FEDERAL NEWS NETWORK

# EXPERT EDITION

## Digital Modernization

**INSIGHTS ON DIGITAL MODERNIZATION FROM:**

- Federal Deposit Insurance Corporation
- NASA
- Department of Homeland Security
- NAVWAR
- Department of Veterans Affairs
- Defense Intelligence Agency
- Environmental Protection Agency
- Air Force
- Defense Information Systems Agency

## TABLE OF CONTENTS



Cloud, DevSecOps and similar tools have given the concept of managed services a new lease on life across the federal government.

Despite numerous attempts beginning in the mid-1990s to get agencies to stop worrying about the underlying technology and focus on mission, the examples of true managed services were limited to a few agencies like NASA or the Bureau of Alcohol, Tobacco, Firearms and Explosives.

But today, the Defense Information Systems Agency, the Environment Protection Agency, the Veterans Affairs Department and many others recognize the value of no longer having to worry if desktops or laptops are working or the network has enough bandwidth. Through the cloud, industry partners are telling agencies, "We will worry about the commodities and you worry about the mission."

That also means the role of the agency chief information officer has evolved.

Karen Evans, the former CIO at the departments of Energy and Homeland Security, and the former federal CIO, said, "the role of the CIO really is now at the maturity of what I think everybody had hoped or envisioned it could be, as the strategic adviser, really looking at it as a risk management officer, really analyzing the mission of the department and how do you infuse new technologies while you're looking at all the risks across the board."

But this doesn't mean CIOs can "set it and forget it."

Agencies must work with their vendor partners to focus on the outcomes they want to achieve in the managed service relationship.

Managed services and what they produce cover a wide range, from enterprise network or security operations outsourcing, to specific productivity support functions like printing, scanning, even contact tracing.

This e-book highlights the different approaches to managed services agencies are taking and the outcomes they hope to achieve. Most of all, the e-book demonstrates the trend that the customer must drive the entire process.

***Jason Miller***
***Executive Editor***
***Federal News Network***

# FDIC modernizing IT with business goals in mind

BY AMELIA BRUST

The Federal Deposit Insurance Corporation is undergoing a major network and IT infrastructure update to shift from legacy systems to cloud computing and automation. Deputy Director of Infrastructure Services Isaac Hernandez said agencies cannot target modernization based on technology alone. As the banking industry changes to meet market demands, so too must FDIC's business lines evaluate impacts on carrying out the agency's mission.

**"We've already established certain practices, such as agile — practices in our environment, where DevSecOps [would] really compliment these approaches, in order to meet our goals."**

**— ISAAC HERNANDEZ, DEPUTY DIRECTOR OF INFRASTRUCTURE SERVICES, FDIC**

The migrations of applications to low-code, no-code cloud platforms assist in reducing FDIC's on-premise footprint from data centers, and, in turn, reduces operational expenses. That also increases resiliency and reduces the likelihood of service outages, Hernandez said.

"By automating these variety of repetitive tasks such as building an environment — whether we're building servers in a virtualization environment, installing software, supporting software, applying security patches — this increases our efficiency and our accuracy that otherwise would have been lost in time productivity and costs," he said on Federal Monthly Insights – Digital Modernization: Automation month.

Automation is key to one of the agency's major goals: DevSecOp automation. Hernandez said his organization wants to combine software development, and security and IT operations. By targeting "container technologies," he said they can package these applications.

"We've already established certain practices, such as agile — practices in our environment, where DevSecOps [would] really compliment these approaches, in order to meet our goals," he said on Federal Drive with Tom Temin.

It also requires a culture change to get the necessary community buy-in. At times, people can be resistant to losing something they are comfortable with, but bringing everybody along, and making it clear that everyone's objectives and missions will still be met, is key. Hernandez said some of the DevSecOps development work is done by federal staff at FDIC, but the majority is done by contractors and partners.

**"So automation is just the foundation and in some cases, just like we find ourselves today — we're talking to each other and we're talking … virtually because of our COVID environment and in situations like this where unforeseen events can happen, we're forced to adjust our business models and automation tasks that we would traditionally do and conduct manually. We were forced to do that quickly."**

**—ISAAC HERNANDEZ, DEPUTY DIRECTOR OF INFRASTRUCTURE SERVICES, FDIC**

As for FDIC's automation priorities, he said it's important to look at the low-hanging fruit, areas which bring value to the business lines, and to not to update or automate things just for the sake of modernization.

"So with that, we started to build foundations of developing governance, for our target infrastructure framework for automation. This is important to avoid the traditional complexities that organically manifests itself in providing a maintenance and support of automation, such as what comes with the implementation of different tools and technologies," he said.

The IT modernization landscape is considerably different than it was a generation ago. If Hernandez were starting a company today, he said he could go to a cloud services provider instead of building out his own data center. And today, it's also important not to conduct retrofitting in siloes. Internally, FDIC has governance processes, various technical review boards that allow decision-making based on set criteria. Business needs a funding scope, he said, and when conflicting priorities arise, senior leadership must help facilitate the path forward based on business priorities and goals.

"So automation is just the foundation and in some cases, just like we find ourselves today — we're talking to each other and we're talking … virtually because of our COVID environment and in situations like this where unforeseen events can happen, we're forced to adjust our business models and automation tasks that we would traditionally do and conduct manually. We were forced to do that quickly," he said.

# Digital modernization saves NASA 'a lot of time, effort and money'

BY PETER MUSURLIAN

**"The infrastructure includes pretty much everything. We have three major contracts fulfilling the majority of the requirements in terms of delivery of the networks, and delivery of the hardware and software on all the application requirements across the networks, and storage solutions, etc. These are all handled throughout the agency, but we collaborate in today's world."**

**— PINAR MOORE, DEPUTY PROJECT MANAGER, NASA**

You might not think a $23 billion annual budget will have you looking for ways to pinch pennies, but if you're NASA, the cost to explore the universe can be out of this world.

Pinar Moore, deputy project manager at NASA, said watching how they spend their money is part of NASA's culture.

