing in digital transformation efforts let organizations, specifically DoD, do more, and do it securely and economically.

# INDUSTRY SPOTLIGHT

## SUPPORTING A MODERN MILITARY WITH A DIGITAL NETWORK ARCHITECTURE

### An interview with Carl De Groote, Senior Director of DoD Sales in Federal Sales, and Karl Dalstad, Director of Enterprise Networking for U.S. Public Sector Sales, Cisco

Today our military needs a new blueprint for a modern digital military. The world of technology has changed the strategies, tactics and procedures required to operate successfully in modern warfare.

Cyberspace is playing an increasing role in how wars will be waged in the 21st century. The modern military relies on cyberspace to conduct critical exercises — everything from tracking force movement to linking and gathering data across weapon systems and battlefield platforms, including aircraft, drones and robots.

Although the digital and cyberspace domain has enhanced the military's mission capability, it has also created a complex national security environment with frequent cyberattacks that severely increase the risk of the military's day-to-day operations.

To learn how a new network approach — a single platform that is simple, automated, intelligent and secure — will better serve the future needs of DoD, GovLoop sat down with Cisco's Carl De Groote, Senior Director of DoD Sales in Federal Sales, and Karl Dalstad, Director of Enterprise Networking for U.S. Public Sector Sales. Cisco also takes seriously its employment of veterans, knowing that there's no one better to understand the on-the-ground challenges the DoD faces on a day-to-day basis.

To meet the needs of modern warfare and properly equip today's military personnel, the military first needs to digitally transform. Moreover, it needs a modernized network capable of providing continuous feedback to simplify and optimize operations and to support an automated millisecond response to cyberattacks. Embracing this type of architecture can lay the foundation for a fundamental transformation of cyberspace.

"Today, military chiefs are looking for systems that will offer a system of joint coalition and warfighting missions, but also enhance and shorten their time to decision," Dalstad explained. "Nowadays the military doesn't have the luxury of calling back to the White House for approval – they make decisions on site. And that can't be done if you're still running on old serial networks or analog networks. You must have a highly efficient, high bandwidth, multi gigabit environment."

***This closed loop of defining intent, collecting context, learning and then implementing new intent based on those insights is what Cisco refers to as "intent-based networking."***

That's where Cisco DNA comes into play, De Groote said.

"In building and operating the network as a warfighting platform, the Defense Department should consider a Digital Network Architecture, an approach used by Cisco to facilitate faster, more flexible network services that support digitized mission processes," De Groote said. "The architecture's key tenets are virtualization, security, analytics and automation with the added benefits of cloud service management and open API (application programming interface)."

Embracing this type of architecture can lay the foundation for a fundamental transformation of cyberspace, De Groote said. "First, closed and hardware-centered models give way to open, programmable and software-centered ones. Second, manual, repetitive command line interface-driven management is largely superseded by policy-based automation. Third, network-embedded, context-based security that reaches from the enterprise to the tactical edge supplants perimeter-based, reactive security. And last, information technology-centered analytics morph into mission-focused cybersecurity analytics."

With this architecture, operators can specify policy for cyber infrastructure, and automation allows the technology to become nimbler and respond to mission conditions far more quickly and intelligently.

"This architecture is grounded in a network infrastructure that is fully programmable and open to third-party innovation and seamlessly integrates the cloud as an infrastructure component," Dalstad said.

Cisco's DNA command center is also an analytics platform, collecting context from the network as it operates. All types of data that were previously isolated on thousands of individual routers, switches and wireless access points can now be streamed to the DNA command center in real time, helping organizations better understand the operation of the enterprise and continually learn to solve complex problems.

This closed loop of defining intent, collecting context, learning and then implementing new intent based on those insights is what Cisco refers to as "intent-based networking."

The combination of an intent-based, secure infrastructure with a platform's single point of policy definition, context collection and learning will become the new approach to building enterprise networks — for the military of the future and beyond.

