DEFENSE CONTRACT MANAGEMENT AGENCY

Access Control

Presented By:

William R. Spence

DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

May XX, 2023

Distribution Statement A: Approved for public release. Distribution is unlimited.

DCMA
DEFENSE CONTRACT MANAGEMENT AGENCY

Agenda

- Definition
- Physical and Logical
- Related Terms
- Data Security
- NIST Special Publication 800-171 Revision 2 Requirements
- Questions

Distribution Statement A: Approved for public release. Distribution is unlimited.

Definition

- **Definition(s):** The process of granting or denying specific requests to
- 1) obtain and use information and related information processing services and
- 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Source(s):
FIPS 201-3 under Access Control

Distribution Statement A: Approved for public release. Distribution is unlimited.

DCMA
DEFENSE CONTRACT MANAGEMENT AGENCY

Physical and Logical

- Keycard or Badge Scanners in Corporate Offices **(Physical)**
  - Organizations can protect their offices by using scanners that provide mandatory access control. Employees need to scan a keycard or badge to verify their identity before they can access the building.
- Information Access Control **(Logical)**
  - Logical access control involves tools and protocols being used to identify, authenticate, and authorize users in computer systems. The access controller system enforces measures for data, processes, programs, and systems.
- Signing Into a Laptop Using a Multi-factor authentication **(Physical and Logical)**
  - A common form of data loss is through devices being lost or stolen. Users can keep their personal and corporate data secure by using a Multi-factor authentication.
- Unlocking a Smartphone With a Thumbprint Scan **(Physical and Logical)**
  - Smartphones can also be protected with access controls that allow only the user to open the device. Users can secure their smartphones by using biometrics, such as a thumbprint scan, to prevent unauthorized access to their devices.
- Remotely Accessing an Employer's Internal Network Using a VPN **(Logical)**

Distribution Statement A: Approved for public release. Distribution is unlimited.

Related Terms

Authentication

- Authentication is any process by which a system verifies the identity of a user who wishes to access the system. Because access control is typically based on the identity of the user who requests access to a resource, authentication is essential to effective security.
- User authentication is implemented through credentials which, at a minimum, consist of a user ID and password.

Authorization (access control)

- Authorization is any mechanism by which a system grants or revokes the right to access some data or perform some action. Often, a user must log in to a system by using some form of authentication. Access Control mechanisms determine which operations the user can or cannot do by comparing the user's identity to an access control list (ACL). Access controls encompass: File permissions, such as the right to create, read, edit or delete a file.
- Program permissions, such as the right to execute a program.
- Data permissions, such as the right to retrieve or update information in a database.

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

3.1.1 - Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] authorized users are identified;
  [b] processes acting on behalf of authorized users are identified;
  [c] devices (and other systems) authorized to connect to the system are identified;
  [d] system access is limited to authorized users;
  [e] system access is limited to processes acting on behalf of authorized users; and
  [f] system access is limited to authorized devices (including other systems).

- **Common Technologies**
  - System Security Plan (SSP), Policy, Procedure
  - Active Directory(AD), Application, Operating System (OS)

- **Lessons Learned/Best Practice**
  - Document how this is being achieved in the SSP
  - Devices limiting access / controlling

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] the types of transactions and functions that authorized users are permitted to execute are defined; and
  [b] system access is limited to the defined types of transactions and functions for authorized users
- **Common Technologies**
  - SSP, Policies
  - OS and application controls
- **Lessons Learned/Best Practices**
  - Document how this is being achieved in the SSP
  - Understanding the limitations of the technical controls

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.3 – CONTROL CUI FLOW

3.1.3 Control the flow of CUI in accordance with approved authorizations.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] information flow control policies are defined;
  [b] methods and enforcement mechanisms for controlling the flow of CUI are defined;
  [c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified;
  [d] authorizations for controlling the flow of CUI are defined; and
  [e] approved authorizations for controlling the flow of CUI are enforced.

- **Common Technologies**
  - SSP, Policies, Training
  - Access Control Lists (ACL), Applications, OS, Role-Based Application Control

- **Lessons Learned/Best Practices**
  - Ensure users know what is authorized
  - Ensure the flows used are authorized
  - **Write what you do and do what you write**

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.4 – SEPARATION OF DUTIES

- **3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] the duties of individuals requiring separation are defined;
  [b] responsibilities for duties that require separation are assigned to separate individuals; and
  [c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals
- **Common Technologies**
  - SSP, Policies
  - OS, Applications
- **Lessons Learned/Best Practices**
  - Separate accounts for the same person is not separation of duties
  - External monitoring

