

STRATEGIC GUIDANCE SURVEY

Perspectives: Optimizing Defense Networks





The Defense Department's Fourth Estate Network Optimization (4ENO) initiative is as bold as it is risky. The ambition is to unify nearly two dozen Defense agencies under a common network by 2025.

As of now, taken together, those agencies use 600 separate contracts to maintain their networks across 850 worksites, and the Pentagon sees the current reality as wasteful and counterproductive.

It's bold because it aims to bring together as many as 357,000 users in DoD's unclassified environment, plus 36,000 more seats on its Secret Internet Protocol Network (SIPRnet). If it succeeds, it will be one of the largest network consolidation efforts ever in government.

It's risky, because large-scale consolidation initiatives must overcome enormous technical, culture and process challenges.

The good news for DoD and the "Fourth Estate" agencies: no one expects to eat the proverbial apple in one bite, nor should they.

Several IT leaders in those agencies told Federal News Network they are leaning on commercial expertise as well as the experiences of the Army and Air Force, who have undertaken their own experiments to deliver enterprise IT as a service.

Paul Gass, chief information officer at the Defense Finance Accounting Service (DFAS), said the end goal is two-fold: optimizing all IT services in an effort to remain a value-added and cost-conscious provider of choice for the department, and ensuring that standardization will reduce the amount of resources needed in ways that refocus the agency's spending toward security improvements.

Ronzelle Greene, the chief information officer for the Defense Counterintelligence and Security Agency, said the greatest benefit from the modernization effort is that DCSA will have the ability to replicate data between the three major sites and implement global traffic managing (GTM) devices to improve security of applications and data.

This survey of Defense agency leaders highlights the fact that while the approaches may be slightly different, the end goals are all the same: delivering mission capabilities more quickly at a reduced cost.

Jason Miller
Executive Editor
Federal News Network

PANEL OF EXPERTS:



Christopher Sherwood, a public affairs officer in the Office of the Secretary of Defense, on behalf of Defense Contract Audit Agency



Ronzelle Greene, Chief Information Officer, Defense Counterintelligence and Security Agency



Christopher Thomas, administrator of the Defense Technical Information Center



Paul Gass, chief information officer, Defense Finance Accounting Service

Discuss your network modernization strategy. How are you focusing on mission areas versus the back office areas network used for administration purposes? What role does network-as-a-service from a commercial provider play into that strategy?

The Defense Contract Audit Agency (DCAA) is an active participant in the Defense Department's Fourth Estate network consolidation effort. Under this construct, we will outsource our IT infrastructure operations to the DoD service provider, while maintaining management oversight and responsibility of our DCAA mission systems. Network-as-a-service is in our future from either the Defense Information Systems Agency (DISA) itself or via a DISA-contracted commercial network service provider.

-- Christopher Sherwood, a public affairs officer in the Office of the Secretary of Defense on behalf of Defense Contract Audit Agency (DCAA)

As the Defense Counterintelligence and Security Agency (DCSA) evolves, so too does the need for changing our IT organization, processes, and technology delivery. The Office of Chief Information Officer (OCIO) leads the DCSA information enterprise by defining a shared vision, setting and enforcing agency policy, and driving the standard for the information infrastructure that supports security oversight and education missions. OCIO ensures that DCSA employees across the globe have the tools, capabilities and access to data, systems and applications to fulfill the agency mission. Our vision is reflected in an aspiration called "DCSA One." It speaks to OCIO's ability to provide DCSA employees with one email, on one single network, working in a single environment.

By subscribing to cloud-based tools, DTIC gains the ability to quickly adopt new and emerging technologies and avoid being locked into legacy products.

"DCSA One" will allow onsite and remote administrative support of the back office area network support functions by leveraging the Defense Information Systems Agency's (DISA's) Multiprotocol Label Switching (MPLS) network, to connect the field offices and major site locations leading to a 10% reduction in overall network costs.