# LEARNING FROM OTHERS: CASE STUDIES

Here we describe two DoD entities that have benefited from modernization. Read how these organizations are modernizing their IT and networks to move into the future.

# JOINT REGIONAL SECURITY STACKS

Automation, movement to the cloud and greater data security are three areas critical to DoD's future and its network modernization. But how can it get there seamlessly? One answer is joint regional security stacks (JRSS). A JRSS is a suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding, and provides a host of network security capabilities.

Recently, the Defense Information Systems Agency (DISA) has partnered with the Army and Air Force to fundamentally change the way DoD secures and protects its information networks by deploying JRSS. And they're working with Cisco to do so.

"In support of the Army, DISA is centralizing the Army's existing worldwide perimeter security infrastructure from hundreds of local security stacks into a JRSS construct," according to a DISA statement. "The Air Force has begun to use the JRSS construct to protect its infrastructure and the Navy is planning the migration of its excepted networks as a first step towards the use of JRSS to protect its infrastructure."

This effort, which incorporates moving to common standards architecture and increasing AI algorithms to detect malware and intrusions, relies less on human intervention, De Groote said in an interview with Defense Systems. "We create a common operating environment to collapse layers of old network architecture and deploy data across the DoD," he said.

Deploying JRSS will enable departments to inspect data, retrieve threat and malware data on the network, troubleshoot, and then patch, protect, and defend the network. It will also improve the effectiveness and efficiency of the network by ensuring that there is sufficient capacity to support the transition of services and capabilities.

> ***"We create a common operating environment to collapse layers of old network architecture and deploy data across the DoD."***
>
> ***Carl De Groote***
> ***Senior Director of DoD Sales in Federal Sales, Cisco***

# THE USS ZUMWALT (DDG 1000)

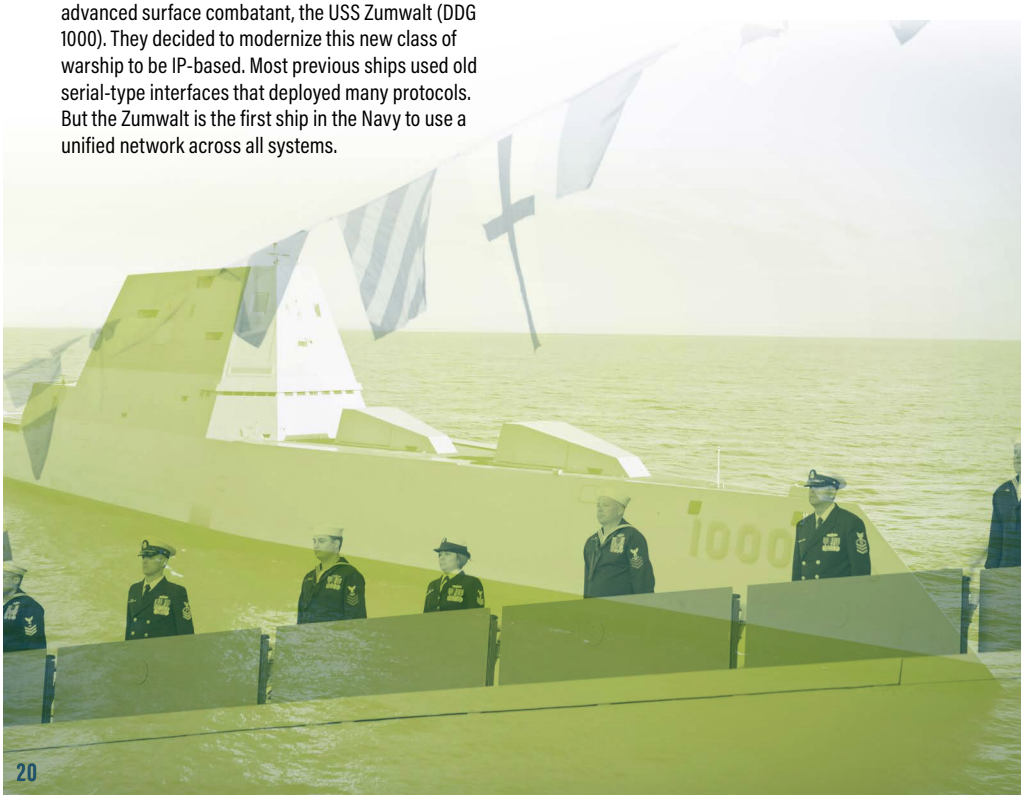
It's no surprise that shipbuilding can be extremely complicated, especially in the Navy. One ship is made up of dozens of types of systems: propulsion, warfighting, alarming, fire suppression, steerage and more. Often, each and every one of those dozens of networks is designed or created by a different subcontractor with a different technology.

