AIR FORCE CIVIL ENGINEER

CONTROL SYSTEMS CYBERSECURITY

Control systems regulate everything, from the thermostats in our homes to the airfield lights illuminating our runways. These seemingly innocuous systems can become the foundation for advanced cyberattacks – compromising our systems and disabling critical infrastructure, which could significantly degrade our ability to execute the mission. All Airmen must contribute to securing Air Force IT and OT to ensure mission success.

"VigilanCE" Training Video*

Learn how all Airmen (to include craftsmen and wage-grade professionals) can help protect against adversaries. This video features interviews with cybersecurity Subject Matter Experts and senior leaders, including:

Lt Gen John Cooper
Deputy Chief of Staff for Logistics, Engineering, & Force Protection

Mr Peter Kim, SES
Chief Information Security Officer

Mr Edwin Oshiba, SES
Deputy Director of Civil Engineers

Watch the 2-Minute Trailer: https://go.usa.gov/xRPMZ
Watch the Full 50-Minute Video: https://go.usa.gov/xN6Pa

*CAC credentials are required to view – internal DoD viewing purposes only, NOT for public release

Reference additional materials for actions YOU can take and recent policy, education, and guidance:

https://www.milsuite.mil/book/groups/air-force-control-systems-community

Connect with the AFCEC Reach Back Center to contact AFCEC/COM with questions pertaining to control systems cybersecurity:

☎ 1 (888) 232–3721

✉ AFCEC.RBC@us.af.mil

Control Systems Cyber Hygiene Checklist for All Airmen

- ❑ Know what control systems (CS) are, the role they play in our daily lives and for the Air Force mission
- ❑ Know your cybersecurity reporting chain and POCs
- ❑ **If you see something, say something**
- ❑ Ensure all personnel and contractors have completed annual cybersecurity awareness training
- ❑ Particularly for CS operators/technicians, understand the cyber impact of changes made to the CS and, if required, coordinate with your cybersecurity reporting chain
- ❑ Incorporate cybersecurity language into maintenance and procurement contracts
- ❑ Read and adhere to cybersecurity policy (e.g., AFI 17-101, AFGM2017-32-01)
- ❑ Seek additional training on cybersecurity and the protection of control systems
- ❑ Encourage organic knowledge-sharing between colleagues, operators, technicians, and across career fields
- ❑ Apply password and administrative access best practices:
    - ❑ Ensure all personnel are educated on their responsibility for password/account protection
    - ❑ Change default passwords to meet DoD password requirements
    - ❑ Use multi-factor authentication where possible (e.g., CAC, biometrics)
    - ❑ Apply “principle of least privilege” to limit authorized users on an as-needed basis with permissions pertinent to the users’ role
    - ❑ Delete unused accounts
    - ❑ Limit access to a CS’s recovery mode to the unique account(s) of individual user(s) with a role requiring access
    - ❑ Do not share passwords
    - ❑ Especially in situations where CS cannot support authentication, implement rigorous physical security controls
- ❑ Secure, control, and monitor physical access to control systems:
    - ❑ Document who has control over the CS equipment locations
    - ❑ If a CS is located in a classified area, document Joint Personnel Adjudication System (JPAS) SMO code and POC
    - ❑ Document and confirm the physical security of CS and components in the inventory
    - ❑ Review and restrict physical access to CS and components on an as-needed basis
- ❑ Disable or remove remote (off-site) access to modems or other devices
- ❑ Diligently install and maintain patches
- ❑ Regularly perform backups
- ❑ Develop and practice recovery procedures for all control systems
- ❑ Do not plug in external, removable devices into CS (e.g., thumb drives, hard drives, personal devices)
- ❑ Do not install new software unrelated to the operations and maintenance of the system (e.g., games, chat, gambling)
- ❑ Remove all non-essential software (e.g., games, chat, gambling) from any CS
- ❑ Before clicking on links or system prompts: stop, think, and check if it is expected, valid, and trusted
    - ❑ Be cautious of any messages you receive that contain a hyperlink even if it seems to be from a friend or a trusted organization