FEDERAL NEWS NETWORK

SPECIAL BULLETIN REVIEW

SECURE REMOTE WORKFORCE

INSIDE THIS ISSUE:


Security that goes
everywhere you go.
Protect your organization with
Lookout, the leader in mobile security.
Lookout
Learn more and
try a 90-day free trial.
carahsoft
The Trusted Government
IT Solutions Provider®

TABLE OF CONTENTS

What has become evidently clear over the last few months, agencies all felt the strain of the surge in remote workers. Few agencies, whether big or small, didn't have to overcome some challenge to ensure their workforce could continue to meet their mission remotely.

Whether it was the Veterans Affairs Department which needed major upgrades to their network or the National Science Foundation, which just had to speed up its rollout of a collaboration software, the move to telework was hardly easy.

On top of that, federal chief information officers immediately faced an increased threat to their data and networks due to the expanded compute surface of mobile devices.

In this e-book, CIOs from the VA, NSF and the Drug Enforcement Administration in the Justice Department explain the steps they took to achieve the balance of security and accessibility as employees worked outside the office because of the pandemic.

Jim Gfrerer, assistant secretary for Information and Technology and chief information officer for VA, said the agency upgraded its Trusted Internet Connections (TIC) gateways to handle the increase in traffic as well as to better secure the agency's data.

Maura Quinn, the deputy assistant administrator of the Information Systems Division at DEA, said the agency had to quickly expand its secure remote workplace capabilities to handle the influx of users.

It's clear from these interviews, no matter how prepared agencies thought they were, the pandemic forced them to rethink how they provide secure and reliable access to remote workers.

Jason Miller
Executive Editor
Federal News Network

VA not resting on laurels after nearly tripling and securing remote workforce

BY PETER MUSURLIAN

If agencies were constantly on guard the past several years, as cyber attacks grew in intensity and effectiveness, the past several months of the pandemic has dumped fuel on that fire of fear and paranoia.

"We get probed and challenged every day," said Jim Gfrerer, assistant secretary for Information and Technology and chief information officer for the Department of Veterans Affairs, on Federal Monthly Insights – Secure Remote Workforce.

In March, like so many large work forces, VA was facing an uncertain future. With nearly 400,000 employees, it is predominantly an on-premise environment.

"Pre-COVID, we had roughly 56,000 folks enterprisewide who were accessing remote access. About 40,000 of that was through a virtual private network or VPN," Gfrerer said on Federal Drive with Tom Temin.

As the pandemic-driven stampede to telework began, the VA nearly tripled its work-from-home employees.

"We ended up leveling out at about 140,000. It was our high water mark," Gfrerer said. "One of the interesting things is, for IT folks, you rarely if ever get the opportunity or demand to test in your production environments."

So with no time to spare, VA put its internet connection gateways through stress tests, pushing all of one day's traffic through one gateway. The line was rated to handle 35,000 to 40,000 and they were pushing 40,000 through.

"That was with cooperation and the patience of our business lines. They said, 'No, we understand you need to test it, we need to do it now, so that folks are ready if we go into some significant telework, you've got to stabilize and upgrade the infrastructure,'" he said.

> **"We're always going to need to provide a certain amount of both VPN and non-VPN access into the network. We're working to balance that solution, but more importantly, we're working — and this is consistent with [the Office of Management and Budget] and other federal cloud initiatives — to provision those in some sort of cloud environment."**
>
> **—JIM GFRERER, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY, AND CHIEF INFORMATION OFFICER AT DEPARTMENT OF VETERANS AFFAIRS**

Gfrerer sang the praises of his vendor partners, the carriers and infrastructure providers, as well as those at the data centers.

"We're always going to need to provide a certain amount of both VPN and non-VPN access into the network. We're working to balance that solution, but more importantly, we're working — and this is consistent with [the Office of Management and Budget] and other federal cloud initiatives — to provision those in some sort of cloud environment," he said. "With the pandemic, I think you had a lot of folks who were scrambling with on-premise environments, and that's a lot harder to

scale up and scale down. In the future and even going forward, we are in a much better position to efficiently, from a cost standpoint, but also effectively from an infrastructure standpoint, look at our cloud service providers and scale up and scale down, as needed, in both environments."

