

STRATEGIC GUIDANCE SURVEY

# Perspectives: Pandemic and IT Modernization



Brought to you by





We use the term “silver lining” a lot when it comes to the coronavirus pandemic and this new normal of working and living. But there are few places in the federal sector that this term resonates more than in the technology offices around the government.

Agencies used the urgency of the pandemic emergency to make the kind of progress around IT modernization rarely seen over the past 20 years.

Not since the massive data breach suffered by the Office of Personnel Management in 2015 and, maybe, Y2K before that, have agency chief information officers found the leadership support, the resources and the partnership from industry to make such significant progress.

Jeff Seaton, NASA’s acting CIO, said “We experienced three years of transformation in the first three months of the pandemic.”

The question now is how can agencies maintain and sustain that realization that technology is more than just the laptop or cell phone, and IT and the workforce combined are the only things that make the agency mission successful?

In this ebook, CIOs and technology executives from civilian agencies tell their pandemic success stories and how it’s setting their IT modernization and digital transformation journeys up for future success.

At the Interior Department, Karen Matragrano, Interior Department deputy CIO for the enterprise services division, said the agency “is on the leading edge of truly modernizing network services. Through the use of software-defined wide area network and collaboration with the Department of Homeland Security on Trusted Internet Connections 3.0, DOI will revolutionize the way users access the resources they need to do their jobs.”

In the end, that’s what all this IT modernization talk is about: changing the way federal employees serve citizens and meet their missions.

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

#### **FEATURED CIVILIAN AGENCY EXECUTIVES:**

**Wayne Jones**, National Nuclear Security Administration CIO

**Jeff Seaton**, NASA acting CIO

**Karen Matragrano**, Interior Department deputy CIO for the enterprise services division

**Chris Chilbert**, the CIO for the Department of Health and Human Services Office of the Inspector General

**Ryan Cote**, Transportation Department CIO



## Discuss how you modernized your network and services over the course of the last 7 months as the pandemic took hold and remote working and remote services surged. How did the pandemic create a sense of urgency for IT modernization?

**Jones:** The pandemic has shifted the National Nuclear Security Administration's traditional work environment. The Department of Energy and NNSA have had to make modifications and updates to support a primarily virtual workforce. DOE and NNSA coordinated to deploy devices to those in need, to expand bandwidth to support a heavier load on our virtual desktop infrastructure and increased the number of licenses for existing teleconferencing technologies to support virtual communication among employees. The rapid change to a remote workforce highlighted a need for additional technology solutions. Staff from the Office of the Associate Administrator for Information Management and Chief Information Officer worked with NNSA's program offices to identify and evaluate a list of services and solutions needed to support the mission goals and objectives. These unprecedented circumstances have prompted us to rethink components of the NNSA OCIO modernization roadmap, and we adjusted our plans to meet more pressing and immediate demands to support a virtual workforce. It is important to note however that due to NNSA's mission, our telework arrangement is more unique than other federal organizations, and 100% telework may not be feasible for some of our mission essential work. NNSA's modernization efforts were well underway prior to the COVID-19 crisis. We took a hard look at what the Federal CIO put out with regard to cloud-based technologies and wanted to follow that framework. Our classified network modernization initiative is divided into three distinct phases. We are currently in phase one, which establishes the architecture base for the network infrastructure upgrade. Phase

one encompasses coordination among mission owners across NNSA program offices and the nuclear security enterprise to perform application rationalization for mission IT applications. This evaluation of applications will be used to determine the best method of migration for current applications onto the modernized classified network.

**Seaton:** We have enabled the NASA workforce to securely work from anywhere for many years. As an agency, NASA already supported occasional telework prior to the pandemic, and many of our projects rely on matrixed teams collaborating from multiple locations across the country to execute our highly complex missions. To support this dynamic, complex and mobile workforce, we've been investing in network upgrades, cloud-based collaboration tools and cybersecurity improvements for the past several years. At NASA, we've also been moving away from standalone desktop computers to mobile laptops to support how our distributed, mobile teams work. Thankfully, these modernization investments put us in a relatively good position to address the significant and sudden change in our work environment caused by the pandemic, as about 90% of the NASA team began working remotely by the end of March this year. We also regularly conduct center and agency telework exercises to test our systems and to learn from and resolve any issues. The lessons we've learned through our Continuity of Operations Program and telework exercises enabled us to rapidly and seamlessly transition into what has become an extended telework environment. For us, the biggest issue was not



modernizing our technology, but changing the way we work to capitalize on the tools that were already available. I like to say we experienced three years of transformation in the first three months of the pandemic. As most of our teams moved to remote work in March of this year, the NASA workforce, out of necessity, learned to use IT-based collaboration tools like video meetings and collaborative, online content creation in ways that many had not before. I think we were all somewhat surprised at how quickly and seamlessly we were able to transition to remote working. I am incredibly proud of NASA's Office of the Chief Information Officer team, including employees and contractors at the centers, who have put in long hours to keep our

IT infrastructure running under tough conditions. Of course, there were issues, and our OCIO team has repeatedly developed creative, innovative and secure solutions to new challenges as they arise to keep the rest of NASA working productively.

