CAPACITY ENHANCEMENT GUIDE: PRINTING WHILE WORKING REMOTELY

PURPOSE

The increase in teleworking across federal agencies has extended the enterprise perimeter into employees' homes. Expanded telework has created additional security challenges, such as ensuring secure remote access and enforcing remote patch and vulnerability management.[1] Printing while working remotely is another security challenge because of the risks posed when agency personnel move data from federal information systems to physical space outside of agency control. These risks include increasing a federal agency's attack surface, reducing the effectiveness of existing cybersecurity controls, and increasing the potential for data loss and exposure. As agencies continue to acclimate to the expanded telework environment, it is important to note that each agency remains responsible for identifying, safeguarding, and managing all records—including hard copies and other printed materials—in accordance with federal laws and regulations.[2]

AT-A-GLANCE RECOMMENDATIONS

- Develop and issue an agency-wide policy on printing while teleworking
- Follow the principle of "allow by exception"
- Establish an approval process
- Communicate data handling and disposal requirements

This Capacity Enhancement Guide details Cybersecurity and Infrastructure Security Agency (CISA) recommendations for developing agency-level policies and procedures related to printing from home while teleworking. Specifically, this guide provides CISA's recommendations on the following topics: (1) developing an agency-wide policy for printer use during remote work, (2) establishing an approval process, and (3) handling, storing, and disposing of printed materials.

AUDIENCE & SCOPE

This Capacity Enhancement Guide provides actionable recommendations for federal civilian executive branch (FCEB) agencies for managing security risks associated with printing while working remotely.

This guide is intended for FCEB senior cybersecurity leadership and provides detail to support a technical discussion with implementation teams. State, local, tribal, and territorial (SLTT) governments and other organizations could also benefit from this guide.

Capacity Enhancement Guides support CISA's role as the Nation's cybersecurity risk advisor by sharing high-priority recommendations, best practices, and operational insights in response to systemic threats, vulnerabilities, and risks.

RECOMMENDATIONS

- **Develop and issue an agency-wide policy on printer use during remote work.** In general, agencies should prohibit employees and contractors from printing while working remotely unless the agency issues a policy that provides a clear exception and employees follow appropriate information security procedures. This policy should specify when it is permissible to print while working remotely and document the processes and procedures related to such printer use. Both federal employees and government contractors should be subject to this policy, and all users should receive proper training. CISA recommends this policy includes the following items:

[1] Please refer to the Remote Patch and Vulnerability Management Capacity Enhancement Guide for Federal Agencies
[2] Please refer to 44 U.S. Code §2904 and 3301; 36 Code of Federal Regulations (CFR) §1222.

- A general rule that (1) strongly discourages employees from printing while working remotely unless circumstances warrant an explicit exception[3] and (2) instructs employees to avoid printing documents that contain sensitive information.
- Enumerated exceptions that clearly define and describe the specific factors that must be established. The agency's mission and operations, as well as the employee's job duties, should determine exceptions.
- A strict prohibition on connecting any unauthorized equipment to Government Furnished Equipment (GFE).[4]
- Instructions on whether employees may seek approval to use personally owned printers and on the preferred method of connection (i.e., wired vs. wireless). This policy should also consider the handling of printer drivers and updates. **Note:** see "Establish an approval process" below.
- Alternative options for printing that may include directing employees to print documents at their local office (in accordance with current safety protocols) or providing government-issued printers to employees who need to print based on their role and responsibilities.
- Identification and potential resolutions of common compliance challenges. For example, the policy should remind employees that both emailing work-related documents to a personal email address and using a commercial printing service for official business are prohibited.

- **Establish an approval process.** Agencies should outline a process that requires employees and contractors to seek and obtain a formal approval before printing work materials from a personally owned printer.
- **Communicate data handling, storage, and disposal requirements.** Agencies should establish procedures for the proper handling, storage, and disposal of all work-related printed materials. Agencies should confirm that employees approved to print while teleworking are aware of their obligation to comply with all federal laws and regulations related to records management and should ensure those employees have completed the required training.

CONTACT INFO

For questions about this guidance and other CISA services available to federal agencies, please contact cyberliaison@cisa.dhs.gov.

Last updated: May 11, 2021

[3] For example, printing while working remotely may be necessary when a "wet" signature is required.
[4] Examples of unauthorized equipment include thumb drives and personal phones.