So some 15 years ago, NASA planted its flag into shared services to consolidate and offer centralized services for the space agency's 11 centers around the country and beyond.

"Everybody was doing their own human resources, travel processing and financial management," said Moore on Federal Monthly Insights – Digital Modernization: Automation month.

The shared services effort is headquartered at Mississippi's Stennis Space Center.

"Basically it provides services such as human resources, procurement, financial management training, an enterprise service desk, a customer contact center, and digital imaging, to name a few," Moore said on Federal Drive with Tom Temin. "I have no doubt that the incoming administration will also see the value of being competitive with private industry and getting the right people in for cybersecurity jobs."

There is a major IT infrastructure that supports those services.

"The infrastructure includes pretty much everything," Moore said. "We have three major contracts fulfilling the majority of the requirements in terms of delivery of the networks, and delivery of the hardware and software on all the application requirements across the networks, and storage solutions, etc. These are all handled throughout the agency, but we collaborate in today's world. So we have people all over the USA."

The philosophy of being tight-fisted, but also reaching beyond the technological cutting edge, has NASA always looking for the best options.

"We are looking at new tools, new services offered across the agency, such as smart anything, WiFi anywhere, laptops versus desktops, Bluetooth video capabilities, apps for our phones, small mobile devices, faster network capabilities, storage solutions, and the list goes on and on," Moore said.

Moore said NASA is continuously looking to improve, by consulting their customers, relationship managers and subject matter experts.

"We investigate all the network and infrastructure problems, hardware, software and IT services incident data to see what is working and what's not working for us," Moore said.

And one other key ingredient to staying at the top of their technological game, is asking questions.

**"Why do we need to modernize? What types of problems are we trying to resolve? How will this change deliver value to our customers? What are their expectations? Do they have the right skills to adapt? Will it require a culture change? How is our current architecture? Can it be simplified? Can we make it more secure, robust, flexible or accessible?"**

**—PINAR MOORE, DEPUTY PROJECT MANAGER, NASA**

"Why do we need to modernize? What types of problems are we trying to resolve? How will this change deliver value to our customers? What are their expectations? Do they have the right skills to adapt? Will it require a culture change? How is our current architecture? Can it be simplified? Can we make it more secure, robust, flexible or accessible? Are there any opportunities to consolidate same and similar services? What are our unique capabilities? How will modernization enhance these capabilities? Are there better and cheaper alternatives to currently what we have? Will the changes create unmanageable risks? How do we migrate? What are the critical steps? How do we realign resources to meet the demand and for transformation?" he said.

But the most important question according to Moore is, "Can we deliver quickly?"

# When it comes to digital modernization, the need to be competitive is constant

BY PETER MUSURLIAN

Karen Evans, the former chief information officer at the Department of Homeland Security, has been at the heart of high-level federal government IT decisions for nearly two decades.

"I was the CIO at the Energy Department when they elevated that position to a direct report to the secretary," Evans said on Federal Monthly Insights – Digital Modernization: Automation month. "Then I had the opportunity to go on to the [Bush] administration and look at, in essence now, the CIO for the federal government as a whole, and then come back into DHS. The role of the CIO really is now at the maturity of what I think everybody had hoped or envisioned it could be, as the strategic adviser, really looking at it as a risk management officer, really analyzing the mission of the department and how do you infuse new technologies while you're looking at all the risks across the board."

Evans arrived at the Energy Department in 2002, when the Sept. 11 attacks were in the forefront of everyone's mind.

"Through the evolution of this, you're really looking at everything now. Because every component, every type of thing that anybody wants to use, like industrial Internet of Things," Evans said on Federal Drive with Tom Temin. "There is no real perimeter that those traditional types of security models work around anymore from an information security perspective … We really did embrace it at DHS, was really looking at technology, not distinguishing between IT and operational technology, but looking at how technology is strategically used in the department."

As CIO, Evans was responsible for including security and infrastructure, among other things, to support the DHS mission. Now with a new administration, that mission continues, she said.

"It's in statute and it's near and dear to everyone in the department," Evans said. "I have no doubt that the incoming administration will also see the value of being competitive with private industry and getting the right people in for cybersecurity jobs."

Evans said she had a "partner with the lines of business folks at DHS." In fact, she called it "a great partnership." She commends management for creating that kind of environment.

**"The role of the CIO really is now at the maturity of what I think everybody had hoped or envisioned it could be, as the strategic adviser, really looking at it as a risk management officer, really analyzing the mission of the department and how do you infuse new technologies while you're looking at all the risks across the board."**

**—KAREN EVANS, FORMER CHIEF INFORMATION OFFICER, DEPARTMENT OF HOMELAND SECURITY**

**"One major accomplishment was dealing with the financial management system. One of the biggest things that happened during my tenure was bringing up the Transportation Security Administration on a modernized financial management system. I mean, that was so exciting, like watching all the different iterations of how to get a modernized financial management system with the components, so that occurred in partnership with the CFO's office."**

**—KAREN EVANS, FORMER CHIEF INFORMATION OFFICER, DEPARTMENT OF HOMELAND SECURITY**

"One major accomplishment was dealing with the financial management system. One of the biggest things that happened during my tenure was bringing up the Transportation Security Administration on a modernized financial management system. I mean, that was so exciting, like watching all the different iterations of how to get a modernized financial management system with the components, so that occurred in partnership with the CFO's office," Evans said.

Evans expected "new" and "innovative" ways to continue in the federal government that will help keep them competitive with the private sector because those behind the wheel of digital modernization never take their foot off the gas.

Another thing Evans said to keep an eye on is the DHS Cybersecurity Talent Management Service (CTMS). "That is being done jointly with the chief human capital officer … to recruit cybersecurity personnel throughout the department. And so that is going to be really exciting, and that's on the horizon. So I'm given a big plug for that, because we will be competitive with private industry with that one," Evans said.

# Why automation is a major strategy element in modernization

*Rob Smallwood, Vice President, Digital Modernization, GDIT*

THIS CONTENT HAS BEEN PROVIDED BY GDIT

In some sense, federal agencies have been modernizing their information technology systems even since they installed the first punch card reader. In contemporary times, though, modernization is driven not only by the continuous advances in technology, but also by the need to control costs and deliver state-of-the-art services.