**Matragrano:** The Department of Interior had previously taken steps to modernize our email and collaboration services, transitioning the entire department to Microsoft Office 365 between November 2019 and March 2020. This modernized application allowed DOI to swiftly adjust to full-capacity remote work. Collaboration across DOI and the federal government increased through the use of video conferencing and external sharing. Prior to the pandemic, DOI had approximately

4,000-5,000 remote workers accessing the virtual private network (VPN). By the third week of March, DOI had 60,000 individual connections to the VPN. DOI bureaus and offices have risen to the challenge and continue to leverage cloud services to truly transform the infrastructure. DOI is taking this opportunity to improve access to services to the benefit of all the bureau and office missions. Additionally, DOI is actively engaged in the enterprise structure solutions (EIS) network transition. DOI is on the leading edge of truly modernizing network services. Through the use of software-defined wide area network (SD-WAN) and collaboration with the Department of Homeland Security on Trusted Internet Connections 3.0, DOI will revolutionize the way users access the resources they need to do their jobs. DOI has unique challenges with employees across the world in over 2,400 offices, some in extremely remote areas. This modernized approach will improve access across DOI.

**Chilbert:** The pandemic was a validation of the modernization strategy Health and Human Services' Office of the Inspector General had embarked on several years ago. We had recognized that in order to enable the broader digital transformation we wanted to introduce to the agency, we first needed to invest in developing a secure, high-performing network. As part of this process, we increased the capacity of our virtual private network, upgraded the core infrastructure to improve the resilience and performance, and adopted managed trust internet protocol services (MTIPS) to provide Trusted Internet Connections. We also adopted a cloud-based productivity suite for email and basic business applications to include video-enabled meeting capability. When the pandemic forced us to shift to a 100% telework posture, our technology was in place to support the move. Most of our focus initially was on helping make sure our employees knew how to use the

technology to allow them to stay productive from home. For the most part, the shift to remote work was seamless for our organization.

**Cote:** The story of Transportation, I think, is a good one. And it really is a testament to the people coming together in a time of urgency and proving that we can work well together with a sense of purpose at speed, and not sacrificing any security or cutting any corners as it relates to configuration or procurement or any of those activities. It's a story about folks in the general counsel's office and in the budget office and procurement office, and of course, the CIO's office, coming together, sort of seeing the tsunami that was coming, if you will, and realizing we had to take some quick actions, and so it's a testament to the people in all those divisions and departments that did that.

It's also a testament to our leadership and the secretary in years ago realizing we needed a shared services model and bringing the network together across all the modes. And really that consolidation is what made this possible. As we brought that network together and collapsed it over the years, we really were lucky in many ways that we were at that point where we could flip a switch and do some pretty amazing things. Honestly, if we did try this two, three years ago, it would have been a much different outcome. The technology was in place. We had a fairly robust telework policy already at DOT prior to the pandemic. We simply had to expand that capability by adding typical virtual private network (VPN) licenses and adding virtual desktop interface (VDI) capacities in our VDI environment, and increasing the bandwidth across all of our connections for what we knew would be the increase in traffic across the network. But then we also really began to look at what new technologies should we acquire, implement, put in place that can sustain this for as long as we needed to sustain it right.

We looked at our primary mission applications and where they lived, whether they were on-premise or in the cloud, and prioritized accordingly to those

applications, and the work tools that we needed to continue working on mission. First and foremost, you need email, you need access to data and your shared drives and folders and documents. You need access to the modal applications, especially the ones the public access regularly. We said how can we not only keep these available, but increase their performance while increasing security? So

we deployed a cloud access security broker (CASB) solution in the cloud and have now locked down a lot of applications, made it much easier to connect, while at the same time giving us greater visibility and flexibility into who's connecting from when and where and how, again, strengthening our cyber landscape by hardening the surface and making it much tougher for our enemies to access.



