National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

WORKING ANYTIME, ANYWHERE: THE EVOLUTION OF TELEWORK

How you can help the NCCoE and NIST address the challenge of improving the management of telework-related cybersecurity and privacy risks.

OVERVIEW

Today, many employees telework (also known as “telecommuting,” “work from home,” or “work from anywhere.”) *Teleworking* is the ability of an organization’s employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization’s facilities. Telework has been on the rise for some time, but sharply increased in 2020 because of the COVID-19 pandemic. For many, telework is now the only way to get work done, and the original concept of “telework” has evolved into being able to work anytime, anywhere.

The technologies used for telework have also evolved recently. Examples of this include the ubiquity of mobile devices, the expectation to be able to access information from anywhere at any time, and the highly distributed nature of data and apps across end user devices, data centers, and clouds. Telework and zero-trust architecture may even be converging in the near future.

All of these changes are affecting cybersecurity and privacy risks, and organizations need to be aware of and manage these risks. Accordingly, we are soliciting public feedback on the topic. We are also building a community of interest so that interested individuals and organizations can follow the progress of our telework cybersecurity and privacy publications and can provide input on them. Contact us at telework@nist.gov to join the community of interest or to provide feedback on the topic of telework cybersecurity and privacy.

PLANNED UPDATES TO SPECIAL PUBLICATION 800-46

Special Publication (SP) 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, was most recently updated in 2016. It presents recommendations for safeguarding the technologies used for telework and remote access.

We are soliciting public feedback on this Special Publication to identify areas that industry, government, and others deem most important to revise or add. Send your comments to telework@nist.gov.

You are welcome to comment and suggest changes and enhancements to any parts of the publication. We are particularly interested in comments on our planned objectives for updating SP 800-46, which are listed in the table on the next page along with the high-level changes each objective is intended to address. You are encouraged to provide feedback on the table, citing the relevant objectives and changes by number and letter, respectively. After we review all comments and finalize the table, it will serve as the basis of determining what needs to be revised in SP 800-46 and other NIST publications on telework cybersecurity and privacy.

Join the Telework Community of Interest by contacting us at telework@nist.gov.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
https://www.nccoe.nist.gov.

CONTACT US
nccoe@nist.gov
301-975-0200

OBJECTIVE	HIGH-LEVEL CHANGES TO ADDRESS
Objective 1: Reflect changes in how telework is performed.	a. More people are teleworking, many of whom haven't teleworked before. b. Many people are teleworking for extended periods of time, with neither the people nor their devices necessarily visiting the organization's facilities during that time. c. Mobile device usage has increased, and mobile devices can do much more than they used to. d. Teleworkers frequently use services not controlled by the organization, such as ad hoc file sharing, instant messaging/chat, and teleconferencing and videoconferencing services. e. Organization-controlled and personally-owned technologies are increasingly intermingled. f. Telework is more often occurring from networks shared with potentially compromised Internet of Things (IoT) devices. g. By default, the networks that the devices are connected to are untrusted and exposed to malicious attacks.
Objective 2: Reflect changes in the role of remote access technologies.	a. The migration to cloud-based applications and services has degraded traditional perimeter-based security models. b. A smaller percentage of telework traffic is passing over an organization's networks unless that traffic is specifically tunneled through those networks, so organizations are losing visibility and control. c. Device and access provisioning occur away from the organization's facilities. d. Many organizations are adopting zero-trust principles.
Objective 3: Update all references and mappings to references.	a. The NIST Cybersecurity Framework and SP 800-53 publications have been updated since the last SP 800-46 revision, so their mappings are out of date. b. The NIST Privacy Framework has been released since the last SP 800-46 revision, so mappings to it could be added to SP 800-46. c. Several other NIST publications with related material have been created or updated since the last SP 800-46 revision.
Objective 4: Shorten SP 800-46 to improve its readability.	a. Some of the existing material is already widely known by today's readers or is no longer relevant to most readers. b. There may be content in SP 800-46 that is now also covered in other NIST publications. c. There are additional telework topics to address, like teleconferencing / videoconferencing security practices or secure file transfer technologies, but they are discrete and evolving. It is unclear how much of this new content should be added to SP 800-46 versus producing separate documents on individual topics.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interesting in joining the Telework Community of Interest, please send an email to telework@nist.gov.