One important strategy for better-performing, more efficient systems is automation, and the driving of automation deeper and deeper into the process that make up an agency's mission delivery. That's according to at least one expert on modern approaches to modernization: Rob Smallwood, vice president for digital modernization at GDIT.

"For any new modernizations that you're bringing to your environment," Smallwood said, "you should incorporate the necessary automations as part of that solution."

He makes the distinction between legacy applications that sought to automate manual, paper processes and an automation-first mindset needed today.

"We take an approach … of automate everywhere it makes sense," he added.

Smallwood said federal modernization efforts nowadays must start with the mission and the basic question of priorities. Agencies must determine, among the hundreds of systems they might typically operate, where to start first. Decisions may rest on cost, obsolescence, or where agencies need to improve customer service.

For example, an agency might be running equipment that is aging and soon out of warranty. Or its software might be increasingly vulnerable in a cybersecurity sense.

It's also important to establish baseline performance metrics for applications and services, Smallwood said. Then make careful inventories of all the components that make up a system. That will enable faster pinpointing of the sources of performance shortfalls, and therefore where to focus modernization efforts.

Inventories are no trivial matter, Smallwood said.

**"We take an approach … of automate everywhere it makes sense."**

**—ROB SMALLWOOD, VICE PRESIDENT, DIGITAL MODERNIZATION, GDIT**

**"You want to empower everyone at all levels to be able to automate and enable them to do their job more effectively and efficiently."**

**—ROB SMALLWOOD, VICE PRESIDENT, DIGITAL MODERNIZATION, GDIT**

"One of the first things we do we try to do in an environment is inventory everything that's there," he said. "And then correlate all that underlying infrastructure up to what are the capabilities and services actually being provided to the users. From there, you can actually start to monitor and get an enterprise view across to really understand where something might be degraded, or where some anomalies might be coming from that could impact performance."

An integrator like GDIT can aid agency IT staffs with best of breed sets of tools to help them avoid the costs and uncertainty of big coding projects when automating various functions into new applications.

"Today, you have tools like UiPath, or Live Objects or other vendors, even ServiceNow and BMC, that have those capabilities built in" Smallwood said. These tools abstract all of the underlying coding that might be required, enabling functional managers to arrange objects without having to understand coding.

This leads to the importance of an overarching governance model for automation and the modernization it supports, Smallwood said. "You don't want to stifle or cause bottlenecks in the automation being created. You want to empower everyone at all levels to be able to automate, and enable them to do their job more effectively and efficiently."

That's possible when multifunctional teams exist within a governance framework for modernization.

Another advantage of working modernization through an integrator, Smallwood said, is that it lets an agency offload the risk of dealing with emergent vendors who possess innovative technology but might have an unproven performance record.

"We can help navigate those obstacles to better enable federal agencies to take advantage of these emergent technologies and vendors," he said.

Finally, Smallwood advised, it's wise for agencies to borrow a page from the agile approach to software development and apply it to automation projects. That is, working incrementally.

He said, "Almost every project that we take on, we work within sprints, working incrementally to move the ball forward."

# Naval Information Warfare Center wants to 'push the envelope' on managed services

BY AMELIA BRUST

Managed services is helping federal agencies simplify operations and have more predictable. One agency contracting with a vendor to deliver ongoing functional requirements is the Naval Information Warfare Center Atlantic.

Teri-Lee Holland, division head for data center and cloud hosting services, performs engineering work for sailors, including cloud hosting services for payroll and HR systems. Her office provides managed services — through industry partners — that mission owners or application owners use, rather than each of our individual application owners providing those services to themselves.

"So let's just take something very basic, like scanning our environments: Instead of each of our mission owners scanning their individual environments, we scan across the full environment, and can provide those scan results not only to our mission owners, but up to [U.S.] Fleet [Cyber Command], so that they can see across the complete infrastructure," she said on Federal Monthly Insights — Digital Modernization (Managed Services).

There are advantages and challenges to the Navy using the Naval Information Warfare Center (NIWC), the former being that Holland's office can reduce the amount of time and resources needed to scan the environment. For example, if each application owner had its own scanner for 100 systems, that would require 200 full-time employees and 200 servers to have a scanner attached.

"We've reduced that to, let's just estimate 10 FTEs across the 100 applications, and then a minimal number of servers to host the scanners so that we can scan the full environment," she said on Federal Drive with Tom Temin. "You're really reducing and pooling those resources together. And those resources are reachable using our incident response process, so our mission owners can submit a ticket and say, 'I need a scan.' And then we have a team of people that go for that."

**"And right now, one of the things that we are looking into is how do we automate as much as we can to move systems from an on premise, legacy data center environment into the cloud. But not just to lift and shift; we want to be innovative and say, 'How do we do that so they can really take advantage of what the cloud offers?' And so those discussions, those pilot efforts are underway, and we're really excited to be hopefully pushing the envelope there."**

**—TERI-LEE HOLLAND, DIVISION HEAD FOR DATA CENTER AND CLOUD HOSTING SERVICES, NAVWAR**



**"The advantage of using cloud native is they've pretty much automated everything that they can, and they continue to work in automation. We are still providing very manual managed services. That's kind of the nature of the requirement that we have on policy, and that's a constant discussion that we're having with officials across the Navy and DoD is how do we meet the same policy we're charged with meeting, but in an automated way?"**

**—TERI-LEE HOLLAND, DIVISION HEAD FOR DATA CENTER AND CLOUD HOSTING SERVICES, NAVWAR**

NIWC Atlantic encompasses a workforce of more than 9,000 Defense Department civilians, military and industry partners. It takes data centers in Charleston, South Carolina; New Orleans, and a disaster recovery site in Kansas City — although these days, Holland said the workforce is scattered across the country.

Her office bundles all of its services to mission and application owners with a single bill, similar to a cell phone bill, and customers can add or remove services as they need. NIWC Atlantic is not the only managed services provider across the Navy, but making those platforms more widely available does drive down costs for mission owners, Holland said.