-- Ronzelle Greene, chief information officer, Defense Counterintelligence and Security Agency (DCSA)

The Defense Technical Information Center's (DTIC) mission is to accelerate innovation by ensuring that the output of work done in our scientific and technical community is broadly shared. DISA's DoDNet, which consolidates back office IT support, allows DTIC to focus on our unique mission activities.

Rather than designing and building our own networks and the accompanying capital investment, DTIC is leveraging the capabilities found in the commercial cloud. By subscribing to cloud-based tools, DTIC gains the ability to quickly adopt new and emerging technologies and avoid being locked into legacy products.

-- Christopher Thomas, administrator of the Defense Technical Information Center (DTIC)



We rely on DoD direction, to include our close partnership with DISA and the DoD CIO, to provide guidance and nested planning for the Fourth Estate Network Optimization. Because network support is decidedly different than, say, database administration, compliance, system production support, etc., we have to continually focus on all to provide mission services.

Both the mission areas and the back office support areas have their strategic vision and plan for optimization. Our IT support is organized by product lines and enterprisewide function or service; we provide IT support specific to payroll services systems, accounting services systems and corporate services systems (which are those systems that span multiple product lines). However, just like other Fourth Estate agencies, we have our own network and the related back office, or enterprisewide support requirements that we

manage internally through dedicated IT support organizations. The network-specific support and the resources associated with it will transfer to DISA with the Fourth Estate Network Optimization (4ENO) initiative, enabling DFAS to be even more focused as an agency on its mission.

We will still be administering our pay, accounting and other production systems. In regards to network-as-a-service, we continue to monitor DoD, government and commercial industry direction to determine what the future looks like and the direction we are going with our systems and environments. DFAS will continue to work toward optimizing all IT services in an effort to remain a value-added and cost-conscious provider of choice for the department.

-- Paul Gass, chief information officer, Defense Finance Accounting Service (DFAS)

What does your modernized IT network's end-state look like? How are you ensuring that innovation from commercial providers is part of that end state?

Through the DISA MPLS network, proven commercial solutions are being successfully embedded into our IT infrastructure. We have recognized that our evolving IT environment is reliant on public-private partnerships. Pairing the strategies and experience we have in OCIO with commercially-provided solutions positions DCSA with an even greater assurance that our future IT network is secure, accessed by those who need it, and continues to demonstrate fiscal value. The network expansion will provide DCSA with 10 times the bandwidth available today and be extended to our three major site locations, as well as our field offices across the continental United States. When finished, the network DCSA supports will include 12,000 concurrent users and provide data replication to support active/active data center configurations.

-- Ronzelle Greene, chief information officer, Defense Counterintelligence and Security Agency (DCSA)

Our adoption of the commercial federal cloud allows us to adopt technology as it is made available. Our goal is to provide our users with the most robust technology, utilizing the best products commercially available. We will continue to maintain and to monitor the technology landscape and insert new capabilities as they become viable. We are working with the Defense Innovation Unit and Joint Reserve Directorate in DDR&E (R&T), and partners in the services to design our future state.

-- Christopher Thomas, administrator of the Defense Technical Information Center (DTIC)

The network expansion will provide DCSA with 10 times the bandwidth available today and be extended to our three major site locations, as well as our field offices across the continental United States.

At end state, DCAA will be hosting and managing its mission systems within an approved DoD cloud service provider, while outsourcing infrastructure with a contracted commercial network service provider. DCAA will actively modernize and innovate our mission systems, but will rely on DISA/DoD contractual oversight to keep the network-as-a-service component current with advancing technologies.

-- Christopher Sherwood, a public affairs officer in the Office of the Secretary of Defense on behalf of Defense Contract Audit Agency

There is no end-state for modernization as it is a constantly changing environment; rather there are many opportunities to innovate, streamline, and excel. For our IT network support in the future, I expect our user environment, back office areas, and common-use IT support to be similar to the rest of the 4th Estate. This enables DoD to maximize on efficiencies and reduce costs. Innovation is key to maximizing efficiencies and productivity, no matter its genesis. No doubt, the DoD will continue to pursue innovative solutions that further its intent for efficacy and success.