## Discuss whether these changes were a quick fix or a long-term solution to your network and IT modernization challenges. How sustainable are the steps you took to ensure your network could handle the surge?

**Jones:** NNSA strives to do the best job possible with the resources and information available at the time. Given these circumstances, NNSA OCIO has made strategic decisions to solve the most pressing issues first. The rapid change to a remote workforce highlighted the need for additional services and solutions for our remote employees. The changes that we made have enabled us to support more staff to work remotely long-term moving forward. We didn't have a true appreciation for the breadth and scope of what we were facing with COVID. As things progressed, we realized that a long-term solution would be necessary to ensure that agency goals and objectives could be supported. Our staff has embraced working remotely and are equally, if not more, productive in their teleworking environments. In the long-term, we will realize many benefits to the new tools that were implemented, such as increased efficiency, increased collaboration, improved security and cost savings.

**Seaton:** My team has been working long hours to keep our IT infrastructure running with high

availability even while faced with unprecedented demand. The importance of reliable and resilient IT capabilities has never been more apparent. Any failure has the potential to prevent thousands of people from being able to work, and as the CIO, I hear about any issues very quickly! A network failure can suddenly disrupt hundreds of meetings and bring everyone across the agency to an immediate halt. We've certainly had to prioritize some work over other projects to address the most pressing issues as well as add additional capabilities to support this very different work environment. We've made some network architecture adjustments to eliminate single points of failure and improve overall throughput. The COVID-19 pandemic has provided an opportunity to underscore the importance of our IT systems and IT modernization and the benefits of adopting digital tools. As we proceed with many of our initiatives, they ultimately enhance the employee experience, whether teleworking or working on site. We have already launched key IT initiatives that have provided tremendous benefit to the agency during the pandemic. For example, in

partnership with our Chief Health and Medical Officer, we identified a laborious, manual process for onsite contact tracing and developed a mobile/web contact tracing and tracking application to more efficiently and effectively protect our onsite workforce. We continue to monitor and increase our virtual private network capacity as needed. We accelerated the launch of the Microsoft Teams mobile app and added the ability to add audio-only participants to Teams meetings. We have enhanced our collaborations with external partners through audio and video meetings using a variety of capabilities, including Instant Meeting, Jabber, Microsoft Teams, WebEx and other NASA conferencing services based on mission requirements. We implemented a secure video streaming capability to support mission needs. And we established a remote process for badge renewals. Since many within the NASA workforce had not used these collaborative tools extensively, and now they were essential to us continuing to work in the remote environment, we developed online training material with the Chief Human Capital Officer's team to host online sessions. Not only to train NASA people on the technology and tools, but to share tips and trick for how to effectively work in a remote environment and even manage the stresses caused by the new ways of working. New technology will continue to emerge providing new capabilities to support our remote workers, so the CIO team is continuously evaluating the changing technology landscape. NASA continues to be productive and resilient, even in this very different, and in some ways difficult, environment.

**Matragrano:** DOI was able to focus resources on long-term and modernized solutions including moving over to the EIS network contract and a shift to cloud resources. DOI sustainably improved remote work access and focused on real change and modernization.

**Chilbert:** Our ability to shift the entire workforce to remote work was the result of the long-term strategy to better support a mobile workforce.

Although we did not anticipate the pandemic, we had recognized that our employees increasingly needed to conduct their work outside traditional office settings due to the nature of OIG's mission. HHS OIG oversees an enormous portfolio, and it is impractical to have dedicated office space everywhere the mission may take our workforce. We did make some additional investments during the pandemic to increase our VPN capacity to ensure that we had the capacity to operate remotely for an extended period. Because our approach was part of a deliberate strategy, the changes are sustainable, and we will continue to look for ways to improve.

**Cote:** Things like software-defined wide area network solutions are perfect for this scenario. Instead of building a network that's always on and you just keep digging them out deeper or building the walls higher, now you've got capabilities where you literally can build, deploy, utilize, tear down, and throw away network connections through SD-WAN. It's really hard for the enemy to attack you if they don't know where you are, or when you are there. So these up and down network solutions through SD-WAN products is a great answer to this problem.

When you need to connect to the network, you do your work, you get off, no one ever knew that you were connected and that connection is temporary, completely encrypted, almost invisible to the enemy. So we've deployed that.