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.5 – LEAST PRIVILEGE

- **3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] privileged accounts are identified;
  [b] access to privileged accounts is authorized in accordance with the principle of least privilege;
  [c] security functions are identified; and
  [d] access to security functions is authorized in accordance with the principle of least privilege
- **Common Technologies**
  - SSP, Policies, Procedures
  - OS, Applications
- **Lessons Learned/Best Practices**
  - Do they really need that privilege or security function?
  - Privilege accounts and non-privileged (user) accounts should be separate for the same person

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.6 – NON-PRIVILEGED ACCOUNT USE

- **3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] nonsecurity functions are identified; and
  [b] users are required to use non-privileged accounts or roles when accessing nonsecurity functions.
- **Common Technologies**
  - SSP, Policies
  - OS, Applications
- **Lessons Learned/Best Practices**
  - Privilege accounts and non-privileged (user) accounts should be separate for the same person
  - Internet access for privilege accounts is a concern

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.7 – PRIVILEGED FUNCTIONS

- **3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] privileged functions are defined;
  [b] non-privileged users are defined;
  [c] non-privileged users are prevented from executing privileged functions; and
  [d] the execution of privileged functions is captured in audit logs.
- **Common Technologies**
  - SSP, Policies
  - OS, Applications, Security Incident and Event Management (SIEM)
- **Lessons Learned/Best Practices**
  - Privilege accounts and non-privileged (user) accounts should be separate for the same person
  - Understanding the limitations of the technical controls

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTEMPTS

- **3.1.8 Limit unsuccessful logon attempts.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] the means of limiting unsuccessful logon attempts is defined; and
  [b] the defined means of limiting unsuccessful logon attempts is implemented.
- **Common Technologies**
  - SSP, Policies
  - OS, Applications
- **Lessons Learned/Best Practices**
  - Ensure setting are implemented….
  - **Write what you do and do what you write**

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.9 – PRIVACY & SECURITY NOTICES

- **3.1.9 Provide privacy and security notices consistent with applicable CUI rules.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category; and
  [b] privacy and security notices are displayed.
- **Common Technologies**
  - SSP, Policies, Training, Printed Banners / Stickers
  - OS, Applications
- **Lessons Learned/Best Practices**
  - Don’t forget about printers

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.10 – SESSION LOCK

- **3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] the period of inactivity after which the system initiates a session lock is defined;
  [b] access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity; and
  [c] previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.
- **Common Technologies**
  - SSP, Policies
  - OS, Applications
- **Lessons Learned/Best Practices**
  - Ensure setting are implemented….
  - **Write what you do and do what you write**

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.11 – SESSION TERMINATION

3.1.11 Terminate (automatically) a user session after a defined condition.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] conditions requiring a user session to terminate are defined; and
  [b] a user session is automatically terminated after any of the defined conditions occur
- **Common Technologies**
  - SSP, Policies
  - Applications
- **Lessons Learned/Best Practices**
  - Screen lock on a computer is not a termination of user session…

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.12 – CONTROL REMOTE ACCESS

3.1.12 Monitor and control remote access sessions.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] remote access sessions are permitted;
  [b] the types of permitted remote access are identified;
  [c] remote access sessions are controlled; and
  [d] remote access sessions are monitored.

- **Common Technologies**
  - SSP, Policies
  - OS, Applications, Virtual Private Networks, Cloud Services

- **Lessons Learned/Best Practices**
  - Know what these means to your environment, know how it impacts other requirements

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.13 – REMOTE ACCESS CONFIDENTIALITY

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and
  [b] cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.
- **Common Technologies**
  - SSP, Policies
  - OS, Applications, Virtual Private Networks, Cloud Services
- **Lessons Learned/Best Practices**
  - If it is protecting CUI in transit it will have to be Federal Information Processing Standards (FIPS) 140-2 or 140-3 validated

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.14 – REMOTE ACCESS ROUTING

3.1.14 Route remote access via managed access control points.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] managed access control points are identified and implemented; and
  [b] remote access is routed through managed network access control points.
- **Common Technologies**
  - SSP, Network Diagrams
  - OS, Applications, Virtual Private Networks, Cloud Services
- **Lessons Learned/Best Practices**
  - Ensure the network boundaries are identified properly

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.15 – PRIVILEGED REMOTE ACCESS

- **3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.**
- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:

  [a] privileged commands authorized for remote execution are identified;

  [b] security-relevant information authorized to be accessed remotely is identified;

  [c] the execution of the identified privileged commands via remote access is authorized; and

  [d] access to the identified security-relevant information via remote access is authorized.
- **Common Technologies**
  - SSP, Policy
  - OS, Applications, Virtual Private Networks, Cloud Services
- **Lessons Learned/Best Practices**
  - The technical implementation should support the policy that is authorized