-- Paul Gass, the chief information officer of the Defense Finance Accounting Service (DFAS)

As your network evolves, what do you see as the biggest benefits from this modernization effort around workforce, security and mission delivery perspectives? How will this effort open up resources—money and people—to focus on mission tasks?

The biggest benefit I see is standardization. It is much simpler to support an environment where everything is similar vs. having to know, understand and operate around many nuances. I do not expect everything to be the same across the board, but minimizing variances maximizes the effectiveness of the resources on hand. For this reason, standardization reduces resources needed and enhances security effectiveness to sustain IT assets. It frees up resourcing to focus on better/more analysis, optimization and innovative solutions that can take us into the future.

-- Paul Gass, the chief information officer of the Defense Finance Accounting Service (DFAS)

As our network evolves, the greatest benefit from the modernization effort is that DCSA will have the ability to replicate data between the three major sites and implement global traffic managing (GTM) devices. The GTM devices will have the ability to analyze traffic patterns to ensure DCSA users are authenticated at the site that provides the best connection. With an active/active data center configuration, user downtime will be diminished by ensuring users are directed to another location should any of the three major sites fail to operate.

-- Ronzelle Greene, chief information officer, Defense Counterintelligence and Security Agency (DCSA)

It is much simpler to support an environment where everything is similar vs. having to know, understand and operate around many nuances.

DTIC benefits from a reliable and robust network infrastructure, which increases our ability to provide rich content to users. Riding on enterprise network infrastructure allows us to focus resources and people on mission activities. With DISA assuming security of the network, we are able to explore other security issues, like documents rights management.

As the services enhance their networks, DTIC will be able to deliver more data intensive, dynamic and visual information.

Research datasets, for example, can be very large, so we're excited for the increasing network capacities and the potential for enterprise storage that helps us give DoD users quick access to information. This opens up opportunities for reuse of the taxpayer investment in datasets. A dataset that one organization created for one purpose may have other applications, creating additional value for the DoD research community.

-- Christopher Thomas, administrator of the Defense Technical Information Center (DTIC)

Once achieved, the DoD Fourth Estate network consolidation will improve IT standardization, security oversight and collaboration capability across the department and, hopefully, improve reliability

and availability of network services. DCAA resources, both personnel and financial, are being transferred to DISA to support the infrastructure services.

DCAA will use remaining resources to manage our mission systems. For DCAA, we look forward to the

