

Report on Supply Chain Compliance Volume 3, Number 9. April 30, 2020

Department of Defense Cyber Exchange creates telecommuting guidance portal

By Sascha Matuszak

The U.S. Department of Defense (DoD) created a [list of best practices](#),^[1] guidance, and tools for maintaining cybersecurity while telecommuting. The guidance documents are accessible to the public and, although they are directed at DoD personnel, do provide basic tips for information technology and compliance departments to shore up cybersecurity during the pandemic. Two guidance documents could be useful materials for training and reminders: [Best Practices for Keeping your Home Network Secure](#)^[2] from the National Security Agency and DoD's one-page [telework dos and don'ts](#).^[3] There is a heightened concern that hackers, stuck at home with nothing better to do, will take advantage of a reduced workforce, telecommuting and the strain of the pandemic to commit cyberespionage and identity theft. Especially with technological solutions springing up quick, taking the time to set up secure networks and protocols is good risk management.

1 "DOD Covid019 Telework Information," Department of Defense Cyber Exchange – Public, last updated April 17, 2020, <https://bit.ly/3eGzrLT>.

2 National Security Agency, "Best Practices for Keeping your Home Network Secure," September 18, 2018, <https://bit.ly/3cB8LKt>.

3 Department of Defense Cyber Exchange, "Do's and Don'ts – Network Utilization and Cybersecurity," last accessed April 24, 2020, <https://bit.ly/3eIYWvQ>.

This publication is only available to subscribers. To view all documents, please log in or purchase access.

[Purchase Login](#)