

Zineb Crowe

CYSE 368 CRN 25090

ODU Spring 2026

Professor Teresa Duvall

TA Joshua Russell

Reflection Paper 4: AERMOR and DOD Cybersecurity Compliance

As a DoD contractor to the U.S. Federal Government, AERMOR's work involves the protection of sensitive and mission critical information of the U.S. Government. In today's fast-paced cyber world, we must adhere to government-mandated regulations and standards, such as CMMC, FedRAMP High, and the NIST Special Publication (SP) 800 series. Specifically, these regulations are put in place to protect Controlled Unclassified Information (CUI) and other sensitive information, as well as ensure the confidentiality, integrity, and availability of federal systems. As a result, our work under the AERMOR contract continues to validate the effectiveness of our robust security controls to protect ourselves in the Navy and DoD environments.

Cybersecurity in AERMOR is aligned with the environment that supports Navy operations. In particular, the NIST SP 800 series provides the foundation for a wide range of security practices. The NIST SP 800-53 standards are a collection of security

controls that define what should be implemented in order to secure federal systems. For example, these controls generally address areas of authentication, authorization, logging, auditing, incident response, risk management, cryptography, and more. Furthermore, compliance requirements like CMMC and FedRAMP High are also heavily based upon the NIST standards and therefore become a benchmark in securing information systems and cloud environments.

FedRAMP High is one of the security classifications given to cloud services provided to the US Federal Government. In fact, it is a must-have for securing those cloud workloads that are considered sensitive. At this level, security requires end-to-end encryption, continuous monitoring, vulnerability scanning and advanced identity and access management controls. Ultimately, the goal of these requirements is to ensure that the sensitive data is secured when it is being stored or processed in the cloud.

CMMC certification is a certification that is applied to the company, not the employee. In other words, CMMC certification verifies that a contractor has implemented the appropriate cybersecurity practices and controls to safeguard government information. Therefore, an employee of a company does not hold an individual certification for CMMC. AERMOR, as a company, is currently in compliance with the current requirements necessary to perform work under Navy contracts and additionally the new certification will be at the company level.

Just like hardware and software need updates to remain current and effective, personnel must also receive ongoing training and reminders concerning the proper handling of classified and sensitive information. For instance, key training includes DoD Cyber Awareness Challenge, Controlled Unclassified Information (CUI) Training, Department of the Navy Privacy Training, FOIA and Privacy Act Training. Additionally, our personnel receive periodic training to understand their responsibilities when handling government data and reinforce the importance of protecting sensitive information.

This training and compliance framework is important for any cloud engineer to understand in their career. Today, in cloud computing platforms, Cloud Engineers play a large role in building out a secure environment on Government Clouds that meet Government compliance standards. For example, this includes building identity and access controls, securing and defining network settings, enabling features like CloudWatch and CloudTrail, and ensuring overall compliance with NIST SP 800-53 and Frameworks like FedRAMP High.

AERMOR consistently demonstrates a commitment to cybersecurity and mission support through adherence to relevant compliance frameworks, the completion of all required training for personnel and the adherence to generally accepted reliable and trusted practices for data protection. Because of this, AERMOR is able to remain ready and fully qualified to perform future DoD and other government work. Consequently, AERMOR compliance and the completion of all required training on all computer systems, software and network facilities are an extension of our overall

cybersecurity and mission support programs. Overall, this achievement of adherence to these frameworks and required training validates AERMOR's adherence to generally accepted reliable and trusted practices for data protection that are essential to being ready and qualified for future DoD and government work.

AERMOR's adherence to CMMC, FedRAMP High, and NIST SP 800-series standards ensures that we maintain a secure and trusted environment for performance of work in support of DoD missions. In addition, combining these standards with employee training and affirmative measures to prevent cybersecurity incidents ensures AERMOR is prepared and proactive in defending DoD infrastructure and information against evolving threats, while also remaining qualified and ready for performance of work on future DoD procurements.