CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

DFARS CYBERSECURITY COMPLIANCE CHEAT SHEET

① DFARS

DFARS stands for Defense Federal Acquisition Regulation Supplement. The acronym doesn't give the layman much of a hint to its actual purpose. DFARS is a security standard set forth by the Department of Defense (DoD) that requires any business or entity that holds Controlled Unclassified Information (CUI) to meet the DFARS minimum security standards or runs the risk of losing all of their DoD contracts. The security requirements of DFARS are complicated and involve following some rather confusing instructions.

② It's Purpose

The internet has become a battleground for nation-state hackers who are desperate to infiltrate the networks of those they see as their enemy. We have seen this with China (PLA) and Russia (GRU) who are out there probing at everything from our critical infrastructure. such as power grids, to political interference in our elections, and digital espionage efforts that attack our businesses and military contractors. In an effort to respond to the increased aggression of nation-state sponsored attacks as well as "rogue" hackers the US responded with a compliance framework called DFARS to increase protection surrounding digital security and tightening any potential leaks of sensitive government information.

Does it Apply to You? ③

If your business processes, stores or transmits Controlled Unclassified Information you are absolutely required to pass DFARS compliance.

- Additionally, if your are a DoD contractor. subcontractor or do business with the DoD required to pass DFARS compliance.
- If a contract contains the provision 252.204-7008 you will absolutely required to comply with DFARS.
- If a contract contains the provision 252.204-7012 you will need to comply with DFARS.

© 2019 Craig Peterson. All Rights Reserved.

Continue reading on next page >

DFARS CYBERSECURITY COMPLIANCE CHEAT SHEET

(CONTINUED)

④ Non-Compliance

Businesses face losing new and existing government contracts. The Government will take a hard-line approach. including disqualification and denial for current and future Department of Defense contracts. This can mean revenue losses in excess of millions of dollars for businesses with DoD contracts in aerospace, engineering, and manufacturing, among others. Because these regulations also oblige contractors to "flow down" the regulation compliance requirements to their tier 1 suppliers. This means Any contractors who outsource their DoD work to subcontractors working with DoD contracted organizations such as independent manufacturers and engineers are also required to meet the same rigorous DFARS regulation standards for data security.

Types of Secure Data ⑤

DFARS compliance is designed to secure sensitive government information as it is processed, stored and transmitted through non-government systems. Information is most vulnerable when it is moved off its secured storage. There are three types of information covered under DFARS.
New, stricter standards, called CMMC, will be online for DFARS in January 2020.

- CDI: Covered Defense Information. These are government policies that have been identified by the DoD as sensitive or vital in the performance of a current government contract. This also includes information found, received or stored by a contractor in the service of a contract.
- CUI: Controlled Unclassified Information. We have covered CUI previously. However, in more detail CUI includes under any information that has been classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any previous or future orders, not excluding the Atomic Energy Act of 1954, as amended (NIST 800-171).
- CTI: Controlled Technical Information. Any technical information that involves the use in any capacity of military or space application.

© 2019 Craig Peterson. All Rights Reserved.

Continue reading on next page >

DFARS CYBERSECURITY COMPLIANCE CHEAT SHEET

(CONTINUED)

⑥ And There's More...

It extensively covers the operation, dissemination, processing and storing of any sensitive government information. DFARS is is a comprehensive and complex standard that covers a multitude of business operations.

- Maintenance
- Media Coverage
- Personnel Security
- Configuration Management
- Access Control
- Audit & Accountability
- System & Information Integrity
- Communication Security
- Accountability & Training

⑦ Patience Required

For many companies completing all aspects of DFARS can be a overwhelming. But if you have the time, patience and know-how to navigate the exciting waters of DFARS cyber security requirements, you may do it yourself! However remember that it is the contractors and their subcontractors that are solely responsible for meeting the DFARS requirements. There is no appeal process in which you can blame a failed DFARS examination on your hired help.

Patience Required (con't) ⑦

If you choose someone to help you with your DFARS compliance it is vital to choose a a security professional that is trustworthy and reputable and has experience with the DFARS process.. The last thing you want is to have paid for help and still not meet the compliance.

Our process works in four stages; they are as follows:

- Application Evaluation: The first step is called an NSAAP.
  - The Network Security Assessment and Action Plan (NSAAP) is exactly what is sounds like: an assessment of a contractor's current information system to determine the gaps and holes in your DFARS cybersecurity compliance. It's like doing an audit on a building before you start the renovation. You need to know where your application fails to meet the requirements before you begin to fix it. The NSAAP will review: the access to information systems, how information is stored and by whom, where data is stored, how security measures are enforced, incident response and reporting and much more!

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

© 2019 Craig Peterson. All Rights Reserved.

DFARS CYBERSECURITY COMPLIANCE CHEAT SHEET

CRAIG PETERSØN.COM

(CONTINUED)

⑦ Patience Required (con't.)

- Remediation Plan: Once the NSAAP is complete, you will need to come up with a plan of attack to fix any potential security leaks. The depth and complexity of the remediation plan will be directly related to how many problem areas were found during the NSAAP.
  - Some remediation plans can be as simple as tweaking some network controls and shoring up protocols. But depending on the state of your network and computing resources an entire overhaul might be necessary to achieve DFARS compliance.
- Continual Monitoring: After your information has been updated and all controls and systems pass NIST inspection, constant vigilance is a requirement for DFARS Compliance. Your system must also be continually monitored for potential hacker threats. This is not a one and done certification.
- Keep Track of your Documents: Once your system has pass DFARS compliance you will receive documentation proving compliance. Be sure to file this away in a safe place. It is the documentation that will provide you legal cover in the event of litigation.

⑧ Get Ready for CMMC

In June 2019 The Department of Defense announced a new framework, Cybersecurity Maturity Model Certification framework, to certify a company's compliance with federal cybersecurity regulations around controlled unclassified information (CUI.) Beginning in 2020 this framework will use a scale from 1 to 5 to evaluate and rate contractors' and subcontractors ability to protect sensitive data. As of September 2020 all defense procurement will have this as regular feature. This means that if you have any military contracts, are a sub-contractor or even a sub-sub-contractor on a military project you will have less than eight months to become compliant by implement changes with the Defense Federal Acquisition Regulation Supplement and National Institute of Standards and Technology guidance on protecting CUI.

- Will defense contractors be ready for CMMC?
- DoD Announces the Cybersecurity Maturity Model Certification (CMMC) Initiative

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We are not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, we make no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. We make no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.
If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

© 2019 Craig Peterson. All Rights Reserved.

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH