FEDInsider

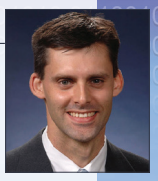
# Four Keys to Increasing Federal Cybersecurity in a Heavy Telework Environment

## Experts Stress the Need for High Security Vigilance during Telework

### Featuring:

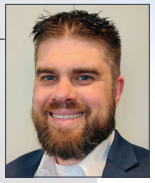
- **Paul Morris**
  *Chief Information Security Officer,* Transportation Security Administration

- **Kevin Stine**
  *Chief, Applied Cybersecurity Division,* National Institute of Standards & Technology



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

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



While many government agencies have been experimenting with telework and its supporting technologies, few were ready to embrace an almost completely remote workforce. But that is exactly what had to happen, and quickly, in order to protect federal employees from the coronavirus pandemic.

In the face of that ongoing health crisis, full teleworking programs have rapidly become integral to mission success within many government agencies. Throughout government, employees and their administrators alike have been adjusting to virtual private network (VPN) technology in conjunction with their home Wi-Fi for accessing federal networks and performing critical mission functions. While the surge of VPN use has caused some initial issues like poor performance and users getting temporarily locked out, it has at least allowed the government to continue its operations.

Despite success with those continuity of operation plans, cybersecurity concerns have emerged as an issue lurking throughout the current teleworking framework. Most homes have less secure networks than those at government installations. Because of this, there is an increased risk of exposing sensitive data as well as having a network attacked by hostile actors. Government agencies must now balance the needs of teleworkers with maintaining a strong security posture.

Agency officials as well as those from industry agree that good cybersecurity is possible in conjunction with large teleworking efforts. But it takes a concentration on best practices as well as ongoing vigilance. Agencies can start with four key points to help keep their employees and data safe while telecommuting.

### Telework, while essential to mission success, opens up new security concerns.

Government is unique in that it can never close, no matter how dire the situation. The need to remain open is one of the biggest reasons why government has recently embraced flexibility in telework policies across the board, said Chief Information Security Officer at the Transportation Security Administration (TSA) Paul Morris. While telework has been utilized in the past, recent events have pushed multiple agencies to move to a maximum telework environment. This has enabled the federal government to meet its current obligations, but not without also creating new security concerns.

Morris stressed that the move to full teleworking has been a learning process, especially in regards to security and certain elements that were not considered before.

"There were specific things like, if you're at home doing work, turn off Alexis," Morris said. "No one thought about that.

Morris also said it was important to tell employees not to use personal electronic devices for government business, since those unmonitored assets are almost certainly more susceptible to attacks. This includes little things like not printing sensitive documents on home printers, or using Wi-Fi with weak or no encryption. Workers need to understand that certain activities like that can jeopardize a federal network now that so many people are working from home.

### Communication and training is essential in maintaining a strong security posture.

Communication is a major factor in maintaining a strong security posture within a telework heavy environment. This includes clearly explaining security and privacy considerations to employees department-wide. And that requires educating employees about the vulnerabilities and risks associated with teleworking, and how they can help prevent cyberattacks with good practices.

"They need to know what process they should follow if they suspect there's something unusual or suspicious on their telework devices while working at home," said Chief, Applied Cybersecurity Division

for the National Institute of Standards and Technology (NIST) Kevin Stine. "Do they call the normal help desk or response team? Those things are important to keep in mind."

Stine also stressed how it is important to remember that because many people will be working in their home environment, privacy should also be respected. This includes when using virtual meeting platforms such as Zoom and Skype. These, while helpful for teams to stay in touch, can become both a security and privacy risk. Agencies need to ensure that they have good rules and policies in place to govern the use of those services.

## Adopt a zero trust architecture to mitigate risks.

Cyber threats loom over every government agency and their employees, even when working within their main offices. With more employees working at home using devices and tools that have fewer or lower quality security measures, it may be time to adopt zero trust networking, suggested Principal Security Architect at Infoblox Federal Chris Usserman.

"I think this really forces organizations to look at how to apply a zero trust architecture with continuous diagnostics and monitoring, because you have all of these federated workers that are all on their own segments effectively coming into your enterprise," said Usserman. "You've now got an unsecured outer shell where you have unsecured devices and appliances as endpoints, and attackers may be using them as a bridge or gateway into the enterprise."

It is important to not take any chances with a government system becoming compromised through one of those telecommuting endpoints, and then having the breach going unnoticed until substantial damage has been done. One of the best ways to do that is through zero trust networking, Usserman said. Because in zero trust, users and devices must continually prove their identity, and are only given just enough permission to perform their specific and required tasks.

## Utilize the domain name system (DNS) to control access to dangerous sites.

Preventing users in a telecommuting environment from accessing dangerous or compromised websites is a critical component in reducing the attack footprint that hostile actors can exploit. Within the office, DNS can be used to restrict sites that an agency doesn't want its workers visiting. But that is more challenging when dealing with telecommuting employees.

"The deal with DNS is if you're at a computer in your office and type Google.com, your computer reaches out to the domain server to find the IP address," Usserman said. "If that's an approved pathway, you can make the connection." But if a user wants to go to a bad domain, one that the agency does not approve of or that should not be visited during working hours, then the request would be blocked by the DNS.

When telecommuting, federal agencies can and should do the same thing when an employee is using an agency VPN or other communications tool, Morris said. Although the agency can't control what an employee does within their private network connection and devices, it can enforce good computing practices when using federal networks.

"We're blocking the same DNS [for telecommuters] as we are internally, and making sure it's handled in a certain way," Morris said. That will help to prevent users from picking up malware at unapproved websites, as well as wasting government resources doing things like looking for pornography. And, it's a natural extension of the same kinds of cybersecurity protections that most agencies are already employing internally.

This Mission Brief was written based on a recent webinar which can be streamed on demand at: Combating The Cybersecurity Risks of Government Telework.

## About Infoblox

Over the past 20 years, Infoblox has been recognized as a leader with 50% market share in core network services, which includes Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP address management (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.


**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**
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**
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