NIST 800-171 Security Control Family	NIST 800-171 High-Risk Security Control Objective per DoD*	High-impact Control per Defense Missile Agency**	NIST 800-53 Relevant Security Controls	NIST SP 800-171 Security Control Description
Access Control	3.1.1		AC-2, AC-3, AC-17	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
Access Control	3.1.2		AC-2, AC-3, AC-17	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
Access Control		3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.
Access Control		3.1.5	AC-6, AC-6(1), AC-6(5)	Employ the principle of least privilege, including for specific security functions and privileged accounts.
Access Control		3.1.8	AC-7	Limit unsuccessful logon attempts.
Access Control		3.1.10	AC-11, AC-11(1)	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.
Access Control	3.1.12		AC-17(1)	Monitor and control remote access sessions.
Access Control		3.1.13	AC-17(2)	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
Access Control	3.1.14		AC-17(3)	Route remote access via managed access control points.
Access Control	3.1.15		AC-17(4)	Authorize remote execution of privileged commands and remote access to security-relevant information.
Access Control	3.1.16		AC-18	Authorize wireless access prior to allowing such connections.
Access Control	3.1.17		AC-18(1)	Protect wireless access using authentication and encryption.
Access Control	3.1.18		AC-19	Control connection of mobile devices.
Access Control		3.1.20	AC-20, AC-20(1)	Verify and control/limit connections to and use of external information systems.
Access Control		3.1.22	AC-22	Control information posted or processed on publicly accessible information systems.

Awareness & Training	3.2.1		AT-2, AT-3	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
Awareness & Training	3.2.2	3.2.2	AT-2, AT-3	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities
Audit & Accountability	3.3.1		AU-2, AU-3, AU-3(1), AU-6, AU-12	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
Audit & Accountability	3.3.9		AU-9(4)	Limit management of audit functionality to a subset of privileged users.
Configuration Management	3.4.1	3.4.1	CM-2, CM-6, CM-8, CM-8(1)	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
Configuration Management	3.4.2		CM-2, CM-6, CM-8, CM-8(1)	Establish and enforce security configuration settings for information technology products employed in organizational information systems.
Configuration Management	3.4.3		CM-3	Track, review, approve/disapprove, and audit changes to information systems.
Configuration Management	3.4.4	3.4.4	CM-4	Analyze the security impact of changes prior to implementation.
Configuration Management	3.4.5		CM-5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
Identification & Authentication	3.5.1		IA-2, IA-5	Identify information system users, processes acting on behalf of users, or devices.
Identification & Authentication	3.5.2		IA-2, IA-5	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Identification & Authentication		3.5.3	IA-2(1), IA-2(2), IA-2(3)	Use multifactor authentication for local and network access to privileged accounts.
Identification & Authentication		3.5.7	IA-5(1)	Enforce a minimum password complexity and change of characters when new passwords are created.
Identification & Authentication	3.5.10		IA-5(1)	Store and transmit only encrypted representation of passwords.
Incident Response	3.6.1		IR-2, IR-4, IR-5, IR-6, IR-7	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
Incident Response	3.6.3		IR-3, IR-3(2)	Test the organizational incident response capability.
Maintenance		3.7.1	MA-2, MA-3, MA-3(1), MA-3(2)	Perform maintenance on organizational information systems.
Media Protection		3.8.4	MP-3	Mark media with necessary CUI markings and distribution limitations.
Media Protection		3.8.7	MP-7	Control the use of removable media on information system components.
Media Protection	3.8.8		MP-7(1)	Prohibit the use of portable storage devices when such devices have no identifiable owner.
Risk Assessment		3.11.1	RA-3	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.
Risk Assessment		3.11.3	RA-5	Remediate vulnerabilities in accordance with assessments of risk.

Systems & Communications Protection		3.13.1	SC-7, SA-8	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.
Systems & Communications Protection		3.13.6	SC-7(5)	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
System & Information Integrity		3.14.1	SI-2, SI-3, SI-5	Identify, report, and correct information and information system flaws in a timely manner.
System & Information Integrity		3.14.3	SI-2, SI-3, SI-5	Monitor information system security alerts and advisories and take appropriate actions in response.
System & Information Integrity		3.14.4	SI-3	Update malicious code protection mechanisms when new releases are available.
System & Information Integrity	3.14.7		SI-4	Identify unauthorized use of the information system.

*with DoD Risk Level per 11/8/18 Guidance (red = severe risk; amber = significant risk)

**General Greaves 1/12/18 memo re best practices against spear phishing, credential harvesting, and insecure perimeter infrastructure