We looked at the whole stack from the endpoint to the users all the way to the top of physical layer or the application layer. We knew we had a lot of people remotely connecting forever. Most of the devices, we issued them and we control. But a large number of devices we don't. Whether they're a home computer, or a home laptop, or even a public computer, sometimes people will work from a variety of places, with a VDI connection, we know we can make that from almost anywhere from almost any device. But what we can't control is what that device might have

been used for prior to that experience, and what may be on that device in terms of threats, malware, ransomware, viruses, any of that sort of stuff. We looked at all of those devices and have hardened them with new end point solutions. We've made a lot of advances over the last seven months. What we think we know today, again, is this is a new reality, it's going to be a prolonged environment where most of our workforce will work remotely from a variety of locations, with a variety of devices. Our job largely remains the same as it always was, which is to provide our users with the tools they need to be productive to continue with the mission of the

department. So now we're simply providing those tools in a slightly modified environment.

It's been a busy seven months for sure. But in a way it was beneficial. We've always been on a modernization journey. Whether you want to call it digital transformation or IT modernization journey, we know we have a lot of legacy debt and we've always been trying to modernize that. This, in a way, was fortunate because it really pushed us and forced us to probably leapfrog a little bit of our timeline. What we had planned out a year or two from now we actually executed in the last seven months. So in a way it's been good for us.



## What are your IT modernization goals over the next 6-12 months? What is the current status of the Enterprise Infrastructure Solution (EIS) program solicitation and how does it underlie your IT modernization goals?

**Jones:** There are so many unknowns facing us and it is a challenge to predict what the world will look like in the next 6-12 months. Given the many variables at play, NNSA OCIO wants to ensure we are prepared to support our workforce in a remote capacity as long as deemed necessary. We want to continue to work with our IT services provider to provide modernized solutions to our employees so that they are able to perform their roles as efficiently while teleworking as they traditionally can in the office.

**Seaton:** The NASA Office of the Chief Information Officer is actively working with agency leaders to identify and prioritize IT modernization needs in support of NASA's broad mission portfolio. We will continue to focus on strengthening the foundation of our environment by modernizing elements of our network infrastructure, moving toward

software-defined access (SDA) and more automated network management approaches. SDA capabilities will allow NASA to perform network management and operations in a more efficient manner and will also enhance the agency's security posture by providing the capability to quickly, efficiently and safely segment portions of NASA's networks tailored to meet mission-specific requirements. The SDA capability will also allow for agile deployment of partner network zones and simpler and faster modification of existing security zones. Speaking of security, of course, we will be continuing to enhance our overall cybersecurity capabilities through a variety of initiatives and projects to give us increasing levels of insight into our IT environment, as well as more granular control over who and what accesses elements of that environment.

As we work with stakeholders to rationalize our application portfolio, we are moving toward more

agile approaches to internal software development while leveraging commercial-off-the-shelf and cloud-based applications more and more, and expect to complete a project to modernize our financial management and procurement system infrastructure in the next year. As an agency, NASA is pursuing a focused digital transformation strategy, looking at how we can leverage technology-enabled capabilities to transform the way we work. These digital transformation efforts include leveraging new and emerging collaboration tools, artificial intelligence and machine learning, model-based engineering, and data analytics to accelerate progress across our mission portfolio. In addition, OCIO will collaborate with missions to support the deployment of more complex science and mission codes in the cloud, and evaluate the further benefits of additional cloud architectures and micro services while leveraging cloud and edge computing power to provide an even more mobile-enabled, easy-to-use and administer IT environment. Also, in terms of technology-enabled transformation, we are continuing to look at optimizing the overall NASA work environment, including applying what we have been learning during the pandemic. As we gradually return to more onsite work, we have a cross-discipline team looking at “the future of work,” where we expect to bridge onsite and remote workers, continue applying IT-enabled collaboration tools and possibly utilize far less onsite office space. NASA has awarded two of its three planned Requests for Proposals. The OCIO communications program backbone core services contract has been awarded and services have been transitioned onto the EIS contract. Our backbone regional services and session initiation protocol services contracts have been awarded and we are in the process of transition for these services now. NASA Backbone Regional Services are expected to complete transition onto the EIS contract in the second quarter of FY 2021, while our SIP services transition should be done by the fourth quarter of fiscal 2021.

The final NASA RFP scheduled to be awarded to EIS is for NASA Mission Services. We expect that RFP to be issued in the second quarter of fiscal 2021, with the transition planned to take approximately 12 months. The remaining NASA services on the legacy GSA contracts are expected to be transitioned to NASA’s enterprise network services contract by the end of FY 2021. NASA expects that its EIS service providers will offer network solutions that leverage modern telecommunications industry capabilities, and thereby continue to strengthen the foundation for NASA’s IT modernization efforts.

