Kael Cepak

CYSE 368

Spring 2026

Professor Teresa Duvall

TA Joshua Russell

KALO

Reflection #2

Internship Reflection – DoD and Government Cyber Requirements

Over the past few weeks of my internship at KALO, my responsibilities have shifted toward learning and understanding the Department of Defense (DoD) and broader government cybersecurity requirements for both new and existing technologies. This experience has given me a much deeper understanding of how strict and detailed cybersecurity standards are when working with government systems, especially those tied to national security. Unlike general cybersecurity practices, DoD requirements emphasize not only protection, but also compliance, documentation, and continuous validation.

One of the most important aspects of this work has been familiarizing myself with frameworks such as Risk Management Framework (RMF) and understanding how systems must be assessed, authorized, and continuously monitored. I have learned that cybersecurity in a government context is not just about implementing tools, but about proving that those tools meet specific regulatory standards. This includes ensuring confidentiality, integrity, and availability while also meeting strict guidelines for access control, encryption, and system auditing. Compared to my earlier work researching products like Goldilock's Firebreak , this task required a more structured and compliance-focused mindset.

Another key takeaway has been understanding how these requirements impact decision-making within a company. Any technology that KALO considers using or partnering with must align with DoD standards before it can even be considered viable. This means evaluating not just functionality and performance, but also whether the technology can pass certification processes and maintain compliance over time. It has become clear to me that even the most innovative cybersecurity solutions are not useful in a government setting if they fail to meet regulatory requirements.

This experience has also helped me grow professionally by improving my ability to interpret complex policies and translate them into practical considerations. Similar to how I previously

had to communicate cybersecurity risks in a business context , I am now learning how to apply regulatory language to real-world systems. This requires attention to detail, critical thinking, and the ability to connect technical requirements to operational goals.

Overall, this phase of my internship has expanded my understanding of cybersecurity beyond technical defense and into governance and compliance. It has shown me that cybersecurity professionals must be able to balance innovation with regulation, especially when working with government or military systems.

Conclusion

My recent experience at KALO has reinforced the importance of compliance in cybersecurity, particularly within the DoD and government space. Learning how technologies must meet strict regulatory standards has added a new dimension to my understanding of the field. This experience has prepared me to think more critically about how security, policy, and business decisions intersect, and it will be valuable as I continue pursuing a career in cybersecurity.