



CMMC

SYSTEM & COMM PROTECTION

Keep the Good In, Keep the Bad Out.

The System and Communications Protection family is all about how your systems talk to each other and who can listen in. It focuses on securing network boundaries, encrypting sensitive data, and protecting CUI as it moves. Essentially, you're putting gates and guards around your digital hallways so only the right traffic gets through.

Proof of Practice

Examples

- ✓ **Firewall and VPN configuration exports**
Saved configs or screenshots showing rules, VPN requirements, and restricted access to CUI networks.
- ✓ **Network diagram with CUI zones**
A current diagram showing CUI systems, external connections, and key firewalls or routers.
- ✓ **Remote access policy and user list**
A policy describing how remote access works, plus a current list of who has VPN/remote access.






The Business Impact

A small manufacturer lets engineers access CUI from home without secure VPN or strong controls. One stolen laptop later, an attacker rides that open path into the network. Proper controls show you protect data in transit and keep untrusted traffic out before it becomes a breach and a lost contract.

Available Resources

-  **FIPS 140-2: Security Req for Cryptographic Modules**
<https://csrc.nist.gov/pubs/fips/140-2/upd2/final>
-  **Cryptographic Module Validation Program (CMVP)**
<https://csrc.nist.gov/projects/cryptographic-module-validation-program>
-  **CISA Guide to Securing Remote Access Software**
<https://www.cisa.gov/resources-tools/resources/guide-securing-remote-access-software>
-  **Zscaler Internet Access (ZIA)**
<https://www.zscaler.com/products-and-solutions/zscaler-internet-access>
-  **Cloudflare Secure Web Gateway**
<https://www.cloudflare.com/zero-trust/products/gateway/>

Quick Wins

-  1. Tighten firewalls to "deny by default."
-  2. Separate admin and everyday user accounts.
-  3. Implement a VPN or ZTNA for remote access.
-  4. Confirm workstations and media are FIPS 140-2 aligned
-  5. Disable unused remote access paths.