This can be expensive but also ripe with problems. If one system is having issues, the skill sets available on the ship may not be able to help.

Using Cisco technologies, the Navy set out to do something different with its most technologically advanced surface combatant, the USS Zumwalt (DDG 1000). They decided to modernize this new class of warship to be IP-based. Most previous ships used old serial-type interfaces that deployed many protocols. But the Zumwalt is the first ship in the Navy to use a unified network across all systems.

The single, encrypted network — called the Total Ship Computing Environment — controls all shipboard computing applications on the Zumwalt, ranging from its lights and machinery control to its radars and weapon systems. Part of the environment is what is known as the Electronic Modular Enclosures, or EMEs. These are packed with blade servers running Cisco network technologies.

The unique computing environment's sailor-centric interface and high degree of automation allow the ship to run more effectively and efficiently.



# CHEAT SHEET

**This takeaway section will give you actionable steps toward modernizing your network, plus best practices and further resources on the topic.**

## Current challenges DoD faces in its technology landscape:

(source: disa.mil)

- Highly manual management of infrastructure and provisioning of services
- Stovepiped/wedge-based design in networking and application hoteling
- Seams and gaps in maintenance and monitoring of end-to-end experience
- Lack of comprehensive documentation of architectures and settings
- Limited support to mobile workforce

## Need to articulate the benefits of network modernization at DoD? Here's what investing in network modernization will do:

- Increase mission effectiveness.
- Strengthen cybersecurity.
- Improve outcomes of IT acquisition.
- Deliver capabilities faster.
- Improve interoperability.
- Save billions of dollars through cost efficiencies.

## 4 Steps of a Network Modernization Strategy

### Step 1: Assessment

Start by assessing the current infrastructure and the processes it supports. Performing an assessment results in a point-in-time baseline, which IT buyers use to identify gaps and needs. It also serves as a benchmark to measure against in the future.

### Step 2: Planning

An IT modernization roadmap sets timelines for completion, project objectives and estimated costs. It describes the phases of modernization — planning, designing and building systems, cloud migrations, testing, and deployment.

### Step 3: Migration

Choose technologies that meet the business objectives of modernization efforts, while maintaining security and integration across the entire infrastructure. Integration projects can be challenging, so consider a solutions partner with a proven track record on the particular integration project.

### Step 4: Monitoring

Monitor performance of new technologies and processes to determine if the modernization efforts meet goals. There's also a need to make sure technologies meet new objectives as scenarios and needs change for the agency.

***For more information, visit cisco.com/go/DoD***

# THANKS TO CISCO FOR TH SUPPORT IN PRODUCING PUBLIC-SECT RESOURCE

HEIR

THIS

TOR

## About Cisco

Cisco designs and sells broad lines of products, provides services, and delivers integrated solutions to develop and connect networks around the world. For over 30 years, we have helped our customers build networks and automate, orchestrate, integrate, and digitize IT-based products and services. In an increasingly connected world, Cisco is helping to transform businesses, governments, and cities worldwide. To learn more visit: **cisco.com/go/DoD**.

## About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 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**.

***The military today needs a modernized network capable of providing continuous feedback to simplify and optimize operations.***

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421
F (202) 407-7501
www.govloop.com
@GovLoop