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.16 – WIRELESS ACCESS AUTHORIZATION

3.1.16 Authorize wireless access prior to allowing such connections.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:

  [a] wireless access points are identified; and

  [b] wireless access is authorized prior to allowing such connections

- **Common Technologies**
  - SSP, Network Diagrams
  - Wireless Access Points, Controllers, Certificates,
- **Lessons Learned/Best Practices**
  - This requirement is applicable even if you don't use wireless, as policy should direct its use is not permitted

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.17 – WIRELESS ACCESS PROTECTION

3.1.17 Protect wireless access using authentication and encryption.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] wireless access to the system is protected using authentication; and
  [b] wireless access to the system is protected using encryption

- **Common Technologies**
  - Wireless Access Points, Controllers, Certificates
- **Lessons Learned/Best Practices**
  - If the wireless is protecting CUI in transit it will need to utilize FIPS 140-2 or 140-3 Validated encryption

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.18 – MOBILE DEVICE CONNECTION

3.1.18 Control connection of mobile devices.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] mobile devices that process, store, or transmit CUI are identified;
  [b] mobile device connections are authorized; and
  [c] mobile device connections are monitored and logged.

- **Common Technologies**
  - SSP, Policy, Procedure
  - Certificates, Mobile Device Management (MDM)

- **Lessons Learned/Best Practices**
  - This requirement is applicable even if you don't use mobile devices, as policy should direct its use is not permitted

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.19 – ENCRYPT CUI ON MOBILE

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified; and
  [b] encryption is employed

- **Common Technologies**
  - SSP, Policy, Procedure
  - Certificates, Mobile Device Management (MDM)

- **Lessons Learned/Best Practices**
  - Encryption associated with this will need to utilize FIPS 140-2 or 140-3 Validated encryption

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L1-3.1.20 – EXTERNAL CONNECTIONS

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] connections to external systems are identified;
  [b] the use of external systems is identified;
  [c] connections to external systems are verified;
  [d] the use of external systems is verified;
  [e] connections to external systems are controlled/limited; and
  [f] the use of external systems is controlled/limited.

- **Common Technologies**
  - SSP, Network Diagrams
  - Firewalls
- **Lessons Learned/Best Practices**
  - This impacts other requirements like split tunneling…

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L2-3.1.21 – PORTABLE STORAGE USE

3.1.21 Limit use of portable storage devices on external systems.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] the use of portable storage devices containing CUI on external systems is identified and documented;
  [b] limits on the use of portable storage devices containing CUI on external systems are defined; and
  [c] the use of portable storage devices containing CUI on external systems is limited as defined.

- **Common Technologies**
  - SSP, Policy, Training
  - Data Loss Prevention(DLP), Data Rights Management (DRM), Endpoint Security / Agents

- **Lessons Learned/Best Practices**
  - This is using company owned device on systems outside of the organizations systems

Distribution Statement A: Approved for public release. Distribution is unlimited.

AC.L1-3.1.22 – CONTROL PUBLIC INFORMATION

3.1.22 Control CUI posted or processed on publicly accessible systems.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:

  [a] individuals authorized to post or process information on publicly accessible systems are identified;

  [b] procedures to ensure FCI is not posted or processed on publicly accessible systems are identified;

  [c] a review process is in place prior to posting of any content to publicly accessible systems;

  [d] content on publicly accessible systems is reviewed to ensure that it does not include FCI; and

  [e] mechanisms are in place to remove and address improper posting of FCI.

- **Common Technologies**
  - SSP, Policy, Procedure, Training
  - Trackers
- **Lessons Learned/Best Practices**
  - Mechanisms can be procedures and incident response actions

Distribution Statement A: Approved for public release. Distribution is unlimited.

AWARENESS AND TRAINING (AT) - 3.2

What does Awareness and Training have to do with Access Control?

- **Training is based on the individuals access**
  - Managers
  - System Admins
  - Users

- **Lessons Learned/Best Practices**
  - It is not a one size fits all, individual needs to be made aware of the security risks associated with their activities which are associated with access

Distribution Statement A: Approved for public release. Distribution is unlimited.

AUDIT AND ACCOUNTABILITY (AU) -3.3

Access Control directly impacts Audit and Accountability

- **Logs are all based on requirements from 3.1 ACCESS CONTROL**
  - Who has access to CUI (users, admins, devices)
  - What CUI they have access to (project based)
  - When they can access CUI (time-based access control)
  - Where they can access CUI from (devices)
- **Lessons Learned/Best Practices**
  - Ensure the logs are capturing everything needed to support an investigation and hold individuals accountable for their actions

Distribution Statement A: Approved for public release. Distribution is unlimited.

