Basic Cybersecurity Compliance Requirements for Government Contractors

	FAR 52.204-21	**DFARS 252.204-7012**
What does the regulation generally require?	Requires that government contractor information systems have certain basic safeguarding protections in place to preserve and protect "federal contract information."	Mandates more extensive safeguarding protections to preserve and protect "covered defense information" and requires rapid reporting of cyber incidents to the Government (i.e., within 72 hours of discovery).
What are the definitions of the key terms?	As defined, "federal contract information" means "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments."	"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html , that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is— (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. "Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.
What specific safeguarding protections are required?	Requires implementation of 17 controls from NIST SP 800-171. Specifically the contractor must: (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices	Requires implementation of all 110 controls described in NIST SP 800-171. These 110 controls are broken out into 14 control families: 1. Access Control – 22 controls including limit system access to authorized users and limit access to types of transactions and functions.

	FAR 52.204-21	**DFARS 252.204-7012**
	(including other information systems). (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute. (iii) Verify and control/limit connections to and use of external information systems. (iv) Control information posted or processed on publicly accessible information systems. (v) Identify information system users, processes acting on behalf of users, or devices. (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (ix) Escort visitors and monitor visitor	2. Awareness and Training – (3 controls) Adequately train managers, system administrator and users of security risks. 3. Audit and Accountability – 9 controls including create, protect and retain audit records to enable monitoring, analysis, investigation and reporting, and trace actions and hold accountable each individual users. 4. Configuration Management – 9 controls including establish and maintain baseline configuration and inventories of information systems and enforce security configuration settings. 5. Identification and Authentication – 11 controls including identify and authenticate users, process, and devices prior to allowing access to systems. 6. Incident Response – (3 controls) Establish operating procedures for incident handling, track, document and report incidents to appropriate officials internal and external to the organization. 7. Maintenance – 6 controls including perform maintenance and provide effective controls on tools, techniques and personnel used to conduct maintenance. 8. Media Protection – 9 controls including protect information system media, both paper and digital, limit access to the media and sanitize or destroy media before its disposal or reuse. 9. Personnel Security – (2 controls) Screen individuals prior to allowing access to systems containing CUI and protect systems during and after personnel actions such as termination or

	FAR 52.204-21	**DFARS 252.204-7012**
	activity; maintain audit logs of physical access; and control and manage physical access devices. (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. (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. (xii) Identify, report, and correct information and information system flaws in a timely manner. (xiii) Provide protection from malicious code at appropriate locations within organizational information systems. (xiv) Update malicious code protection mechanisms when new releases are available. (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	transfers. 10. Physical Protection – 6 controls including limit physical access to systems, equipment and environments to authorized personnel, protect and monitor physical facilities and infrastructure. 11. Risk Assessment – (3 controls) Conduct periodic risk assessments of organizational operations, assets, people, and associated processing, storage or transmission of CUI. 12. Security Assessment – 4 controls, including periodically access and monitor security controls, develop and implement plans of action to correct or eliminate deficiencies and vulnerabilities. 13. System and Communications Protection – 16 controls, including monitor, control and protection communications at external and internal organizational boundaries, employ techniques, designs and principles that promote effective security. 14. System and Information Integrity – 7 controls, including timely identify, report and correct system flaws, protect from malicious code and monitor system security alerts and advisories and respond appropriately.

	FAR 52.204-21	**DFARS 252.204-7012**
When do I need to be in compliance?	Compliance required at time of contract award.	Mandates compliance on or before December 31, 2017. If not in compliance at time of contract award, the contractor should notify the CO in writing of any requirement that has not yet been implemented in its system security plan (SSP) as well as a written a plan of action and milestones (POAM) for remediation for any such gaps.
Do cyber incidents need to be reported to the Government?	No	Yes. Upon discovery of a cyber incident, the contractor must "conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support." All cyber incidents must be reported to DoD at http://dibnet.dod.mil within 72 hours.
Does this requirement need to be flowed down to subcontractors?	Yes	Yes