5 foundational steps to DoD cybersecurity compliance

Stephen Robison | Friday, September 9, 2022

While companies that operate as part of the Defense Industrial Base (DIB) wait for the implementation of Cybersecurity Maturity Model Certification (CMMC), it is still important that they monitor current cybersecurity obligations and compliance requirements.

Existing contractual requirements create legal obligations for DIB businesses to implement and maintain certain cybersecurity measures throughout the entirety of the contract process or risk losing the contract. Noncompliance can result in “withholding progress payments; foregoing remaining contract options; and potentially terminating the contract in part or in whole,” according to a June 2022 memo from the Department of Defense.

With new cybersecurity laws going into effect every day, the most beneficial step an organization can take is to lay a solid foundation of compliance and protection for your data, employees, and company. While the steps below are aimed at prime contractors, flow down requirements may imply downstream liability for sub-contractors.

1. Determine your data and where it is stored

Because there is no “one size fits all” solution, it is in your best interest to find the most cost effective cybersecurity measures. This starts with a determination of what data you possess and where it lives. Defense Federal Acquisition Regulation Supplement (DFARS) regulations only apply to covered contractor information systems, or “unclassified information system[s] that [are] owned, or operated by or for, a

contractor and that processes, stores, or transmits covered defense information." This means an organization can limit their cost of compliance by determining what data requires these controls and separating the information out from beginning.

2. Conduct a system audit

Once you understand what data you possess and where and how it is stored, you should determine what measures you already have in place. Some security measures - such as export control or privacy - may already suffice for certain levels of data. This step will determine where and how to effectively implement new security measures complying with all requirements.

3. Educate employees

Human error is one of the leading causes of cybersecurity incidents and data breaches. While the first two steps above address technical concerns, you cannot overlook the importance of proper employee training. Each worker needs to understand their role in protecting your organization's information and contract data. This step is important in ensuring the cyber environment is a true reflection of the work being completed.

4. Create policies and procedures

Once a system has been created and employees have been trained, your organization must guarantee that these practices will continue. Creating policies and procedures will create continuity across your systems, ensuring there is no cross contamination and all data is appropriately safeguarded with the proper cybersecurity measures.

5. Maintain and monitor

Having created a safe environment with properly trained employees following specific procedures, the next step is certifying that all systems remain compliant. This means adequate audits, controls, and reviews of the system and information within. This step should also include the continual evaluation of any new requirements. If there is any deficiency in one of the above controls, this step should highlight and include the appropriate remedy to ensure continued compliance.

While every federal agency has their own unique and complex regulations, these foundational measures will provide a strong framework to building any cybersecurity compliant environment. Additionally, the U.S. Small Business Administration has provided a basic overview of cybersecurity best practices, common threats, and available resources at Strengthen your cybersecurity

McDonald Hopkins' national Data Privacy and Cybersecurity Practice Group has expansive knowledge in assisting clients working in the Department of Defense and other federal agencies and would be happy to assist you with any of your Data Privacy of Cybersecurity needs. If you would like to learn more about how to implement these changes and stay ahead of your competition, please contact Stephen Robison. If you are a federal contractor and looking for experienced federal contracting attorneys please click here.

Stephen Robison