Since NIWC Atlantic began piloting cloud infrastructure in 2016, their processes across the Department of the Navy and Defense Department have matured to bring cloud-native managed services to application owners. Holland is excited to see what is ahead: namely, more collaboration to take advantage of managed services.

"The advantage of using cloud native is they've pretty much automated everything that they can, and they continue to work in automation," she said. "We are still providing very manual managed services. That's kind of the nature of the requirement that we have on policy, and that's a constant discussion that we're having with officials across the Navy and DoD is how do we meet the same policy we're charged with meeting, but in an automated way?"

Automation and the services already put into cloud regions are less competitive for NIWC Atlantic because those are only the services that the agency can utilize. But services which are not yet automated — that's where Holland said her office specializes, where they can get the information the Navy and Fleet Cyber Command need to ensure security of the network. The migrations for data center consolidation in 2011 and 2012 were some such examples of manual processes.

"And right now, one of the things that we are looking into is how do we automate as much as we can to move systems from an on premise, legacy data center environment into the cloud," she said. "But not just to lift and shift; we want to be innovative and say, 'How do we do that so they can really take advantage of what the cloud offers?' And so those discussions, those pilot efforts are underway, and we're really excited to be hopefully pushing the envelope there."

# From pandemic to SolarWinds to ice storms, managed services saving VA's help desk from customer woes

BY AMELIA BRUST

When a hurricane or some other natural disaster hits a Department of Veterans Affairs facility, and the agency's Office of Emergency Management responds, it needs to know its IT equipment will work.

That falls to VA's Office of Information Technology, which is part of a growing trend of federal agencies that use managed services. This approach allows agencies to shed the costs of owning and updating the infrastructure needed to supply continuous services.

Right now, Lynette Sherrill, the Office of Information Technology's executive director of Enterprise Command Operations, said her organization is almost entirely virtual due to the pandemic. In addition, although they are based in Austin, Texas, Sherrill said neither the SolarWinds cyber breach nor the recent winter storm, which knocked out most of the state's power – including at her own home – was enough to stop central data center operations. That was a relief considering the enterprise service desk is one of the most complex service desks in the entire U.S. IT industry, running about 60,000 calls per week, she said.

"It is running about 3 million calls a year, and handling and touching more than 5.5 million tickets a year," she said on Federal Monthly Insights – Digital Modernization (Managed Services). "And we have about 575 agents on the phones throughout the week to respond to any it issues that VA may have. So scale and scope here is a big deal."

When VA pushed out about 150,000 end users to their homes as the result of the pandemic, many of whom were first-time teleworkers, the service center took those calls, she said. Agents had to help with needs such as laptop set-ups and network connections remotely, and in the first eight weeks, call volumes doubled.

It is a feat she said only a managed service provider could have spanned as quickly as it did.

"At the Service Desk, we have a managed service provider contract, and they were able to mine the data of the tickets that were coming in, give us that feedback and say, 'Hey, it's all: How do I get my computer set up?' And that allowed us to partner with them and very quickly create a video that we published on the VA.gov website," Sherrill said on Federal Drive with Tom Temin. "And in the front-end messages, users called into the service desk, we point them to that video so that they could at least try themselves while they're waiting on the phone because these calls take an hour or longer. And when our average handle time at a service desk – you plan for anywhere from 8 to 12 minutes."

It kept customer satisfaction rates high during a time when there was also increased empathy from people who may otherwise be annoyed at the long wait times, she said. The managed service provider surged and brought in an extra 200 agents on the phone within three weeks. But Sherrill said that was because the provider's contract with VA is based on a service-level agreement, not the number of people they have. The contract also has two key metrics: Critical performance indicators and key performance indicators.

"The critical performance indicators are the ones that drive the contract incentives or disincentives as the case may be, our critical performance indicators are first-contact resolution," she said. "We don't want the customer to have to wait for anything if we can help it. But… if it's a more complex problem that the agents can't resolve, then we do have to send it off."

There is also the indicator of average speed to answer, which is usually around 45 seconds. At the height of the pandemic, that critical performance indicator "was blown out of the water, because there's no way they could answer – they could have put 10,000 agents on the phone and not [be] able to answer in 45 seconds," she said.

VA also introduced chatbots to shift some users off the phone lines and off agents' workloads. Still, Sherrill said that an agent can handle up to eight chatbots at a time, depending on the agent's experience level. She sees the technology being used more going forward. But she clarified that chatbots are not the same as a traditional live chat session with an agent on the other end. Chatbot is artificial intelligence technology that has a workflow behind it and can connect a customer to an agent, but the customer can also ask it questions to search prior to that connection.

"But at any point, when the customer says, 'Hey, I'd like to speak to somebody' – the chat bot knows to immediately try to connect them to an agent," she said.

**"At the Service Desk, we have a managed service provider contract, and they were able to mine the data of the tickets that were coming in, give us that feedback and say, 'Hey, it's all: How do I get my computer set up?' And that allowed us to partner with them and very quickly create a video that we published on the VA.gov website."**

**—LYNETTE SHERRILL, EXECUTIVE DIRECTOR OF ENTERPRISE COMMAND OPERATIONS, OFFICE OF INFORMATION TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS**

**VA also introduced chatbots to shift some users off the phone lines and off agents' workloads. Still, Sherrill said that an agent can handle up to eight chatbots at a time, depending on the agent's experience level. She sees the technology being used more going forward.**

# Defense Intelligence Agency emphasizing customer centricity in 5-year strategy

BY AMELIA BRUST

A new strategy from the Defense Intelligence Agency Chief Information Office published at the beginning of 2021 helps lay out the agency's data and IT goals. The document was not only for its employees and other agencies the DIA works with — it was also a message to vendors and other partners on what the needs are and how they can help.

It's also a "tweaking" of the DIA CIO Strategy for 2021-2025 released last year, which is broken up into four overall goals: Drive customer centricity, deliver data to the point of need, optimize the DIA CIO core, and equip the workforce. As for that fourth goal of equipping the workforce, DIA's CIO Jack Gumtow said the term "workforce" was clarified to include vendors and academic partners.