**Matragrano:** All EIS task orders are complete and the transition is well underway. DOI is utilizing the EIS program to pilot and transition to network management/security solutions that will allow DOI to leverage commodity internet for connectivity, rather than traditional telecom mechanisms. DOI will be able to adjust to different demands quickly and support remote locations more successfully.

**Chilbert:** The Department of Health and Human Services awarded an enterprisewide contract under the EIS program in August, and HHS OIG will be participating in that award. Our priority is to work with the HHS EIS Program Management Office to transition to the new contract. Since the vendor has not changed, the initial phase will not involve significant changes to the underlying technology. One change we are making is to eliminate landlines telephone services to the maximum extent possible. As part of our previous efforts to move to a cloud-based productivity solution, all OIG employees can make and receive calls via their laptops. Longer term, we will be working with the EIS PMO and EIS vendor to explore modern technologies such as 5G and software-defined wide area network. Our goals in adopting modern technologies are to improve our ability to dynamically manage our network, improve security and resilience, and increase performance.

**Cote:** In addition to the hardware upgrades, re-architecting pieces of the network plays a big part in that. I think we’re on track. I think if you watch

or read the street, we did recently award the [EIS task order] contract to AT&T. We're very happy with that partnership. Even with the pandemic, I had five executives from AT&T in my office last week in Washington, D.C., and myself and the deputy CIO, and our network team, we all sat down for over an hour, and we talked about the future of the EIS contract and the solution, and what it brings to the department and the need for it to be executed in a timely fashion without errors or mistakes, or downtime and things like that. We're very excited about this new opportunity. We think the work done by GSA for all the providers is a benefit to government as a whole. It gives us a better opportunity to build out a bigger, faster, more robust, more secure network, without a lot of the headache of constantly re-competing these things or worrying about who has the latest and greatest technology. We let GSA do all the heavy lifting, and now we get to partner with their chosen providers. Again, in our case, we like AT&T for this. They've been a partner of ours now for many years. We think we're going to execute this ahead of schedule, hopefully.

SD-WAN remains a critical piece of the puzzle, even with the proliferation of everything mobile and with the somewhat still out there promised benefits of 5G networks. At the end of the day, everyone in this business knows that most important part of the puzzle is getting the application to the user. That application is riding a wired network somewhere, a hard network layer one. There are data centers all over the globe, and even our own internal data centers where these applications reside, where the data resides, and that connection is made to do an application somewhere on a terrestrial based network. And again, until we launch data centers in space, I suppose, and start riding Starling, we're faced with reality that this data is a terrestrial based network and we're probably riding someone's 10G fiber to and from data centers out to the endpoints. And then when you get to the cloud, again, you're taking a route somewhere; that's not mobile or wireless. For the most part, this network remains a hard wired connected network terrestrial base, whether it's copper or fiber. And that's the path to the mission. So our job is to make sure that path is large, robust and secure and always available to our users.



## How are you ensuring your technology goals mesh with your agency's business and mission goals? How is the need for citizen services impacting your digital transformation goals?

**Joel:** Our primary function is to be a mission enabler for NNSA. NNSA OCIO works closely with the various programs, functionalities and site offices within NNSA to ensure they have the services and solutions they need to get their jobs done. Whenever a need is identified, we work to determine whether or not the tool or technology requested is feasible in our computing and infrastructure environment. We do everything in

our power to deliver what is needed within reason and without detracting from our long-term goals and objectives. NNSA OCIO is always working to modernize the NNSA enterprise to ensure our employees have what they need to do the mission critical national security work required to keep our nation safe. The pandemic made us rethink our approach to modernization, so we reprioritized some of our existing goals and objectives, which

brought some items forward that were already on our list to begin with.

**Seaton:** The NASA CIO is responsible for developing and implementing an agency IT strategic plan that aligns with and supports the NASA Strategic Plan. The development of this IT strategy is done in collaboration with key mission and mission support stakeholders and NASA leadership to align resources and technology plans with the overarching goal of supporting mission success. My office continues to champion efficient and effective IT capabilities across the agency, while also working to ensure that our IT assets and data are protected from cyber threats, working closely with our customers to better understand and support their mission needs. Regarding citizen services impacting our digital transformation goals, one of the primary ways we interact with the public is by sharing the data and discoveries generated from our vast portfolio of space exploration, science and aeronautics missions. In collaboration with the NASA Chief Scientist and our Office of Communications, we are undertaking a web modernization effort to deliver NASA content even more effectively, leveraging new digital capabilities and tools to enhance the reach and impact of so many unique NASA datasets.

