AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems). 1. Authorized Users are identified 2. Processes acting on behalf of authorized users are identified 3. Devices authorized to connect to the system are identified when creating, accessing, transmitting, and/or storing regulated (FCI/CUI) 4. System access is limited to authorized users 5. System access is limited to process acting on behalf of authorized users 6. System access is limited to authorized devices
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute. 1. The types of transaction and functions that authorized users are permitted to execute are defined. 2. System access is limited to the defined types of transactions and functions for authorized users.
AC.1.003	Verify and control/limit connections to and use of external information systems. 1. Connections to external systems are identified. 2. The use of external systems is identified 3. Connections to external systems are verified 4. Connections to external systems are controlled/limited 5. The use of external systems is controlled/limited.
AC.1.004	Control information posted or processed on publicly accessible information systems. 1. Procedures to ensure FCI/CUI is not posted to processed on publicly accessible systems are identified. 2. A review process is in place prior to posting of any content on publicly accessible systems. 3. Content on publicly accessible systems is reviewed to ensure that it does not include FCI/CUI. 4. Mechanisms are in place to remove and address improper posting of FCI/CUI.
IA.1.076	Identify information system users, processes acting on behalf of users or devices. 1. System users are identified 2. Processes acting on behalf of users are identified 3. Devices accessing the system are identified

IA.1.077	Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems. 1. System users are identified 2. Processes acting on behalf of users are identified 3. Devices accessing the system are identified
MP.1.118	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse. 1. System media containing CUI is sanitized or destroyed before disposal. 2. System media containing CUI is sanitized before it is released for reuse.
PE.1.131	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals. 1. Authorized individuals allowed physical access are identified. 2. Physical access to organizational systems is limited to authorized individuals. 3. Physical access to equipment is limited to authorized individuals. 4. Physical access to operating environments is limited to authorized individuals.
PE.1.132	Escort visitors and monitor visitor activity. 1. Visitors are escorted 2. Visitor activity is monitored
PE.1.133	Maintain audit logs of physical access
PE.1.134	Control and manage physical access devices. 1. Physical access devices are identified. 2. Physical access devices are controlled. 3. Physical access devices are managed.
SC.1.175	Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. 1. The external system boundary is defined in the System Security Plan (SSP). 2. Key internal system boundaries are defined in the System Security Plan (SSP). 3. Communications are monitored at the external system boundary. 4. Communications are monitored at key internal boundaries.

	5. Communications are controlled at the external system boundary. 6. Communications are controlled at key internal boundaries.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 1. Publicly accessible system components are identified. 2. Subnetworks for publicly accessible system components are physically or logically separated from internal networks.
SI.1.210	Identify, report and correct information and information system flaws in a timely manner. 1. The time within which to identify system flaws is specified. 2. System flaws are identified within the specified time frame. 3. The time within which to report system flaws is specified. 4. System flaws are reported within the specified time frame. 5. The time within which to correct system flaws is specified. 6. System flaws are corrected within the specified time frame.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems. 1. Designated locations for malicious code protection are identified. 2. Protection from malicious code at designated locations is provided.
SI.1.212	Update malicious code protection mechanisms when new releases are available.

SI.1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed. 1. The frequency for malicious code scans is defined. 2. Malicious code scans are performed with the defined frequency. 3. Real-time malicious code scans of files from external sources as files are downloaded, opened or executed are performed.