"Customer centricity" stems from the common assumption that IT does things for IT's sake rather than for customer purposes, he further explained to Federal News Network Executive Editor Jason Miller.

"Customer centricity is really about getting engaged with the customer or your partner, as the case may be, and understanding what they really want to do — not in a, 'Hey, I need this system, can you go build it?' but it's their daily OODA loop. So we understand ahead of what they're doing, that we can anticipate their needs, and then validate those needs with them, and then move out," Gumtow said on Federal Monthly Insights — Digital Modernization (Managed Services). OODA loop stands for "observe, orient, decide, and act," a type of military decision-making process.

He also said DIA stood up a customer experience group that brings together personnel from another center or within the CIO's office, to hold discussions of what works or doesn't. The iterative process helps IT staff become more ingrained with customers' needs.

**That transparency extended to what OCIO staff were doing, to their customer interactions, to budgets and to goals or objectives. Gumtow said this approach would limit any doubts that the CIO's office was acting in others' best interests — not just their own.**

"Another piece of this is in the past, CIO writ large has been not as transparent as what I would like to see," Gumtow said on Federal Drive with Tom Temin. "So when I came into this job almost three years ago, June of 2018, one of my first goals going in is transparency."

That transparency extended to what OCIO staff were doing, to their customer interactions, to budgets and to goals or objectives. Gumtow said this approach would limit any doubts that the CIO's office was acting in others' best interests — not just their own.

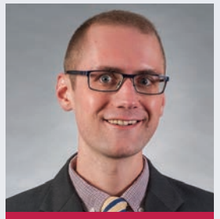
Meanwhile, cloud computing crosses all four strategy goals, and developments such as the Commercial Cloud Enterprise (C2E) contract recently awarded to IBM, Google, Amazon, Microsoft and Oracle makes for some exciting possibilities, Gumtow said. He predicted a large learning curve to become fully conversant in cloud technology, and that factoring physical limitations including transport lines and the potential for network outages must be considered for the cloud ecosystem.

"So you have to have that level of redundancy and resiliency built into it. And it can't be just a single node, cloud node back on the East Coast that provides support to the whole world. That's just not feasible," Gumtow said. "So the opportunity [of] C2E with multiple clouds, multiple opportunities — yeah, it's exciting within the constraints that I said that, hey, there's a level anxiety of ensuring that we understand how to orchestrate across all that."

**"Customer centricity is really about getting engaged with the customer or your partner, as the case may be, and understanding what they really want to do — not in a, 'Hey, I need this system, can you go build it?' but it's their daily OODA loop. So we understand ahead of what they're doing, that we can anticipate their needs, and then validate those needs with them, and then move out."**

**—JACK GUMTOW, CHIEF INFORMATION OFFICER, DEFENSE INTELLIGENCE AGENCY**

# How and why to sign up for contemporary managed services



*A.J. McNamara, Director, Managed Services, GDIT*

THIS CONTENT HAS BEEN PROVIDED BY GDIT

Managed services have come a long way in the 30 years since federal agencies first sought to escape the cycle of buying, maintaining and replacing PCs and the software they ran. Today vendors offer a range of up-to-date programs that lower the capital expenditure, or CapEx, obligations and move them to a recurring fee operational expense, or OpEx model.

Why does that matter?

Managed services "really enables that organization to achieve cost efficiencies, improve operations, realize value, and also free themselves up to focus on their mission," said A. J. McNamara, the director of managed services at GDIT.

**"[Managed Services] really enables that organization to achieve cost efficiencies, improve operations, realize value and also free themselves up to focus on their mission."**

**—A.J. MCNAMARA, DIRECTOR, MANAGED SERVICES, GDIT**

For several administrations, policy has emphasized the OpEx model because of several benefits. Among them – and one McNamara underscored – is having predictable costs, and thereby freeing capital for investment in infrastructure modernization or development of new applications and services.

But managed services are about more than simply costs. McNamara said that properly structured, managed services can lead to better performance, whether some crucial function like security operations or printing, or of the mission itself.

"They're really about outcomes," he said.

When thinking about managed services therefore, the process must start with thinking not so much about specific requirements or service level agreement details, but rather about the outcomes the agency wants.

Managed services and what they produce cover a wide range, from enterprise network or security operations outsourcing, to specific productivity support functions like printing, scanning, even contact tracing.

"We partner closely with the agencies and really focus on what is the outcome that they need to achieve," McNamara said, adding that without that initial understanding it's difficult to proceed to requirements and SLAs that will support what the agency really wants.

Another way to think about managed services is whether they are what GDIT terms transformational and transitional.

Transformational "is like it sounds," McNamara said. "You take a service and you adopt it very quickly. You're transforming into this managed service delivery model." He cited the Veterans Affairs Department, in which GDIT consolidated 12 help desk centers, assuming operation of them and delivering help desk as a service departmentwide.

The transitional approach move the agency more incrementally, examining each type of services "in a more methodical and thought out way." GDIT is conducting that approach with NASA, where 60 separate services are in the queue.

When contemplating managed services, it's important to understand some of the challenges and even misperceptions about managed services that may exist in the agency. For example, McNamara said, moving to managed services – and to the OpEx model itself – requires something of a cultural change in organization oriented toward capital spending and equipment capacity planning.

**"One of the big things we really focus on is developing clear outcomes-based service level agreements and clear transparency. And it's important these goals are shared across the whole organization."**

**—A.J. MCNAMARA, DIRECTOR, MANAGED SERVICES, GDIT**

"Misperceptions that people have with adopting managed services primarily concern loss of control, lack of flexibility, in general fear of change," McNamara said. "One of the big things we really focus on is developing clear outcomes-based service level agreements and clear transparency," he added. "And it's important that these goals are shared across the whole organization, not something that only the CIO believes."

As for SLAs, McNamara reiterated the need for an outcome orientation. He cited the example of financial reporting, where the requirement is for delivery of a financial report on the first day of every quarter.