**Matragrano:** The goal of DOI's IT program is to enable the mission. DOI IT created an Integrated Project team made up of members across the department. We collected over 900 requirements from the mission areas to include external collaboration. We ensured the diversity of the DOI missions were at the forefront of crafting the new service.

**Chilbert:** HHS OIG's IT priorities are directly derived from the objectives laid out in the agency's strategic plan. The underlying technical capabilities needed to execute OIG's strategy include the need to support an increasingly mobile workforce, the need to securely put data at employees' fingertips, the ability to seamlessly and securely share data with our public and private sector partners, and

the ability to enable advanced analytics on large data sets. One of the primary services that HHS OIG provides is the ability for citizens to report waste, fraud and abuse in federal healthcare programs such as Medicare and Medicaid. Our tips website is an example of a cloud-based, modern application that citizens can access from any device to report potential fraud enabled by our digital transformation efforts.

**Cote:** One of the most important ones probably is we're in the middle of and mostly done, in fact, with bringing all of the Department of Transportation web applications into a single platform. We have roughly 1,700 or so public facing websites that are customer focused. Whether it's truck drivers or pilots or people wanting to get a drone license, we have a lot of external public facing websites. Over the years, those were always handled locally in the modes. We've taken all of the department websites, brought them into a single unified platform, and secured it first and foremost, made sure it's safe and encrypted at every level. Then we're in the midst of upgrading all of those websites to be compliant with HTTPS, and different things like that. We've made them responsive to mobile devices, whether it's trying to improve UI/UX interface or other things like that. Again, we know we have a lot of customers that come at us from a lot of different devices and a lot of different ways so we want to make sure that that every website we deploy is responsive in the best possible way. We're constantly building new ones because we're getting new requirements and we're deploying new capabilities. We're making sure that when we deploy the sites now, it's deployed in the latest, greatest platform with all that's best for the public.

At the same time, we have a lot of internal stuff, too. We provide service to the 50,000 plus internal DOT employees. Whether it's health benefits or time card systems or different things like that, we also have a lot of internal facing applications that we need to make sure are always up. One of the big things we've done is move some things to the cloud and begin to replicate them. We now have

multiple instances of the same application – all virtual of course – deployed across the country. We did an assessment a few years ago and looked at a lot of what we call single points of failure. A lot of these applications resided in one place only, or they might have been in a either government data center or even cloud, but they were one of one. And so we’ve had to scale out these applications.

We’ve replicated them across multiple data centers. And [we] just make sure now that we’ve got multiple paths to multiple instances so even if we experienced either an outage on a network or an outage in the data center, that traffic can be rerouted and these things have greater uptime than they’ve ever had.



## How are you considering/currently using the “as-a-service” model to help ensure your agency is prepared for future emergencies or surges in use by employees or citizens?

**Jones:** NNSA currently leverages “as-a-service” software products for productivity suites and enterprise offerings as needed. These tools increase our flexibility and allow us to provide NNSA’s workforce with the flexibility needed to ensure our work can continue regardless of an employee’s location. When it is reasonable, cloud-smart and managed services make sense, especially for organizations where 100% telework is a viable arrangement. As our staff become more acquainted with virtual capabilities, we have seen an increase in positive experiences with collaboration tools. While “as-a-service” may not necessarily help NNSA prepare for emergencies, we do use these types of offerings to support customer demand.

**Seaton:** NASA is aligned with and fully supportive of the federal Cloud Smart strategy. We continue to move toward cloud-based capabilities when it makes the most business sense in support of our missions. My office has established foundational capabilities with multiple cloud providers, enabling our missions to more rapidly implement infrastructure-as-a-service and platform-as-a-service cloud-based computing and storage capabilities, reducing, but not eliminating, the

