DOD Guidance on Cyber Security

The primary purpose of this document is to collect and convey emerging information related to DOD's Guidance on Cyber Security.

In response to high profile data breaches, the DoD has engaged in an effort to strengthen its response to Cyber Security. This includes the establishment of many new guidance documents that levy new requirements on DoD contractors related to protection of sensitive information.

The document contains links to:

- Memos
- Documents
- Articles
- Other Guidance and Resources

Disclaimer: While efforts were made to capture a complete chronology, pertinent information may not be included. The third-party links are provided as a convenience and ATI is not responsible for any of these sites or their content. The information is provided 'as is' without warranties of any kind, express or implied, including accuracy, timeliness and completeness. ATI bears no risk, responsibility or liability for any action taken based on information presented herein.

Definitions

- Defense Federal Acquisition Regulation (DFAR) 252.204-7012 - clause that describes requirements for Safeguarding Covered Defense Information and Cyber Incident Reporting
- National Institute of Standards and Testing (NIST) 800-171 - publication that provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry. The security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.
- National Institute of Standards and Testing (NIST) 800-171A - publication that provides information on assessing NIST 800-171
- National Institute of Standards and Testing (NIST) Handbook 162 - The Handbook is intended to be a guide to assist U.S. manufacturers who supply products within supply chains for the DOD and who must ensure adequate security by implementing NIST SP 800-171 as part of the process for ensuring compliance with DFARS clause252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting,"
- National Institute of Standards and Testing (NIST) 800-172(DRAFT) - provides an enhanced security requirements to help protect the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) associated with critical programs or high value assets in nonfederal systems and organizations from the advanced persistent threat (APT).

DOD Guidance on Cyber Security

- Cybersecurity Maturity Model Certification (CMMC) - CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats. The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.

DoD Guidance on Enhanced Protections to be required by DoD Contractors

- November 4, 2010 Executive Order 13556 Controlled Unclassified Information[1]
- October 2016 48 CFR 252.204-7012 - Safeguarding covered defense information and cyber incident reporting[2]
- April 11, 2017 USDI Memorandum Guidance on Implementation of Controlled Unclassified Information[3]
- May 17, 2018 USDI Memorandum - Controlled Unclassified Information Implementation and Oversight for Defense Industrial Base(DIB)[4]
- Sept 17, 2017 USD ATL Memorandum Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting[5]
- June 22, 2018 Audit of the Protection of DoD Information Maintained on Contractor Systems and Networks [6]
- June 2018 NIST Special Publication 800-171 Revision 1 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [7]
- November 6, 2018 Memorandum from Under Secretary of Defense regarding guidance for assessing compliance and enhancing protections required by DFARS Clauses 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting [8]
- November 6, 2018 DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented [9]
- December 17, 2018 Memorandum from Assistant Secretary of Defense regarding how they plan on strengthening Contract Requirements Language For Cyber Security in the Defense Industrial Base [10]
- January 21, 2019 Memorandum from Under Secretary of Defense Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review [11]
- February 5, 2019 on Strategically Implementing Cybersecurity Contract Clauses [12]
- June 19, 2019 NIST SP 800-171 Rev2 - Draft - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [13]
- June 19, 2019 NIST SP 800-171B Draft - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets [14].
- February 2020, NIST SP 800-171 Rev2- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [15].
- July 2020, NIST SP 800-172 (DRAFT)- Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 (Final Public Draft) [16].
- September 29, 2020 - DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to

assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. [17]

Articles/Briefings That Summarize the DoD Intent and Plans

- American Bar Association briefing on the Cyber Security Landscape for Government Contractors [18]
- Article from a law firm summarizing how DoD plans on tightening its enforcement of Cyber Regulations related to contractor's protection of data [19]
- Memorandum from Inspector General DoD re: Audit of the Protection of DoD Information Maintained on Contractor Systems and Networks (June 22 2018) [20]
- Protecting Critical Technology Task Force [21]
- 2018 Akin Gump article "DoD and Other Agencies Seek to Enhance Contractor's Cyber and Supply Chain Security" [22]
- October 25, 2018 Defense Trade Advisory Group, DDTC and DSS Oversight of Unclassified Technical Data [23]
- April 20, 2020 - Authorized Telework Capabilities and Guidance per DoD CIO Memo [24]
- September 2020 - DFARS Interim Rule and CMMC Impacts [25]
- October 27, 2020 Department of Defense Formally Implements Cybersecurity Maturity Model Certification Requirements for Department of Defense Contractors [26]

DOD Acquisition Guidance

- Guidance to assist acquisition personnel in the development of effective cybersecurity strategies to enhance existing protection requirements provided by DFARS clause 252.204-7012 and NIST SP 800-171 can be viewed [27]
- Information concerning how System Security Plans will be reviewed/assessed by DoD is located [28]
- DOD Guidance for assessing compliance of and enhancing protections for a DOD contractor's internal Unclassified Information System can be found [29]

DOD Guidance on Cyber Security

DOD Guidance on Cyber Security