"Traditionally, the SLA is simply based on, what is the availability of the system. But not actually on whether the system is available on that day." That is, an SLA that specifies a certain uptime percentage, but under which the system might fail on the first of the month – that's not an outcomes based SLA.

# EPA wants to build cybersecurity-aware culture along with IT modernization

BY AMELIA BRUST

Where IT modernization is concerned, the Environmental Protection Agency's technology leader said, "everything is fair game."

EPA CIO Vaughn Noga said historically the agency has evaluated IT systems and applications continuously, rather than just when something becomes obsolete. He said his organization is routinely looking for more efficient and cost-effective solutions.

"We've been fairly successful. I think one of our one of our biggest challenges, quite frankly, is our desire to evolve is faster than our resources can support both in funding and in people," Noga said on Federal Monthly Insights – Digital Modernization: Enterprise Modernization.

Nevertheless, he stayed positive about this challenge, adding that in his view it reveals a dedicated workforce. Several years ago, Noga and his team established a set of "wildly important goals" which he said have strengthened since the pandemic. The first goal was to create a cybersecurity-aware culture and reduce barriers to fielding and operating new applications and systems.

"And it's a long way of saying we need to make it easier for our state agency stakeholders. We need to focus on how do we field systems, how do we take them through the [extract, transform, load] process?" he said on Federal Drive with Tom Temin. "And quite frankly, we need to reduce the barrier and the burden on our stakeholders, so they can they can be productive much quicker."

The CIO's office is also ensuring that data is accessible and driving decision-making – that means using data that as close to 100% digital as possible. To this end, EPA last year looked at all information collection requests and identified opportunities to move paperless activities to digital, Noga said.

**"And it's a long way of saying we need to make it easier for our state agency stakeholders. We need to focus on how do we field systems, how do we take them through the [extract, transform, load] process?" And quite frankly, we need to reduce the barrier and the burden on our stakeholders, so they can they can be productive much quicker."**

**—VAUGHN NOGA, CHIEF INFORMATION OFFICER, ENVIRONMENTAL PROTECTION AGENCY**

This enables work from anywhere or anytime, which he said became more important over the last year and revealed an opportunity to rethink business processes.

"I think it's one of the things that we tend to overlook when we're [in] normal operations is the business process," he said. "But when you change the way you conduct business, it gives you an opportunity to actually re-address those and relook at your business processes to rethink them."

Noga said it is easy to fall victim to "shiny object syndrome" and let the discovery or availability of new technologies drive modernization. However, he said, his predecessor, was skilled at engaging senior leadership during the application review process.

"So when someone identifies a need or an opportunity to develop an application, before they go off and develop it, they submit it for review and the senior IT leaders look at it," Noga said. "They may comment to it. They may say, 'Hey, that sounds like a great idea, I want to be part of this effort.' And from there, you really look at what are the internal technologies you currently have that could support that before you go off and look for new technologies."

**"So when someone identifies a need or an opportunity to develop an application, before they go off and develop it, they submit it for review and the senior IT leaders look at it. They may comment to it. They may say, 'Hey, that sounds like a great idea, I want to be part of this effort.' And from there, you really look at what are the internal technologies you currently have that could support that before you go off and look for new technologies."**

**—VAUGHN NOGA, CHIEF INFORMATION OFFICER, ENVIRONMENTAL PROTECTION AGENCY**

One caveat for EPA is that Noga's office is tied to systems operated by regulated industries or by states, which collect data on emissions and related matters – data that is then sent to the agency. So if EPA wants to modernize its technology beyond what those reporting parties are using, that is where the Central Data Exchange comes into play. EPA began an initiative called CDX Reimagined so that regulated entities can do business with the agency more easily.

Overall, Noga said EPA wants to create a cybersecurity-aware culture, and that requires a fair amount of educating the workforce about what to look for in the systems, which they put in place to protect against malicious actors.

"And part and parcel of that is working with them to understand what their role is in protecting the IT systems and the data and the assets of the EPA," he said.

# Air Force determining if managed services can help consolidate data across bases

BY AMELIA BRUST

For the Air Force's enterprise IT and cyber infrastructure division, connecting airmen and guardians with the data they need along the entire transactional path, to do their mission, is the focus.

Col. Bobby King, senior materiel leader for the division, said that starts with the endpoint devices and any software or security tools which are on those devices. The data, as he said, "is all over the place," including in a Cloud One program and at various data centers at bases.

King said the different bases and organizations operate their own data centers with various costs and capabilities. He sees an opportunity to be more efficient – by consolidating much of that disparate data into the cloud.

"It also makes the connectivity to that data much easier – and wherever the guards can reach it, no matter where they are around the world," he said on Federal Monthly Insights – Digital Modernization: Enterprise Modernization.

**"It also makes the connectivity to that data much easier – and wherever the guards can reach it, no matter where they are around the world."**

**— COL. BOBBY KING, SENIOR MATERIEL LEADER, ENTERPRISE IT AND CYBER INFRASTRUCTURE DIVISION, AIR FORCE**

From an IT infrastructure perspective, the Air Force wants all of the service's bases to look the same, which is currently not the case. Maj. Gen. Michael Schmidt – program executive officer for the Command, Control, Communication, Intelligence and Networks (PEO-C3I&N) at Hanscom Air Force Base, Massachusetts – said they have supported IT infrastructure in a piecemeal fashion with end-of-year funding for a while.

"Having an enterprise-level Help Desk, not a help desk necessarily at every base that is different … there's a lot of things that we can do by pulling that IT infrastructure together, having a common infrastructure across all of our bases, and everything from security to user experience all benefit from getting to that goal," Schmidt said on Federal Drive with Tom Temin.

That is why his organization asked commercial vendors about the best way to do that. Enter managed services – the idea of outsourcing IT functions to a third party.

Schmidt said the Air Force is using its enterprise IT as-a-service risk reduction effort to determine what it would incentivize for managed services providers in their service level agreements, such as the time it takes to answer help desk calls, or system up time.

"During the risk reduction effort, we're being very careful not to unnecessarily link payments to contractors, to those SLAs – not that we're not holding them responsible for everything, because we are – but at the same time, we want them to tell us what SLA's they think we should use," he said. "And so ultimately, as we move into production, and really try to incentivize financially the contractors, that we're confident that we have the right SLAs that we're putting on the contract."

