REDUCING THE CYBERSECURITY RISKS OF PORTABLE STORAGE MEDIA IN OT ENVIRONMENTS

Portable storage media continue to be useful tools for transferring data physically to and from Operational Technology (OT) environments. For example, media can be used for updating firmware for a device in an isolated OT network or retrieving log data for offsite diagnostics. Universal Serial Bus (USB) flash drives are commonly used, in addition to external hard drives, CD or DVD drives, and other removable media.

Though portable storage media are convenient, their usage poses cybersecurity risks for operational environments. Procedural, physical, and technical controls are important for minimizing the likelihood of a cyberattack from portable storage media usage. The National Cybersecurity Center of Excellence (NCCoE) has developed cybersecurity considerations to be integrated into a broader cybersecurity risk management program to help OT personnel use portable storage media securely and effectively.

PROCEDURAL CONTROLS

An organization should develop policies that support asset management and enforce:

- Purchasing, authorizing, and managing organization-owned media. Devices provided by other sources should be considered untrusted.
- Procuring devices that support hardware-based encryption standards such as FIPS.
- Prohibiting media usage unless expressly authorized. Authorization should be limited to specific personnel and purposes.
- Procedures for provisioning, usage, storage, sanitization, and destruction.
- Enabling logs for traceability (e.g., system and user identity, device serial number, date and time).
- Training staff on policy and procedures.

PHYSICAL CONTROLS

One way to minimize risk when using portable storage media is to apply physical controls for accessing, labeling, and storing the media.

- Media should be stored in a physically secure location where only authorized individuals have access.
- Approved portable storage media should be inventoried and labeled. Labels may indicate:
  - Who may use it
  - On which network/system it may be used
  - Its functional purpose

Having a designated space to store approved media, in conjunction with access control and labeling, is a foundation for a well-implemented set of physical controls. This can be part of a larger asset management program.

NIST Special Publication
NIST SP 1334
https://doi.org/10.6028/NIST.SP.1334
September 2025

TECHNICAL CONTROLS

Media should be protected consistent with guidance found in NIST SP 800-82, Revision 3. An organization should establish technical controls that enforce:

- Disabling unnecessary ports. This can be done logically (e.g., BIOS, operating system, or group policy) or physically (e.g., port locks, epoxy, locking cabinets).
- Restricting devices or file execution through allowlisting solutions.
- Scanning of media before and after use.
  - Use updated malware detection software for automatic scans.
  - When inserting media into unsupported devices, scan from an approved alternate device.
- Reformatting devices before reusing them on different equipment or environments.
- Write-protection when files only need to be read.
- Disabling Autorun.
- Encrypting the data stored on portable storage media using a FIPS-certified algorithm.
- Detection of removable media activity by configuring alerts on insertion and data transfer.

TRANSPORT AND SANITIZATION

Transportation within and between organizations introduces risk, which can be reduced by applying additional physical and logical controls. NIST SP 800-53, Revision 5 provides additional details on Media Protection.

- Encryption or a locked container can be used to securely transport USB devices within an organization.
- Hash or checksum verification should be performed when transporting files (e.g., between the integrator and the asset owner).
- Sanitization should be performed prior to disposing of the USB device. Media sanitization should include monitoring, reviewing, approving, tracking, and documenting actions. For more details, see NIST SP 800-88, Revision 2*, Guidelines for Media Sanitization.

CONCLUSION

Organizations can reduce the cybersecurity risks of USB device use with secure physical and logical controls on the access, storage, and usage of USB devices, and training on how to utilize USB devices safely and effectively in OT environments.

For more information on specific controls, please refer to Guide to Operational Technology (OT) Security (NIST SP 800-82 Rev. 3), Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5), and Guidelines for Media Sanitization (NIST SP 800-88 Rev. 2*).

* Rev. 2 is in initial public draft phase

LEARN MORE

For more information about NCCoE Manufacturing, visit: https://www.nccoe.nist.gov/manufacturing

@NISTcyber

linkedin/showcase/nccoe