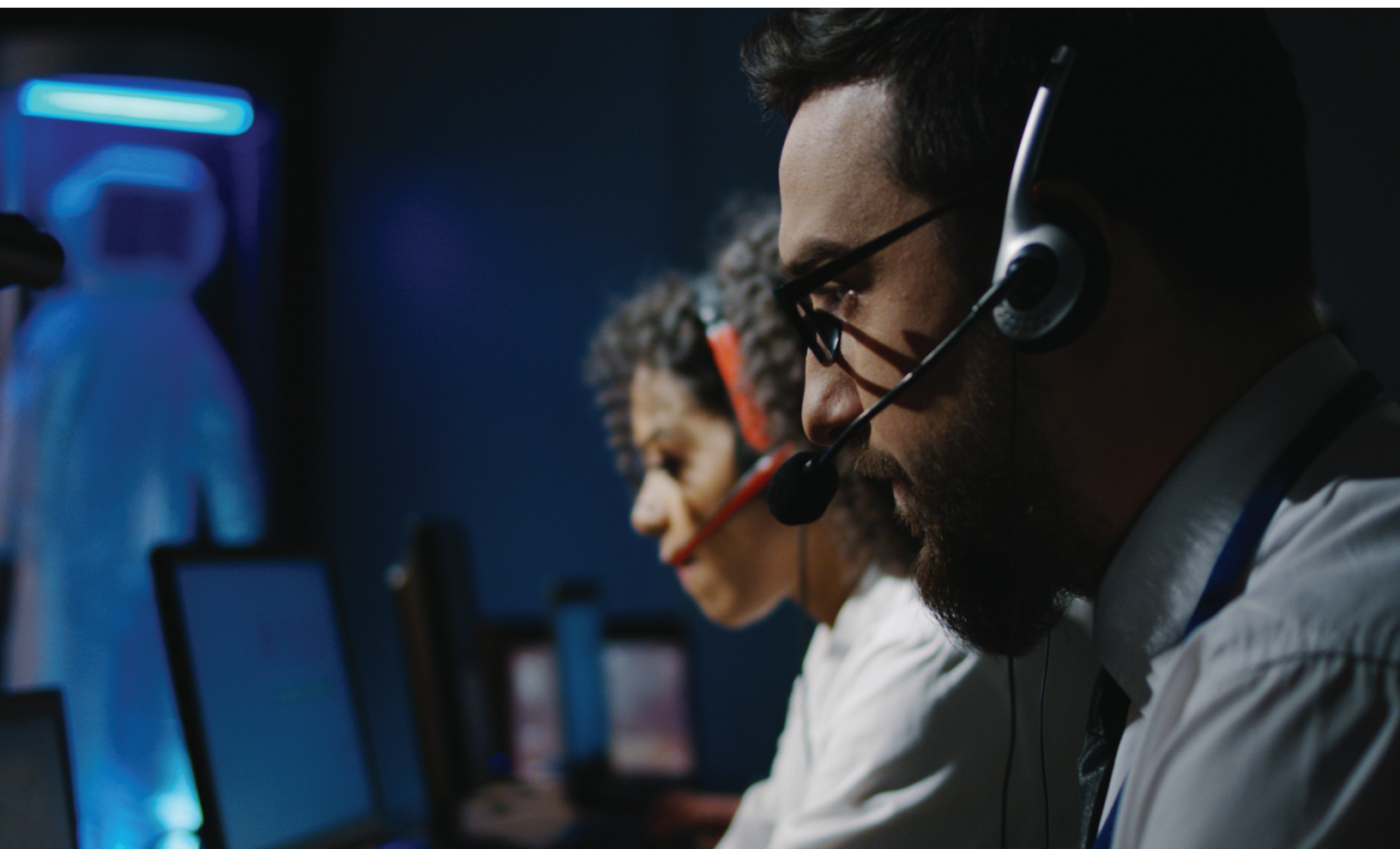
potential network improvements consolidation will bring.

**-- Christopher Sherwood, a public affairs officer
in the Office of the Secretary of Defense on
behalf of Defense Contract Audit Agency**

How has the COVID pandemic changed your thinking about what you need from your network in terms of mobility and providing technology services to customers?

DTIC supports a worldwide customer base. Under COVID, we saw our use of network bandwidth expand and the need to engineer more fault tolerance into the network. We recognize that the network extends beyond DoD control and user access issues are impacted by user internet

service provider (ISP) choices, home WiFi and other devices on their home network. Remote meetings with customers and industry partners has also increased. Having the tools to support virtual meetings with those outside the department has become essential.





Use of mobile devices to access our tools has grown. We were developing our interfaces to take advantage of larger screen sizes customers had in their offices. We must now also adjust to support the smaller screen size of mobile devices. With the accelerated transition to mobile devices we need to understand how our content will be consumed on these as a primary means of accessing information.

DTIC will leverage commercial technologies to identify new ways to present data. We need to be prepared to evolve at the pace of technology

and quickly adapt to the changes in how our users consume information.

**-- Christopher Thomas, administrator of the
Defense Technical Information Center (DTIC)**

By virtue of our audit mission and the geographically distributed nature of our employees, DCAA was supporting a mobile workforce long before COVID and was well positioned to deal with the increase in remote telework. When we shifted to 100% telework, however, we did encounter network bandwidth limitations. Accordingly, we

have been working to expand both circuit size and virtual private network (VPN) capacity to adequately support a 100% telework environment, should that requirement become necessary again for any reason in the future.

-- Christopher Sherwood, public affairs officer in the Office of the Secretary of Defense, on behalf of Defense Contract Audit Agency

DCSA is undergoing an exciting transformation in how it meets its mission and OCIO is here to make that possible. The COVID-19 pandemic highlighted new ways of working and practices that will likely become the norm.