**"Some of the most important SLA's are subjective, and that is really a challenging thing to deal with from a contractual standpoint. So user experience, measured by user satisfaction, to me, is the most important metric out there. But that is a hard one to contractually incentivize."**

**—MAJ. GEN. MICHAEL SCHMIDT, PROGRAM EXECUTIVE OFFICER, COMMAND, CONTROL, COMMUNICATION, INTELLIGENCE, AND NETWORKS (PEOCIN), AIR FORCE**

His office needs to ensure contracting vehicles and the SLAs are flexible enough, in case funding is unstable in a given year. Schmidt said they cannot afford to put the government in a position of paying for something it did not receive, or which led them down a different, more challenging path for King's division than expected.

"Some of the most important SLA s are subjective, and that is really a challenging thing to deal with from a contractual standpoint," Schmidt said. "So user experience, measured by user satisfaction, to me, is the most important metric out there. But that is a hard one to contractually incentivize."

# Air Force pursues lines of effort for IT risk reduction at bases

BY AMELIA BRUST

If it could, the Air Force would prefer to have airmen and guardians only perform the work they need to do – and find other solutions where possible. This presents a major industry partnership opportunity, according to two of the military branch's technology leaders.

Since 2017 the Air Force has been examining risk reduction which, as Col. Bobby King, senior materiel leader for the enterprise IT and cyber infrastructure division, told Federal News Network, is divided up into three lines of effort: network-as-a-service, end user services, and compute and store. The Air Force awarded other transaction agreements to Microsoft and AT&T to provide commercial solutions for network as a service in 2018.

The end user services line of effort refers to everything that airmen and guardians will interact with, from the endpoint, the operating system and security tools on that endpoint, and the enterprise or local help desks.

**"There's some elements to working with the cloud that we wanted to explore in a risk reduction effort to augment and improve that enterprise-provided cloud – Cloud One. And so we awarded an OTA for compute and store. And the idea there was to have a single pane of glass that allows the vendor partner and the Department of the Air Force to see everything going on in the cloud,as well as get after the on-prem, disconnected ops-types requirements that were provided to us from our lead [major command] – Air Combat Command."**

**— COL. BOBBY KING, SENIOR MATERIEL LEADER, ENTERPRISE IT AND CYBER INFRASTRUCTURE DIVISION, AIR FORCE**

As for the "computer and store" line of effort, King said in a continuation of the interview, the Air Force has a Cloud One program as well as 74 live mission systems.

"There's some elements to working with the cloud that we wanted to explore in a risk reduction effort to augment and improve that enterprise-provided cloud – Cloud One," he said on Federal Monthly Insights. "And so we awarded an OTA for compute and store. And the idea there was to have a single pane of glass that allows the vendor partner and the Department of the Air Force to see everything going on in the cloud, and as well as get after the on-prem, disconnected ops-types requirements that were provided to us from our lead [major command] – Air Combat Command."

But how does the Air Force conclude what is a good user experience?

Maj. Gen. Michael Schmidt – program executive officer for the Command, Control, Communication, Intelligence, and Networks (PEOCIN) at Hanscom Air Force Base, Massachusetts, said that what is right for an airman at one base might not support the mission at another base if the technology needs are different.

"I would say we are trying to capture the enterprise level requirements, that would be the common denominator in general across all bases at the same time, [King] has a number of teams – actually, we do both on Bobby's collateral side and our on our classified side of going out and right now, we're doing these [Advanced Battle Management System] experiments or [joint all-domain command and control] demonstrations at various places around the world," Schmidt said on Federal Drive with Tom Temin**.** **"**And we're sending our teams out to really, if you will, help trick out those bases, even though they might not be risk reduction bases for [enterprise IT as a service]."

Schmidt said the Air Force knows which bases have "kind of an ancient infrastructure" relative to their data needs and mission requirements. The service sends teams to help each base individually, rather than on a per-experiment basis. He said having those teams of people who know the true ins and outs of the Air Force's IT infrastructures and be hands-on has proven to be the most effective method.

**"And we're really seeing some quick wins at some of these bases that we didn't get – maybe we didn't know before, why they seem to have so many problems? So it's been really helpful tying ABMS or JADC2 experiments or demonstrations to some of our IT infrastructure, things that we're trying to get after."**

**—MAJ. GEN. MICHAEL SCHMIDT, PROGRAM EXECUTIVE OFFICER, COMMAND, CONTROL, COMMUNICATION, INTELLIGENCE, AND NETWORKS (PEOCIN), AIR FORCE**

"And we're really seeing some quick wins at some of these bases that we didn't get – maybe we didn't know before, why they seem to have so many problems?" he said. "So it's been really helpful tying ABMS or JADC2 experiments or demonstrations to some of our IT infrastructure, things that we're trying to get after."

# Digital modernization never finished for DISA, but chasing trends isn't the answer

BY AMELIA BRUST

Modernizing information technology needs to happen continuously, especially if that technology serves an enterprise as large and diverse as the Defense Department. However, continuous modernization can lead agencies to think they have to update a lot at once – causing a "technical deficit."

It will take a shift in thinking, said Steve Wallace, systems innovation scientist at the Defense Information Systems Agency. He said DoD needs to apply DevSecOps-type processes across the board, in order to have smaller micro deployments.

"That constant evolution is key," Wallace said on Federal Monthly Insights – Digital Modernization: Enterprise Modernization. "That way, it's not such a huge shift every time – but again, just that constant evolution."

His colleague Raju Shah, director of the Enterprise Engineering and Governance Directorate at DISA, said it is also a matter of continuous "learning." Clean, reliable and useful data is key to the enterprise's main goal: Delivering IT for all of DoD and consistently provide a good experience to warfighters – at a speed that enables them to empower the decision-making, Shah said.

"As our commander has stated, velocity of delivering the services is a key. And that's the area we are continuously invest[ed] with … specifically, zero trust principles, and using automation and orchestration, to provide the speed – not only the speed, but also remove the human factors and utilization of data," Shah said on Federal Drive with Tom Temin.

