DEPARTMENT OF DEFENSE
OFFICE OF SMALL BUSINESS PROGRAMS

PROJECT SPECTRUM

CYBER-YOU

Powered by MOVEAMERICA

PREPAREDNESS

CMMC PREPAREDNESS TRAINING

(LEVEL ONE)

HANDOUT

ACCESS CONTROL (AC)

CYBER CHALLENGE

- Users are being careless about locking their screens when they are away from their desks leaving them unsecure.
- Training has helped the issue, but what can be done to mitigate this issue further?

SOLUTION

Administrators can set the device to automatically go to a lockout screen when idle for a set period.

ACCESS CONTROL

(AC)

CMMC SOLUTION

AC.2.010 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

□ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details.
If “Not Applicable,” provide rationale.

IDENTIFICATION & AUTHENTICATION (IA)

CYBER CHALLENGE

- Each year there are large data breaches exposing logins, passwords, e-mail addresses, and other personally identifiable information (PII) .
- How can the impact of these breaches be reduced at your organization?

SOLUTION

Your administrator can set up an automatic password change after a preset number of days. It is best to set it to disallow previously used passwords.

IDENTIFICATION & AUTHENTICATION (IA)

CMMC SOLUTION

IA.2.079 Prohibit password reuse for a specified number of generations.

□Implemented □Planned to be Implemented □Not Applicable

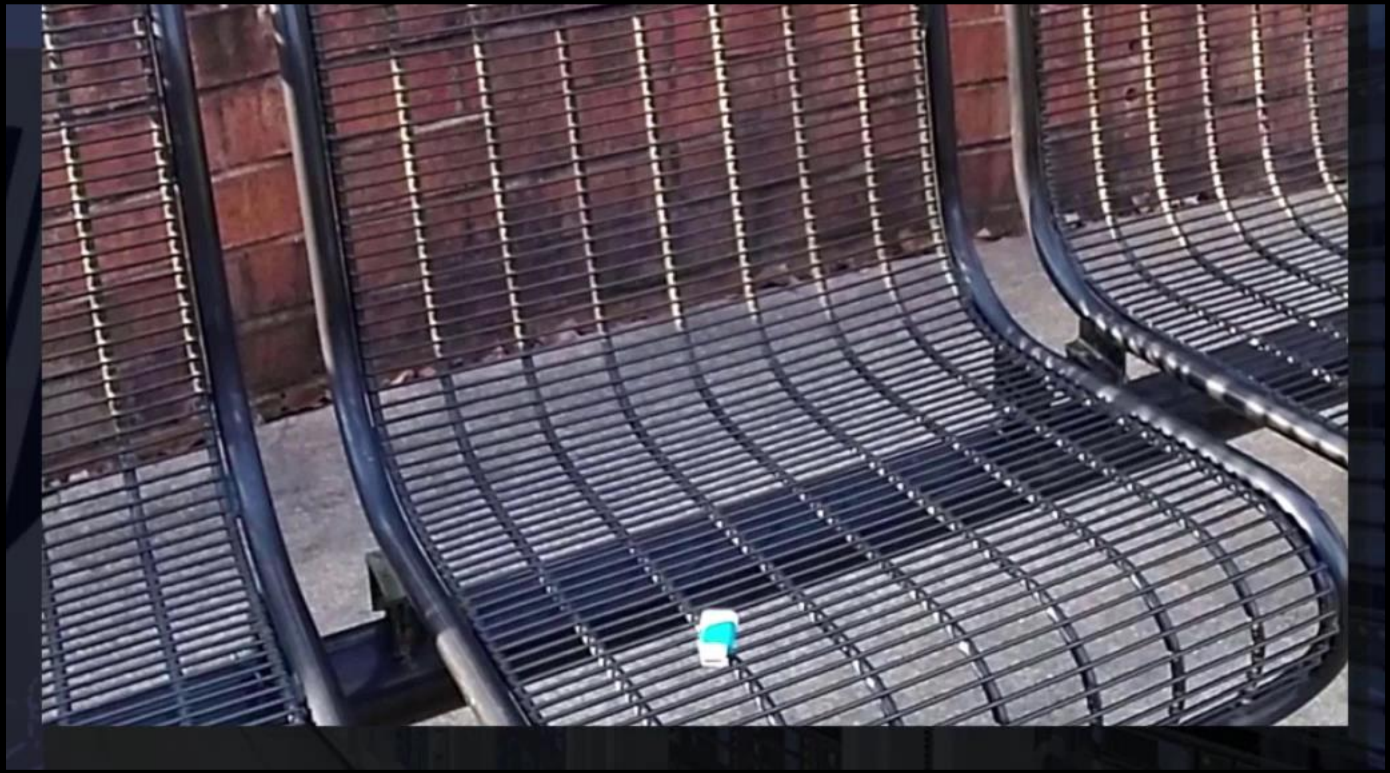
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

MEDIA PROTECTION (MP)

CYBER CHALLENGE ?