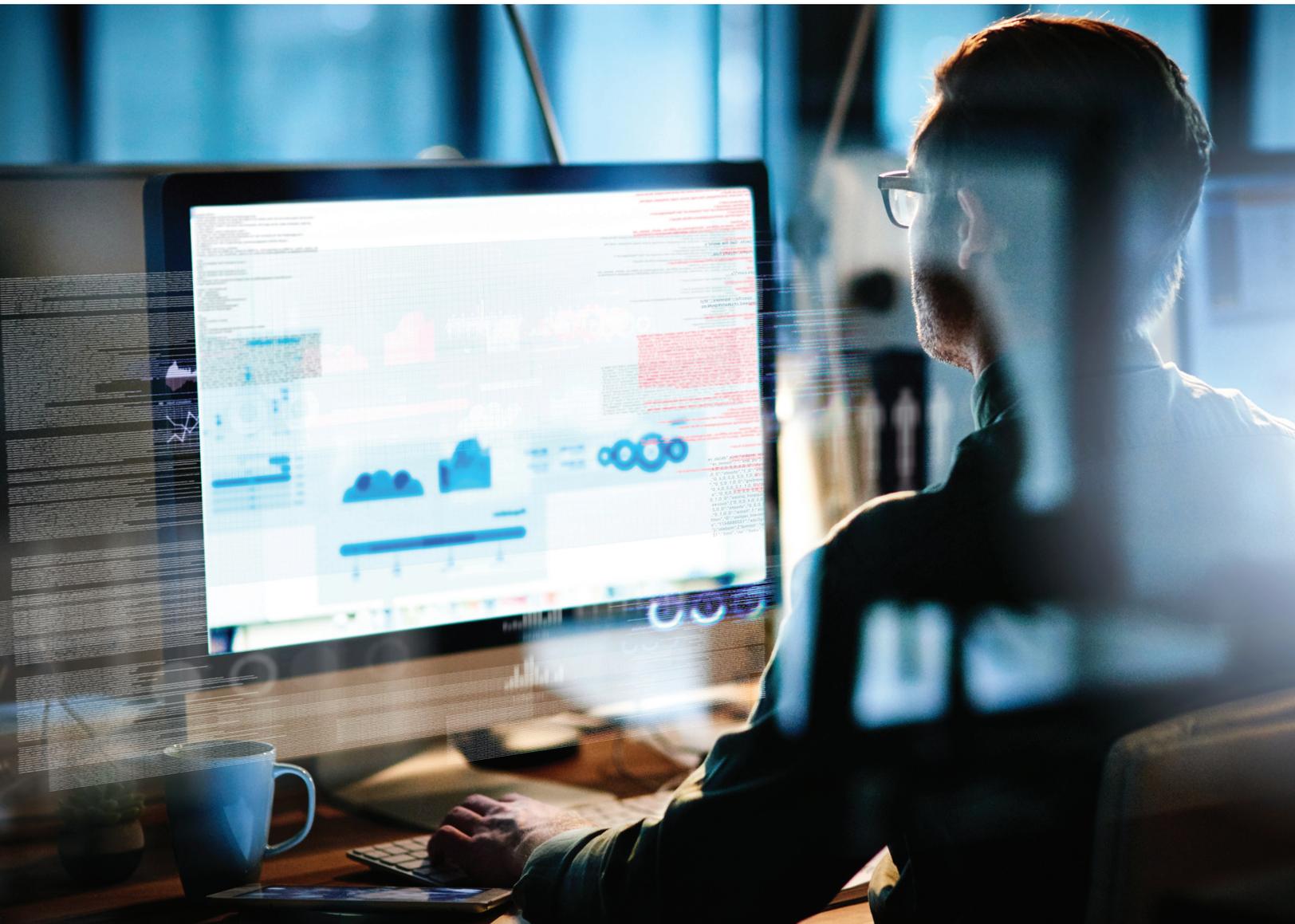
requirement for onsite data centers. Last year, we completed a migration from an on-premise email system to Microsoft’s Office 365 software-as-a-service platform for email and collaboration, a move that enabled us to seamlessly transition about 90% of our workforce to a remote telework environment in late March. There are many other applications that we’ve migrated to the SaaS model over the past years as well. Another as-a-service capability that might not be relevant to many organizations, but is certainly of interest to NASA, is the emerging Ground Station as-a-service model for spacecraft communications and data processing. Really, everything-as-a-service is where we are moving. Those services that deliver value at an advantageous price point will continue to succeed, enabling organizations that leverage these services to focus their efforts on the more unique aspects of their business, and not be as concerned about capacity or short-term surge demands because they can simply buy more when needed.

**Matragrano:** DOI’s enterprise contracts are set up to give us the flexibility to use more diverse services and the ability to adjust upward or downward based on our needs.

**Chilbert:** To the greatest extent possible, HHS OIG is employing platform-as-a-service and software-as-a-service to support internal or external facing applications. Because of our mission, the HHS OIG website has seen an increase in traffic from citizens since the start of the pandemic, and it has been able to handle the increased load well due to the PaaS environment it resides on. For employees, we have been developing applications on a common SaaS platform that will reduce maintenance costs in the long-term, but more importantly, it reduces the time needed to develop new applications and provides a common experience across all of them.