Embracing technology to meet mission requirements, while also not chasing new technology just for the newness of it, requires a balance.

"You could create the best widget, if you will, in the world, but if it doesn't satisfy the actual need, that widget goes on a shelf, and is never useful to anyone, and it never sees the light of day," Wallace said.

**"As our commander has stated, velocity of delivering the services is a key. And that's the area we are continuously invest[ed] with … specifically, zero trust principles, and using automation and orchestration, to provide the speed – not only the speed, but also remove the human factors and utilization of data."**

**—RAJU SHAH, DIRECTOR, ENTERPRISE ENGINEERING AND GOVERNANCE DIRECTORATE, DEFENSE INFORMATION SYSTEMS AGENCY**

Often a solution already exists in the department or elsewhere in the government, which can be leveraged or adopted faster than if something needs to be built from scratch, he said. His advice was to make sure exploring new technology was a small part of an organization's overall effort – not the primary objective.

One modernization project that DISA is deploying throughout DoD now is the Defense Enterprise Office Solution (DEOS). Wallace said it is mainly a collaboration platform but DEOS' new tools will also generate large amounts of data – which will last longer than many other tools. DEOS is also a cloud technology, which Shah said is central to digital modernization.

Beyond cloud computing, the armed services often require some type of edge computing to counterbalance environments where broadband may be unavailable. Shah and Wallace also said edge computing is helpful because it can optimize data locally, rather than transmitting it back to the cloud. This is important because the more data which is generated, the more useless data is also generated – and not all of it can or needs to be analyzed.

All of this is to say that digital modernization means to continuously examine a system's architecture. For Shah and Wallace at DISA, there is no such thing as sustainment. In addition, no matter how long or hard the team has worked on one piece of technology, they must always be prepared to set it aside for something new coming down the pike.

"This is a constant evolution – if you sit still, you're going to lose," Wallace said. "And so, we have to constantly be looking at how we can make ourselves better. It's just like an athlete."

**"This is a constant evolution – if you sit still, you're going to lose. And so, we have to constantly be looking at how we can make ourselves better. It's just like an athlete."**

**—STEVE WALLACE, SYSTEMS INNOVATION SCIENTIST, DEFENSE INFORMATION SYSTEMS AGENCY**

# Digital modernization starts with the mission, not the digits

*Gwen Cadieux, Director, Enterprise IT & Managed Services, GDIT*

THIS CONTENT HAS BEEN PROVIDED BY GDIT

Technology refresh, business process improvement, and improving services delivered to customers and constituencies – they're all inputs to the ongoing modernization efforts at federal agencies. Agencies caught in the technical debt of outdated technologies are finding the soundest approach to modernization is not simply to upgrade technology for technology's sake, but rather to approach modernization from the outside in. It means looking at the desired service outcome, than reworking process behind the scenes to enable the service, then choosing the best technology to support the process.

Gwen Cadieux, the director of enterprise IT and managed services at GDIT, is a strong proponent of that approach, having seen it succeed across a variety of agencies.

The outside in approach also lets agencies manage another crucial element, namely the budget.

"I think one of the biggest issues is the budgets, not only the size of the budgets, but the budget cycles, and being able to fit the amount of modernization that takes place, or needs to take place with some of our enterprises, and within those budgets," Cadieux said.

**"We have tools that help us identify those dependencies [to mission delivery plans] and keep track of those dependencies as the baseline continues to change."**

**—GWEN CADIEUX, DIRECTOR, ENTERPRISE IT & MANAGED SERVICES, GDIT**

She said that by taking a technology-first approach to modernization, agencies often risk siphoning off dollars unnecessarily by acquiring redundant products. Cadieux cited one agency that had purchased seven network management tools, each for a different segment of the network, each needing its own maintenance and upgrade costs. She cautioned against the "shiny object syndrome" when presented with new products. Better to ask, "Okay, that's great, but what problem are you trying to solve with that? Do you really need that right now?"

Another risk of adding technology is that it can interfere with technical dependencies within or among complex systems. Cadieux said an integrator like GDIT, with its constellation of best-of-class technology partners, can help an agency strategize technology modernization, taking into account dependencies and refresh cycles. Ideally, this happens within the context of the mission delivery plans that should be driving the product acquisitions.

**"The true driver [to modernization] is the speed of change, and how quickly you need to get new capabilities, new technologies into an architecture."**

**—GWEN CADIEUX, DIRECTOR, ENTERPRISE IT & MANAGED SERVICES, GDIT**

"We have tools that help us identify those dependencies and keep track of those dependencies as the baseline continues to change," Cadieux said.

For example, she added, "You don't just start ripping out routers and putting in software defined network routers. You have to plan that out. You have to understand what the implications are across your enterprise."

Cadieux said agencies are finding success in the incremental but continuous approach to digital modernization. That means determining a single, mission or service delivery requirement. Then designing the technical means to achieve it. Surprisingly, she said, this can deliver more improvement faster than the outdated grand design, big bang, or waterfall development approaches of the past.

"The true driver is the speed of change, and how quickly you need to get new capabilities, new technologies into an architecture," Cadieux said. "It's an iterative process. You don't really have the time to wait until you get all the way to the end."

In this manner, customers can see progress while offering feedback on the next round of capabilities needed. In other words, use the DevOps or DevSecOps model.

"I think most of our customers are comfortable or familiar enough with the DevSecOps process that it's not as hard a sell as maybe 5 or 10 years ago," Cadieux said.

Cadieux said emerging technologies such as 5G telecom, robotic process automation and artificial intelligence will transform mission delivery and bring all sorts of new efficiencies to agencies. But agency teams must first establish the mission need, she said.

Important to establishing the mission need, she said, is involving all of the parties with a stake in modernization. That includes the users themselves.

"If you don't talk to them," Cadieux said, "you're missing a huge piece of your of your requirements and information to help inform better decisions about what kind of technologies you may or may not need."

GDIT

For more information visit:
**https://federalnewsnetwork.com/digital-modernization/**