VA, and all agencies, will have to remain vigilant to avoid being successfully targeted by hackers, which means technical superiority as well as an educated workforce.

"We put a high premium on ensuring our workforce is aware and trained. The human is always, at least now, going to be the weakest link. And so, our previous efforts around our phishing campaigns in education, we added some additional functionality both in our email and our web services, so people could report phishing attempts a lot easier. All that created a much better security awareness environment with our workforce. I'm really proud of our workforce and how they've responded because as everyone's experienced, the threat actors are still out there, and they're looking to take advantage of the chaos and the pandemic. So I think from a human-factor standpoint our folks performed really, really well and will continue to enable and double down on the education," Gfrerer said.

The human is always, at least now, going to be the weakest link. And so, our previous efforts around our phishing campaigns in education, we added some additional functionality both in our email and our web services, so people could report phishing attempts a lot easier.

— JIM GFRERER, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY, AND CHIEF INFORMATION OFFICER AT DEPARTMENT OF VETERANS AFFAIRS

NSF had secure telework down to a science years ago

BY PETER MUSURLIAN

One Friday in March, the 1,600 employees of the National Science Foundation (NSF) left the office and on the following Monday they were all working from home. It's a familiar story to so many across the country, but the NSF might have been a little more prepared to make the switch.

The NSF accepts electronic proposals from around the world and determines which ones merit funding. Over the years, panels of reviewers, from all over the U.S., have met to size up the researchers' proposals.

"Some of that was done electronically, before COVID," NSF Chief Information Officer Dorothy Aronson said on Federal Monthly Insights – Secure Remote Workforce.

"We migrated to a laptop with a docking station and monitor when you were on site and the laptop was configured in such a way that it was secure, so when you were away from the office, you could take it home with you and securely access the NSF internal network through a virtual private network."

— DOROTHY ARONSON, CHIEF INFORMATION OFFICER AT THE NATIONAL SCIENCE FOUNDATION

Since that fateful day in March, all of the work done by those panels has been done entirely electronically.

"We were in the middle of testing out Zoom as our virtual interaction tool," Aronson said on Federal Drive with Tom Temin. "We had been using a combination of Webex and BlueJeans before that. People were finding Zoom very easy to use, so we transitioned everyone away

from Webex and BlueJeans more or less overnight. That was a fabulous benefit for the agency. Because before people had to understand how to use a variety of tools to interact and people were not all interacting in the same way, and getting everyone into a homogeneous methodology really worked well."

"We really are not experiencing additional security risks as result of our distributed workforce. We do send out more training materials to people to heighten awareness about phishing campaigns and that might be floating around, but we have not really experienced tremendous impact security-wise."

— DOROTHY ARONSON, CHIEF INFORMATION OFFICER AT THE NATIONAL SCIENCE FOUNDATION

Early into the office-to-home transition, there were concerns across the country about the security surrounding Zoom and other online chat services. The NSF avoided those concerns.

"We have been using a secure implementation of Zoom from the beginning. We had been working in the government cloud, we had been requiring passwords on meetings," Aronson said. "So when the press started talking about the lack of security in Zoom, the Zoom they were talking about was not actually the configuration that we were using. So we just pressed forward and did not experience zoom bombing, or the other problems that we had heard about."

Aronson said the transition from one online chat tool to another did not pose a problem because NSF had trained users on safety.

"Human behavior is very important. So the way we implemented Webex and BlueJeans before and the way we trained our customers to use those tools was an important factor in keeping things secure. We did not experience any more risk in using the Zoom product than we had with the others," Aronson said.

In 2017, NSF moved its offices from Arlington to Alexandria, Virginia. That moved put them into and even more secure position than they could have imagined, as the pandemic hit in 2020, and telework became the new normal.

"At that time (three years ago), as a precaution, in order to ensure that work would not be impacted negatively or there wouldn't be an outage for customers as they moved, we migrated to a laptop with a docking station and monitor when you were on site and the laptop was configured in such a way that it was secure, so when you were away from the office, you could take it home with you and securely access the NSF internal network through a virtual private network," Aronson said.

