



Orbital ATK Summary Document of DFARS, FAR, and NARA Rule Updates



- The DFARS defines “**Covered Defense Information(CDI)**” as:
 - “Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.”
 - Details about exactly what information is included in CUI can be found at the CUI Registry:
<https://www.archives.gov/cui/registry/category-list.html>
- The final rule’s safeguarding standards require agencies to protect CUI “at all times in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders.” This includes the requirement for agencies to ensure that CUI is protected by “non-executive branch entities,” **including private contractors**
- The CUI Basic and CUI Specified standards addressed in the final rule will rely upon the **National Institute of Standards and Technology’s (NIST) Special Publication (SP) 800-171** as the source of controls on CUI

- DoD published the Interim Rule on December 30, 2015 which amended DFARS 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting.” This amendment accomplished the following:
 - It extended the time for contractors to implement into their data network the security requirements specified by National Institute of Standards and Technology (NIST) **Special Publication (SP) 800-171**. This new clause gives us until **December 2017** to fully implement 800-171.
 - Within 30 days of contract award, Orbital ATK must notify the DoD Chief Information Officer of those elements of NIST 800-171 which are not currently in place within the contractor’s network.
 - The Interim Rule retained the obligation of contractors (and subcontractors) to notify DoD of a cyber incident associated with their data networks.

- FAR 52.204-21, **Basic Safeguarding of Covered Contractor Information Systems**, was issued in June 2016, and requires contractors to implement a minimum set of controls to safeguard their information systems that process, store or transmit Federal contract information. The focus of the rule is on protecting contractor systems, rather than specific government information.
- The clause imposes a set of **15 “basic” security controls** for contractor information systems where Federal contract information transits or resides. These security controls are a subset of the 109 controls listed in NIST SP 800-171. Examples are:
 - Limit information system access to authorized users or devices.
 - Authenticate or verify the identities of users, processes or devices as a prerequisite to allowing access to organizational information systems.
 - Limit physical access to organizational information systems, equipment, and operating environments to authorized individuals.

- **What?** The NARA Final Rule was just released on Wednesday, September 14th regarding the safeguarding of Controlled Unclassified Information (CUI):
 - Does not directly apply to Defense contractors
 - Sends a strong signal regarding what contractors and sub contractors can expect in terms of additional and significant safeguarding requirements for CUI
 - Publication of this final rule enables the FAR Council to move forward with a separate FAR rule addressing the implications of this new requirement on contractors that handle CUI. **A forthcoming FAR clause will apply CUI security controls to contractors.**

- **Who?**
 - NARA stands for the National Archives and Records Administration organization
 - Applies to Federal agencies and their federal information systems
 - We may be required to comply with newly implemented FAR clauses resulting from this Final Rule.

- **Where?**
 - Any federal agency or federal information system that contains CUI

- **When?**
 - This rule is effective on November 14, 2016

- **Why?**
 - To establish an open and uniform program for managing unclassified information that requires safeguarding or dissemination controls.
 - Prior to now, more than 100 different marking for this classification of information was used such as FOUO, SBU, etc.