Security and Compliance for Remote Federal Workers

Adapting to Remote Work Environments

Highlights

In its immediate response to the COVID-19 pandemic, the U.S. Navy increased its available bandwidth for remote users by 150 percent to 250,000[3].

In response to the novel coronavirus pandemic, the Office of Management and Budget (OMB) made an unprecedented call[1] for agencies to maximize telework flexibilities, resulting in 98 percent of the federal workforce working remotely[2]. This abrupt and wide-scale shift to a remote work environment required agency security teams to adjust with little to no planning, placed a tremendous strain on all aspects of security operations, and intensified risk beyond the norm for federal infrastructure.

In some ways, this shift merely accelerated modernization initiatives that were already underway. But what was once a slow and segmented approach to telework prior to the pandemic quickly leaped forward to require support for critical internal government functions such as sensitive communications, acquisition activities, and essential citizen services.

One of the greatest and universal challenges of security and compliance is securing endpoints. This becomes particularly difficult in a telework environment where there is less visibility and control. There are indicators of compromise specific to remote environments that security personnel must be aware of, such as an unusually slow computer, pop-ups that don't seem to adhere to browser rules, the loss of USB port use, or mouse/keyboard locks up. Remote environments are particularly vulnerable to SMBv3 Client/Server Remote Code Execution Vulnerability, Scripting Engine Memory Corruption Vulnerability (IE Flaw - Remote Exec), and other Zero-Day malicious code drops or executions.

The Role of Frameworks

So, how do agencies secure these remote endpoints? Security teams can and should turn to commonly referenced security standards and frameworks for cybersecurity best practices and effective guidance on the methods necessary to ensure security and compliance. At a minimum, agency personnel should reference compliance requirements as identified in FISMA, HIPAA, or CMMC, as well as department- and agency-specific policies. These are by nature required and thus something that must be tackled immediately.

There are commonly referenced security frameworks such as the NIST CSF, NIST 800 series publications and the CIS Controls, which provide a more holistic approach to cybersecurity across the agency, and to which many compliance requirements align. Additionally, telework-specific guidelines have been released by CISA in TIC 3.0 Interim Telework Guidance. For example, within its universal security capabilities list we see controls such as configuration management, vulnerability assessment, dynamic threat detection, strong authentication, backup and recovery of data, etc.

Specific to the home environment, CIS provides its CIS Controls Telework and Small Office Network Security Guide which includes guidelines for securing small office and home office environments, such as how to properly set up devices, networks and encryption standards that each federal worker can apply to his/her home environment.

Given these available frameworks, we already have a rich body of guidance available to assist us in properly securing remote endpoints for any enterprise. That being said, properly securing remote environments is less about doing something fundamentally different, and more about doing the same essential security basics in different environments—with a focus on doing those basics well. In order to prioritize these efforts, we need to focus our attention on the most basic controls: asset inventory, secure configuration management, vulnerability management, audit logging, and change control.

How then do we successfully implement these controls and properly secure remote points for federal employees in a maximum telework situation, given the constraints presented in home environments? The good news is that the following technical constraints don't have to preclude the security of remote endpoints when using the right tools.

Technical Constraints

- » **Lack of security diversity:** Am I really secure?
- » **VPN will not connect, or drops connection:** Have we considered how well our VPN network can scale? Remote traffic loads? Would split-tunnel VPNs reduce loads?
- » **Security software requires secure encrypted VPN connection:** Are we being shortsighted and thinking VPN access was all we needed for remote security hygiene?
- » **No alternative connection options to meet the remote security needs of my agency:** Can your tools utilize a SOCKS5 proxy as many webservers in the DMZ do?

How Tripwire Helps

The following Tripwire solutions run with an agent on the client and are able to connect to the management console by SOCKS5 Proxy, meaning they don't require VPN connectivity. So even if an agency's VPN is completely disconnected, rest assured Tripwire security software is still doing its job and still forwarding information up to agency servers—offering premium endpoint protection for remote federal enterprise environments.

Tripwire® Enterprise

Tripwire provides cybercrime controls, change detection, and secure configuration management via file integrity management and system integrity management. tripwire.me/TE

About the NIST CSF

In understanding the role of security frameworks, we can view the NIST Cybersecurity Framework (CSF) as a kind of an organizing framework for security strategy at the enterprise level. Then, we can view the NIST 800 series publications, i.e. 800-53, as a series of detailed technical standards. The CIS Controls in many ways serve at the operational level under which technical specific sub-controls and technical standards are grouped, and in turn can be mapped to the NIST CSF. This set (and others) of standards and frameworks have proven to be effective in ensuring security and compliance.

Tripwire Log Center™

Tripwire provides a client that collects logs in a lossless fashion in real time on an agency endpoint. So if the endpoint periodically doesn't have connectivity back to the agency infrastructure, it will cache the log data and throttle it up once it has reestablished a secure TCP connection that can use a SOCKS5 proxy. tripwire.me/TLC

Tripwire IP360

Tripwire's vulnerability management solution has a client on the endpoint that can run scheduled (disconnected) full vulnerability scans 24 hours/day and then forward that information up to the vulnerability network manager at agency headquarters.

Regardless of the duration of the COVID-19 pandemic's impact, it is very likely that telework will become a constant, involuntary arrangement for much of the federal workforce. With this in mind, it is important to understand the security impacts and to deploy solutions that help agencies overcome VPN hurdles and ensure the highest standard of security monitoring. tripwire.me/IP360

SOURCES

1 https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-13.pdf

2 https://federalnewsnetwork.com/wp-content/uploads/2020/05/050120_FNNtelework_survey_results_FINAL.pdf

3 https://www.defense.gov/Explore/News/Article/Article/2147123/growth-in-dod-telework-capability-may-outlive-coronavirus-pandemic/