So three years later, after the office relocation move, NSF avoided the pandemic problems that so many workplaces encountered.

"When we went to working 100% from home, there wasn't a learning curve for most staff who were used to teleworking part time or even those who had working in the office, but maybe periodically just took their computer home for the weekend, which is kind of the way I did things. So we all were familiar with that setup," Aronson said.

Aronson said they feel secure because they use "well-tested and well-understood" two-factor authentication.

"We really are not experiencing additional security risks as result of our distributed workforce. We do send out more training materials to people to heighten awareness about phishing campaigns and that might be floating around, but we have not really experienced tremendous impact security-wise," she said.

How to secure mobile devices in the age of mass teleworking

THIS CONTENT HAS BEEN PROVIDED BY LOOKOUT

The year 2020 will be long-remembered for many reasons. Information telework – and the resulting explosion in use of mobile devices as network endpoints.

That means protection of mobile devices is more important than ever. More than securing devices and mobile workforce per se, it's important to think of this effort as helping secure the agency enterprise itself.

As Bob Stevens, the vice president for the Americas at Lookout explained in a recent interview, agencies early in the pandemic response rushed to obtain mobile devices – smart phones and tablets, specifically – for those who suddenly needed them. Now, in a sort of second wave of activity, they are buttoning up this part of the enterprise. He said agencies are going to stick with teleworking on a large scale.

Key to understanding the best strategies for protecting mobile devices is to understand "they are outside the infrastructure. They've always been outside the infrastructure," Stevens said. And yet, enterprise data comes into the devices for onboard processing and storage. Stevens said any strategy for securing mobile devices must prioritize the data.

> **"What we know of phishing in the mobile world versus the desktop-laptop world is completely different."**
>
> — **BOB STEVENS, VICE PRESIDENT FOR THE AMERICAS AT LOOKOUT**

He added, "Techniques to secure them is a defense-in-depth approach."

Elements of defense-in-depth include:

- A virtual container on the device to isolate government applications and data from the user's personal apps and data. "You'll have your work inside that container where it's protected and encrypted," Stevens said.
- VPN service for reaching back into the network that encrypts data in transit.
- Anti-virus, anti-phishing and anti-man-in-the-middle attack software stack. In particular, Stevens said, Lookout can detect when a session is being terminated by a seemingly benign WiFi connection that's actually a man-in-the-middle attack collecting data – including credentials

– coming from the device. These measures reinforce the container and add protection against unwanted root access (which can bypass the container) or jailbreaking.

- Application monitor running on the device to ensure apps are free of malware.

"It's really all of those things that are needed to protect the mobile devices," Stevens said.

As for phishing, Stevens said this form of email remains the most common vector for sophisticated adversaries, such as nation-state actors, to get into a mobile device and the data it holds. Moreover, "what we know of phishing in the mobile world versus the desktop-laptop world is completely different," he said.

"On a mobile device, phishing can happen many, many different ways," Stevens said, including from text messages and in a myriad of apps like WhatsApp or mobile versions of social media. A big part of minimizing the risk is training users to be alert for the mobile-specific phishing avenues.

"We can tell pretty quickly, whether it's going to have either risky behavior or malicious behavior. And we're going to notify both you and the organization to ensure that that no one actually uses that application."

— BOB STEVENS, VICE PRESIDENT FOR THE AMERICAS AT LOOKOUT

Application monitoring, Stevens said, principally requires scanning them for viruses and other attacks, and checking to see if they are communicating only with authorized servers – and not servers in, say, China or Russia, or whether it's monitoring the user's location.

Lookout's technology, Stevens said, can scan at high speed applications users download. Applying artificial intelligence, "we can tell pretty quickly, whether it's going to have either risky behavior or malicious behavior, and we're going to notify both you and the organization to ensure that that no one actually uses that application."

Also key to mobile device assurance is having visibility into all the devices being used on the network, if only to ensure that users have up-to-date operating systems that can accept the latest patches.