**Cote:** I tell vendors all the time – and I get, as you can imagine, 100 calls or emails a week from people

trying to sell the department things – you have to be flexible and you have to give me a solution that solves a problem for me, first and foremost. But give me something that is subscription based, something that I can get in and out of, if I need to, if something better comes along, or if we have problems. I think the future more and more has to be as-a-service, which is anathema to the vendors. You want to get somewhere and you want to get sticky, and you want to stay forever and be a good partner and get revenue for a decade, which is fine. Strive for that. You will get that if you prove that your solution is the best. But it really also has to be presented as-a-service to us as long as the service is good, solves problems for us, it's absolutely viable, and it's as-a-service.



# How COVID-19 caused course adjustments in the IT modernization journey

INSIGHT BY AT&T



**Chris Smith**  
*Vice President Civilian  
and Technology,  
AT&T Public Sector*

COVID-19 was a trial-by-fire for IT departments across the federal government. Some were better prepared, operating on the leading edge of technology, while others were still heavily legacy-oriented, and had to play catch-up. But the pandemic forced all of them to learn how to operate differently.

“We’ve got over 150 million people in the workforce. And traditionally, when you look back at the studies, somewhere between 4% and 7% were working from home on a regular basis. But that changed overnight, ramped upwards of 50% or 60%,” said Chris Smith, vice president of civilian and technology at AT&T Public Sector. “So there was a tremendous need for organizations to shift from large campus based or field based offices back to the home. In March, we saw increases in our core network traffic from 20-30%, which was necessary to allow workers - that had not to this point been home - to access the mission critical assets to continue the job without any loss in continuity.”

And many of those agencies have massively different mission sets, from national security at the Department of Homeland Security to the varied domestic services at the Interior Department, which had to manage increased activity at national parks. But despite the variations in their roles, all are necessary to maintain a functioning society.

Some agencies were even called on to deliver greater services than usual in response to the pandemic, which in some cases required new or increased capabilities.

“The Small Business Administration was sought out and relied upon to implement significant stimulus funding for critically important small businesses to support the backbone of the economy. And they gave out, on behalf of Congress, the President and the Treasury, more than half a trillion dollars in very short, two to three week timeframes each time. I was staggered,” Smith said. “It became a great example of using the as-a-service model. We’re their network provider, and we were able to scale up and then to use as-a-service contact center capabilities to manage it. In my experience, no agency has ever done that, in that time with that amount of money.”

Smith said SBA is the perfect example of a federal agency that was on a specific modernization path but had to adjust course in the face of the pandemic. And that's a key part of the modernization journey, Smith said.

"What does modernization mean? It's not an endpoint. It's this continual leveraging of the best capabilities out there," he said.

Historically, it's largely been driven by the virtualization of technology. It started with storage, as the proliferation of data began to exceed the physical capacity of hardware to manage. Then storage virtualized, and the costs reduced. Then virtualized compute followed, commonly referred to as "the cloud," and the costs continued to decrease as well. Combining those two things together allowed organizations to continue processing increasing amounts of data.

"The question was, how can you move those workloads, and connect people to them around the globe?" Smith said. "Now that we're virtualizing capabilities within the network, that's how you can scale when you have an event like we are living through right now."

Another part of IT modernization that the COVID-19 pandemic accelerated was the adoption of collaboration tools. Working collaboratively requires networks to be high-performing, and able to scale securely. Many agencies are using cloud technologies to do that, and that's where Smith said the majority of workloads should be moving in the near future.

"I think the reality is we're going to see a much more dispersed workforce and those technologies in my mind, better enable the productivity of the individual, the capacity for them to work more efficiently," he said.

Agencies need to start looking toward context-based workloads, he said, especially for critical infrastructures and government services. Emerging technologies like 5G and edge computing are going to enable things like infrastructure inspections and mobile capabilities for healthcare.

"A lot of what we talk about is this really high speed throughput and low latency that's going to enable things like driverless vehicles, improved situational awareness for public safety, enhancements on research campuses and the management of thousands of miles of forests and park lands," Smith said.

Modernization, if done right, will allow CIOs to enable new technological advancements within their agencies, without having to spend too much time focusing on infrastructure to support it.

"One of the key pieces to modernization is not having a legacy albatross around your neck," Smith said. "A constant challenge for agencies is the struggle for funding to maintain long term programs. Take the capital out of the equation and buy it as a service. And that includes consistent technological refreshes, so you stay ahead of the modernization curve. It allows agencies to stay focused on the mission."