FEDInsider

# Securing Government Telework Against Cybersecurity Threats

## AS MORE EMPLOYEES WORK REMOTELY, NEW CYBERSECURITY CONCERNS MOVE TO THE FOREFRONT

As a response to the global pandemic, most federal agencies have transformed their workforces from mostly on-premise operations over to having a majority of their employees teleworking, with many state and local governments following that same plan. For many of the employees of those agencies, working from home is a new concept, as are the cybersecurity-related responsibilities that had previously been handled by their agency's staff back at the office.

This situation has forced agencies to rely on their employees to practice safe computing techniques. Employees working from home need to understand not only their new roles in relation to their job responsibilities, but also what they need to do in order to keep their agency networks, data and fellow employees safe from a cybersecurity standpoint.

There are several key points that agencies should consider when trying to keep their newly remote workforce safe. And these lessons should also be shared with employees so that they can help to protect themselves and their agencies as everyone adjusts to this new working environment.

### TELEWORKING SHOULD BE INCLUDED IN EVERY MODERNIZATION PLAN

While some government agencies had various levels of telework infrastructure and planning already in place, most military bases did not. Because of this, the military was caught a bit flatfooted compared to civilian agencies when shifting over to massive remote working operations. Officials at most bases had to work with employees to develop and implement solutions that allowed the military to maintain mission readiness.

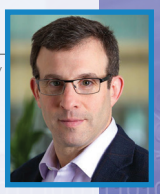
"There's 300 locations across the world for the Air Force system, and so as we realized what was happening, we found that at most of our bases, people don't have laptops," said Chief Technology Officer of the Air Force Frank Konieczny. "They had desktops, and they worked there. And they live close. When we told everybody to go home and work, it was like, what am I going to work on when I go home? If I don't have a laptop, how am I actually going to communicate with everybody?"

Defining how to work from home for workforces that have never done it before, or only did it on a very limited basis, has not been an easy task. Some agencies were assisted by the fact that they were in the middle of modernization efforts, which helped in the deployment of new equipment to supplement their teleworking efforts.

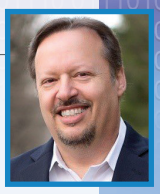
"We have been on a March to Modernization and work to minimize our technology debt that we've been carrying for a little while," says Pete Gouldmann, Enterprise Risk Officer for Cyber at the Department of State. "That put us in a good position because we had already transitioned to a cloud-based collaborative platform and were already allowing remote access. We were able to scale that fairly rapidly to be able to support a global presence and global access. We had and continue to operate several different types of remote access capabilities based upon what is needed by the end user."

### FEATURING:

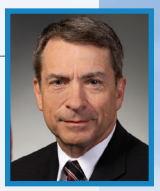
- **Jeff Greene**
  *Director,* National Cybersecurity Center of Excellence, NIST



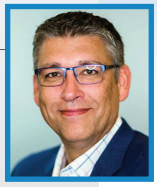
- **Pete Gouldmann**
  *Enterprise Risk Officer, Cyber,* Department of State



- **Frank Konieczny**
  *Chief Technology Officer,* U.S. Air Force



- **Chris Usserman**
  *Principal Security Architect,* Infoblox



- **Allen McNaughton**
  *Director, Systems Engineering,* Infoblox Federal

## UNDERSTAND THE UNIQUE RISKS PRESENTED BY BYOD & IoT WITHIN MODERN HOMES

With a sudden surge of remote workers, securing non-government issued devices has been a challenge. The so called Bring You Own Device (BYOD) model helps get workers online quickly, but this can be risky as it places less secure and less controlled devices on government networks. Then you also have the unique home environment to contend with. There are devices in most modern homes that are not very secure, and they will now at least be peripherally connected to government networks when you have employees working from those locations.

"One of the aspects you're going to need, if you don't already have it, is visibility into what those [home-based] endpoints are doing with your remote workforce in respect to mission systems. Maybe you throw a VPN onto a BYOD device into someone's living room that would allow you to have the control over that workspace without having to take over the liability of the host architecture," says Chris Usserman, Principal Security Architect at Infoblox.

And those home environments can be unlike anything that would populate a government office. It can include devices like Internet of Things (IoT) sensors with no security at all, as well as things like PlayStation 4s and Xbox One game consoles that thrive because of their ability to easily network with game servers and other gaming peripherals.

"We have IoT devices. We've got Google Nest, you know, devices for our HVAC. We've got game consoles. We've got all of these other devices that are within a trusted workgroup now, and you don't have any control or visibility over what those devices are doing," Usserman said. "That's one of the challenges, having the visibility and a near real-time understanding of what's happening with your resources, no matter where they are in the world."

## GOVERNMENT TELEWORKING IS HERE TO STAY

Most agencies have no idea when teleworking will end, or even if it will end once the pandemic is defeated. Because of this, most have adapted to the changes that remote working brings. Others should try and normalize operations as much as possible.

"We all have to realize that teleworking is going to be a way of life," Konieczny said. "It's foreign, especially on the government side, but we're getting to the point where telework may be a permanent entity. That's going to be great for some people. But you have to understand the security implications of this also."

While teleworking has become commonplace, there is still a learning curve that employees face with understanding the technology involved. This includes understanding security and their new roles in it.

"We roll out the right tools, but we need to make sure we also do the training," said Jeff Greene, Director of the National Cybersecurity Center of Excellence at NIST. "We can't assume people know how to use the tools. I think we need to try to find a way to make sure people really enter remote collaboration with a mindset of what level of security they need to apply, if any.

Agencies should install a sense of security into every aspect of their employee's teleworking mindset. Even the smallest interactions can have big security consequences if not done correctly.

For example, employees, "need to think about even a simple phone call like it was a data transfer," Greene said. "There must be a mindset shift when you can't just walk down the hall and chat with someone." Government needs to adopt that, because teleworking is likely here to stay.

### About Infoblox

Over the past 20 years, Infoblox has been recognized as a leader with 50% market share in core network services, which includes DNS, DHCP, and IPAM, collectively known as DDI. Building upon this proven foundation, Infoblox is bringing DDI and core network services to the next level with a robust offering of secure cloud-managed network services.

### About Carahsoft

Carahsoft Technology Corp. is a trusted government IT solutions provider. The company combines technological expertise with a thorough understanding of the government procurement process to help Federal, State and Local Government agencies select and implement the best solution at the best possible value.


FEDInsider

**Hosky Communications Inc.**
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider/
@FedInsider

carahsoft

**Carahsoft**
1493 Sunset Hills Road
Reston, VA 20190
Contact: Jenna Tabatabaian

(703) 889-9726
Jenna.Tabatabaian@Carahsoft.com
www.Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

Infoblox
NEXT LEVEL NETWORKING

**Infoblox**
One Dulles Technology Center
13454 Sunrise Valley Drive, Suite 570
Herndon, VA 20171

(844) 226-4910
info@Infoblox.com
www.infoblox.com
Facebook.com/Infobloxinc
Linkedin.com/company/infoblox
@Infoblox