How can you secure your network from most unauthorized USB storage devices being used on your network?

SOLUTION



- The administrator can turn on bitlocker encryption on the USB devices and then on the network’s group policy to only allow encrypted USB’s.
- Personal devices are not likely to be encrypted. This solution will block personal devices also.

Media Protection
(MP)
CMMC SOLUTION

MP.3.125 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

□ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details.
If “Not Applicable,” provide rationale.

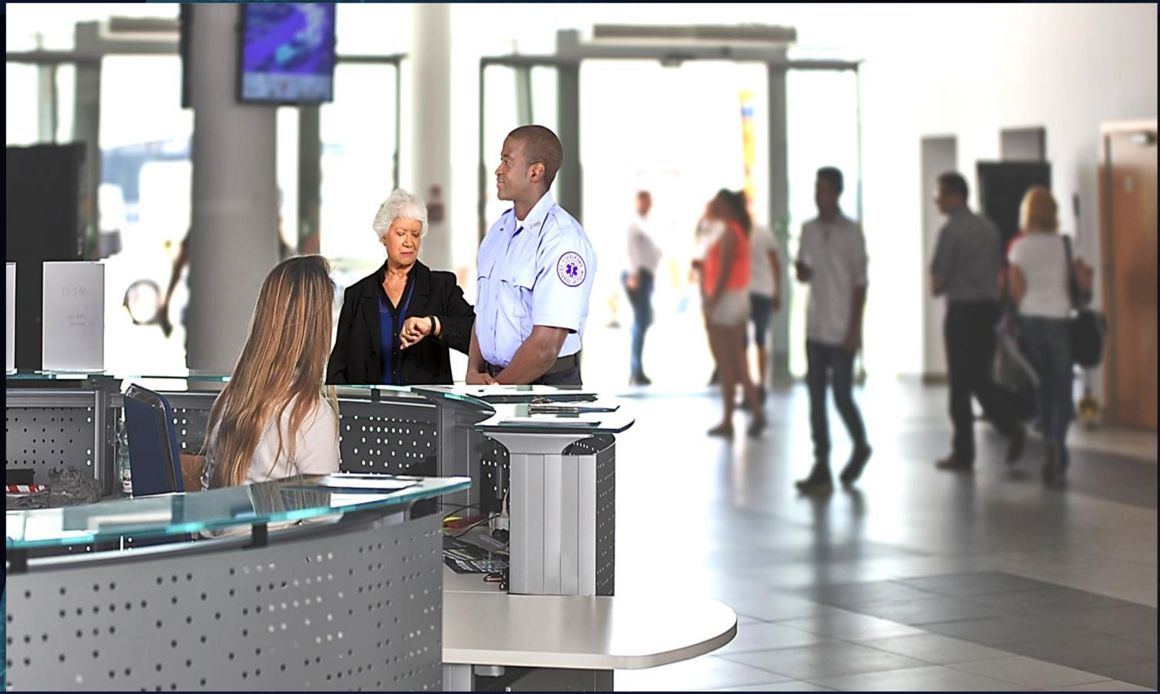
Physical Protection (IA)

CYBER CHALLENGE ?

Unauthorized visitors are often roaming the building halls looking for a point of contact.

- How can you limit this activity at your organization?

SOLUTION



Your DIB company should escort visitors and monitor activity with audit logs of physical access.

Physical Protection (PE)

CMMC SOLUTION

PE.1.132 Escort visitors and monitor visitor activity.

□ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details.
If "Not Applicable," provide rationale.

SYSTEMS & COMMUNICATIONS PROTECTION (SC)

CYBER CHALLENGE ?

- The network is suffering a brute force login attack from a vast array of IP Addresses.

- This attack is running tens of thousands of login and password variations against the network remotely, targeting the administrator/root accounts.

SOLUTION

The administrator should disable the ability for an administrator/root account to login remotely on the network.

SYSTEMS & COMMUNICATIONS PROTECTION (SC)

CMMC SOLUTION

SC.3.184 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks. 9i.e., split tunneling).

□ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details.
If “Not Applicable,” provide rationale.

SYSTEM AND INFORMATION INTEGRITY (SI)

CYBER CHALLENGE ?

- Your organization is seeing a high number of scam e-mails from lookalike domains .
- How should this behavior be handled?

SOLUTION

The administrator can quarantine mail from these ‘doppelganger’ domains. Shut down the domain and acquire it through the Uniform Domain Name Dispute Resolution Policy (UDRP) process.

SYSTEM AND INFORMATION INTEGRITY (SI)

CMMC SOLUTION

SI.2.217 Identify unauthorized use of organizational systems

□ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details.
If "Not Applicable," provide rationale.