CM.L2-3.4.5 – ACCESS RESTRICTIONS FOR CHANGE

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

  Determine if:
  [a] physical access restrictions associated with changes to the system are defined
  [b] physical access restrictions associated with changes to the system are documented
  [c] physical access restrictions associated with changes to the system are approved
  [d] physical access restrictions associated with changes to the system are enforced
  [e] logical access restrictions associated with changes to the system are defined
  [f] logical access restrictions associated with changes to the system are documented
  [g] logical access restrictions associated with changes to the system are approved; and
  [h] logical access restrictions associated with changes to the system are enforced.

- **Common Technologies**
  - SSP, Policy, Procedure, Training
  - Service Desk ticketing systems, Trackers

- **Lessons Learned/Best Practices**
  - Ensure the physical access to systems (server rooms, communications closets, etc..) is defined

Identification and Authentication (IA) 3.5

Access Control is dependent on proper identification and authentication

- **Establishes guidelines for strong identification and authentication**
  - Identifiers
  - Multi-Factor Authentication (MFA)
  - Temporary access
  - Passwords
- **Lessons Learned/Best Practices**
  - Use Multi-Factor Authentication (MFA)

Distribution Statement A: Approved for public release. Distribution is unlimited.

INCIDENT RESPONSE(IR) - 3.6

Incident Response is dependent on Access Control

- **Establishes when an incident occurs**
  - Unauthorized access
    - Physical
    - Logical
- **Identifies who to report it to**
- **Lessons Learned/Best Practices**
  - Know who to report

Distribution Statement A: Approved for public release. Distribution is unlimited.

Maintenance (MA) – 3.7

Maintenance is dependent on Access Control

- **Who can perform maintenance**
  - Authorized access
    - Physical
    - Logical
  - Unauthorized access
    - Physical
    - Logical
- **Lessons Learned/Best Practices**
  - Supervise maintenance personnel without required access

Distribution Statement A: Approved for public release. Distribution is unlimited.

Media Protection (MP) 3.8

Media requires Access Control

- **Who can access the media**
  - Paper
  - Electronic
  - Authorized access
    - Physical
    - Logical
  - What, Where, when…
- **Lessons Learned/Best Practices**
  - Access to media is limited

Distribution Statement A: Approved for public release. Distribution is unlimited.

Personnel Security (PS) - 3.9

Access Control is dependent on Personnel Security

- **Who can get access to CUI**
  - Authorized access
    - Physical
    - Logical
- **Lessons Learned/Best Practices**
  - Not everyone needs access (i.e. Cleaning Access)

Distribution Statement A: Approved for public release. Distribution is unlimited.

PE.L1-3.10.1 – LIMIT PHYSICAL ACCESS

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

- **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**
  Determine if:
  [a] authorized individuals allowed physical access are identified
  [b] physical access to organizational systems is limited to authorized individuals
  [c] physical access to equipment is limited to authorized individuals; and
  [d] physical access to operating environments is limited to authorized individuals.
- **Common Technologies**
  - SSP, Policy, Procedure
  - Access Badges
- **Lessons Learned/Best Practices**
  - Master keys to buildings…
  - Cleaning personnel

Distribution Statement A: Approved for public release. Distribution is unlimited.

Risk Assessment (RA)

Access Control is dependent on Personnel Security

- **Who can get access to CUI**
  - Authorized access
    - Physical
    - Logical
- **Lessons Learned/Best Practices**
  - Not everyone needs access (i.e. cleaning personnel)

Distribution Statement A: Approved for public release. Distribution is unlimited.

Risk Assessment (RA) -3.12

- **Access Control can impact the risk assessment**
- **System Security Plan**
  - Identifies
  - Documents
- **Lessons Learned/Best Practices**
  - Write what you do and do what you write

Distribution Statement A: Approved for public release. Distribution is unlimited.

System and Communications Protection (SC) – 3.13

- **Access Control is supported by System and Communications Protection**
- **Where is the CUI**
  - Network protections
- **Who can Access it**
  - Privilege
  - Non-Privilege
- **Lessons Learned/Best Practices**
  - Not everyone needs access (i.e. cleaning personnel)

Distribution Statement A: Approved for public release. Distribution is unlimited.

System and Communications Protection (SC) 3.14

- **Access Control is supported by System and Communications Protection**
- **Where is the CUI**
  - Identified in CUI Flow from 3.1
  - Identifies where protections are needed
- **Lessons Learned/Best Practices**
  - Know the CUI flow

Distribution Statement A: Approved for public release. Distribution is unlimited.

DCMA
DEFENSE CONTRACT MANAGEMENT AGENCY

Questions

Distribution Statement A: Approved for public release. Distribution is unlimited.