FAR Clause 52.204-21(b)(1)	NIST 800-171 Reference	Basic or Derived	800-171 Family
(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1	Basic	Access Control
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2	Basic	Access Control
(iii) Verify and control/limit connections to, and use of, external information systems.	3.1.20	Derived	Access Control
(iv) Control information posted or processed on publicly accessible information systems.	3.1.22	Derived	Access Control
(v) Identify information system users, processes acting on behalf of users, or devices.	3.5.1	Basic	Identification and Authentication
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	3.5.2	Basic	Identification and Authentication
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	3.8.3	Basic	Media Protection
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	3.10.1	Basic	Physical Protection
(ix) Escort visitors and monitor visitor activity… …maintain audit logs of physical access, and… …control and manage physical access devices.	3.10.3 3.10.4 3.10.5	Derived	Physical Protection
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	3.13.1	Basic	System and Communication Protection
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5	Derived	System and Communication Protection
(xii) Identify, report, and correct information and information system flaws in a timely manner.	3.14.1	Basic	System and Information Integrity
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.	3.14.3	Basic	System and Information Integrity
(xiv) Update malicious code protection mechanisms when new releases are available.	3.14.4	Derived	System and Information Integrity
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.14.5	Derived	System and Information Integrity