An example of the change in DCSA's mindset is the implementation of the mobility management program (MDM). The MDM platform will allow single sign-on to all mission applications and enable the agency to manage all mobile devices to ensure security measures are implemented to protect data.

OCIO has worked hard to drive a successful balance between access and security. During the past year, a catalog of secure collaboration and communication tools was rolled out across the enterprise. OCIO is implementing technology, practices, and policies to enable these types of scenarios in ways consistent with what a user would experience using commercial systems and tools.

-- Ronzelle Greene, chief information officer, Defense Counterintelligence and Security Agency (DCSA)

I don't think COVID changed our thinking much; it certainly accelerated our plans. Our DFAS workforce and IT infrastructure was well prepared before the COVID pandemic to protect the health of our workforce by transitioning to a full-time telework environment. We did not face many

OCIO is implementing technology, practices, and policies to enable these types of scenarios in ways consistent with what a user would experience using commercial systems and tools.

challenges during the transition, outside of managing the fact that our workforce tends to schedule their large teleconference meetings at the same time, resulting in over-subscribing our and DISA's conference bridges. However, that was an easy fix after a couple days of learning and leaning on our other available tools, like internal instant messaging.

The only change I made was the acceleration of our previous plan to expand our available network bandwidth to support wider use of virtual meetings, including video capability. I believe the pandemic response caused the department to consider a new perspective, and we will continue to need to support a mobile workforce indefinitely.

-- Paul Gass, the chief information officer of the Defense Finance Accounting Service (DFAS)

The Air Force and Army's enterprise IT-as-a-service initiatives are providing lessons learned that will be useful to Defense agencies as we deal with respective and unique technology challenges that must be overcome to achieve the Fourth Estate Network consolidation.

Discuss how the Air Force and Army's enterprise IT-as-a-service initiatives are influencing your network modernization efforts. What factors are you paying close attention to that may apply to your strategy's continued evolution?

The Air Force and Army's enterprise IT-as-a-service initiatives are providing lessons learned that will be useful to Defense agencies as we deal with respective and unique technology challenges that must be overcome to achieve the Fourth Estate Network consolidation. DCAA will be a customer of the network-as-a-service model and will be no longer responsible for infrastructure services.

-- Christopher Sherwood, a public affairs officer in the Office of the Secretary of Defense on behalf of Defense Contract Audit Agency

I cannot speak to whether or not the Air Force and Army's initiatives are directly impacting our own network modernization efforts. I have no doubt that the DoD CIO and DISA are incorporating lessons learned in their efforts to optimize the Fourth Estate network. The concept is similar – consolidate service delivery across many users to maximize efficiencies. As a Fourth Estate agency, we will follow the guidance of the department.

-- Paul Gass, the chief information officer of the Defense Finance Accounting Service (DFAS)

We are looking to the service initiatives to replace our cloud managed hosting environment; specifically, we have an initial agreement with the Air Force to migrate our mission systems to their Cloud One environment. This will enable us to gain the benefits of their DevSecOps, containerized infrastructure and cybersecurity layer.

It also frees up the time and resources required to contract for services that we can now order off

In modernizing our IT network, it is critical that we build in resiliency and redundancy.

of an available vehicle. We see this as especially important as we address the growing cyber threat to the network.

In modernizing our IT network, it is critical that we build in resiliency and redundancy. We are closely monitoring vendor participation in the service provided cloud offerings and the availability of industry tools and services.

Of particular interest to DTIC are the commercial vendor partners with a focus on artificial intelligence and machine learning (AI/ML) and user identity management. We are also tracking how these new environments support the critical access we need to provide to our industry partners outside the firewall for enterprise activities. It is important that this infrastructure also supports our customers' adoption of mobile devices, as it continues to grow.

-- Christopher Thomas, administrator of the Defense Technical Information Center (DTIC)

DCSA has embarked on its own IT-as-a-service initiative. DCSA is working with the General Services Administration's Office of Assisted Acquisition Services client support center to support the "DCSA One" IT requirement.