"It's important to have the visibility into the operating systems you have deployed," Stevens said, "because if you've got one that's really old it could have a bunch there's no patch for because those companies stopped supporting those versions."

DEA doesn't miss a step in its transition to a secure remote workforce

BY PETER MUSURLIAN

The way the Drug Enforcement Administration made the move from pre-COVID office life to what the federal workforce has been living through since March was aided by already having the foundation in place to transition to a large-scale, secure remote workplace.

"We were positioned pretty well, because we had a pretty mobile workforce already," said Maura Quinn, the deputy assistant administrator of the Information Systems Division at DEA, said to Federal News Network's Jason Miller on Federal Monthly Insights – Secure Remote Workforce. "Our workforce already had mobile devices, so smartphones, and we have mobile device management,

> **"Our workforce already had mobile devices, so smartphones, and we have mobile device management, so we manage those phones securely. So we were in good shape there. And we already had a virtual desktop interface (VDI) solution and also we had a virtual private network (VPN) solution."**
>
> **— MAURA QUINN, DEPUTY ASSISTANT ADMINISTRATOR OF THE INFORMATION SYSTEMS DIVISION AT THE DRUG ENFORCEMENT ADMINISTRATION**

"[We're looking for] ways where the workforce that is out in the field, and maybe not in the office, can move data from a smartphone into our environments, to be able to scan documents, to be able to move evidence around securely in different ways."

— MAURA QUINN, DEPUTY ASSISTANT ADMINISTRATOR OF THE INFORMATION SYSTEMS DIVISION AT THE DRUG ENFORCEMENT ADMINISTRATION

so we manage those phones securely. So we were in good shape there. And we already had a virtual desktop interface (VDI) solution and also we had a virtual private network (VPN) solution."

But, although the system was in place, with so many at the agency using them, DEA had to expand that universe — and they had to do it fast.

"Before COVID, on the VDI side, we could support about 1,200 concurrent users. And on the VPN side, we could support about 900. We have about 15,000. So that wasn't going to work for us," Quinn said.

So Quinn met with her team and asked them what they needed to do to expand their secure remote workplace capabilities, sooner rather than later.

"By the time COVID came around and we had the requirement to go to maximum telework, we were able to support 10,000 on our VPN, and eventually we were able to support and can support about 2,500 on our VDI. That's concurrent users. So we were in pretty good shape," Quinn said.

VPN supports 10,000 laptops at DEA that can only be used on an internal network, getting access using a PIV Card or multi-factor authentication.

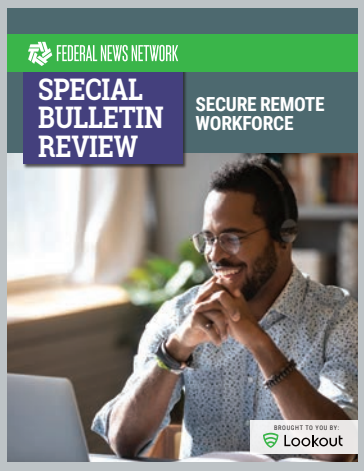
"Using our internal network laptop, we can access our internal network. So 10,000 of our workforce could do it that way concurrently. And then VDI, basically bring your own device or you bring another government's device, and again, you can sign in that way using the credentials that we provide. So we can support a total of 12,500 concurrent users," Quinn said.

Although they worked fast to get into the position they are in today with their secure remote workforce, DEA is planning on adding additional functionality.

"[We're looking for] ways where the workforce that is out in the field, and maybe not in the office, can move data from a smartphone into our environments, to be able to scan documents, to be able to move evidence around securely in different ways," Quinn said.

DEA got up to speed quickly and is moving along smoothly. But now, Quinn said, they might be suffering from "telework fatigue."

"People are tired of sitting in their homes and would like to get back into the office. I think in the long run, having a better mix of telework and in person work will be something that we'll strive for," she said.


FEDERAL NEWS NETWORK
SPECIAL BULLETIN REVIEW
SECURE REMOTE WORKFORCE
BROUGHT TO YOU BY:
Lookout