-- Ronzelle Greene, chief information officer, Defense Counterintelligence and Security Agency (DCSA)

How DoD is embracing commercial innovation to maintain its IT modernization momentum

INSIGHT BY AT&T



Tim Blount

Director, Technology and Strategic Programs, AT&T



Jonathan Sutherland

Director, U.S. Air and Space Force, AT&T

The Defense Department is embracing mobility in its workforce. The pandemic forced DoD to adapt to remote work, and those efforts were so successful that both employees and leadership want to keep it around, because it's fundamentally changed the way DoD agencies do business. And now that it's gotten a taste of how unfettered IT modernization can improve its ability to carry out the mission, DoD wants to keep the momentum up.

To do that, DoD has recognized it has to change not just technology itself, but also its policies and processes, many of which stem from as far back as the 1970s and 80s, and seriously inhibit commercial innovation.

That's part of an effort to leverage more commercial solutions rather than building their own. And this new approach is already proving to have multiple advantages as the Army and Air Force lead the way with their modernization efforts.

"We're working on an Air Force Enterprise-IT-as-a-service initiative, where we're transforming three bases in a network-as-a-service model to this commercial model. We're also doing that for the Army," said Jon Sutherland, director for U.S. Air Force, U.S. Space Force and DoD Agency Solutions at AT&T. "Our vision there is to modernize commercial best practices to comprehensively rebuild and modernize communication infrastructure capabilities for Tyndall and let that be the model for how a DoD base should transform."

For one thing, turning to vendors that provide as-a-service models helps free up resources to focus on the mission. That means tech-savvy uniformed personnel are freed up for more military pursuits, such as cyber defense, or even offense. It also lowers the capital investments required to achieve these capabilities. That's because

it allows DoD to take advantage of private industry's investments rather than building capabilities out themselves. All DoD has to do is customize for mission operations.

But this also requires DoD to modernize its acquisition practices in addition to the technology, because current models can't keep up. DoD has to find new ways to acquire products and services.

"DoD recognizes they have to change the way they acquire," said Tim Blount, director of Air Force Solutions at AT&T. "If you look at what they're doing with the as-a-service models now, Army and the Air Force were both awarded on an Other Transactional Agreement (OTA), which allows them to be a little more open with how they acquire and how they track it through the acquisition system for what was assessed and what's not. They're also looking at a similar thing for 5G, where they're doing these pilots to test out different 5G capabilities."

That also allows DoD to leverage commercial best practices, which among other benefits can lend itself to better user experience. And that's something DoD employees are looking for, especially as the department is looking to embrace more flexible, mobile telework capabilities. Employees want to have the same experience at home or in the field as they do in the office. That's the end state DoD should be pushing for.

Part of that is the rapid adoption of various environments to facilitate mobility, including 5G, LTE and WiFi. Another part involves taking

a close look at DoD's virtual private network capabilities to ensure that employees could all access the network as needed. And DoD has to pay special attention to ensuring its employees are still able to collaborate effectively.

"Collaboration tools have become a major focus for the DoD, allowing them to hold meetings via Zoom, or WebEx or Teams. Now it's really become the norm," Sutherland said. "It doesn't replace face to face, but having conferences and meetings where you don't have to travel, it actually makes a huge difference in not only the financial piece, but also in the productivity of the workforce. So I think, talking to the DoD, future networking requirements are really going to be a blend of in office, teleworking, and a mobile workforce. And they're very excited about working with industry on how to make this a reality."

It also means cybersecurity benefits, such as software-defined networking, which ties in nicely with President Joe Biden's recent executive order on cybersecurity, which encouraged agencies to adopt a zero trust strategy quickly.

"I'm happy to say that the Air Force and the Army are both attacking this with a lot of vigor, because they do see that a lot of the bureaucracy that's been in place for many years just doesn't conform to the new vision world we live in, in a commercial space," Sutherland said. "So that's another important piece where we're working as a partner with the Army and Air Force in driving technology forward into the 21st century here for the DoD."

All trademarks and service marks are property of their respective owners.