

David Seliquini

CYSE 368

Summer 2026

Professor Teresa Duvall

TA Jade Hines

Wise Technical Innovations LLC

Reflection #3

Date: July 24, 2026

I have now officially reached the 150 hour mark of my cybersecurity internship at Wise Technical Innovations. Looking back at my first 100 hours, most of my time was spent just trying to absorb the heavy academic stuff required to become a Certified CMMC Professional and Assessor. For this final 50 hour block, I finally got out of the classroom mindset and focused entirely on the day to day realities of working in a real auditing firm. This part of the internship really helped me bridge the gap between my physical risk management background in the Navy and the practical side of digital compliance.

Over the last few weeks working my regular Tuesday and Thursday shifts, I got to see how the strict rules of NIST SP 800-171 actually play out when you are talking to real clients. One of the biggest things I learned is just how important people skills are in auditing. When I was taking the assessor course, grading a client's security plan felt like a purely technical exercise. But when you are actually sitting in the office and watching the team interact with defense contractors, you realize that soft skills matter just as much as

technical knowledge. A lot of contractors get completely overwhelmed by the strict rules of the CMMC Assessment Process. The assessment team has to act like both an evaluator and an educator. They have to explain exactly why a piece of evidence is not good enough without making the client feel attacked or compromising the audit.

The most challenging part of this final stretch actually had nothing to do with client evidence. It was dealing with the sudden changes to the CMMC program itself. Just a few weeks ago, we got a notice that the rollout of Phase Two of the CMMC rule was suspended for 60 days. In the federal compliance world, this is a massive deal. The delay sent a shockwave of uncertainty through the Defense Industrial Base, and at WTI, it immediately changed our daily pace. Contractors who were rushing to get in line for their assessments suddenly hit the brakes. Everyone is just waiting to see if the DoD is going to change any of the rules or timelines before they spend more money.

Being in the office when that suspension hit was a real eye opener about the growing pains of this program. We spent a few days breaking down the potential impacts with Koren and the senior assessors. The hardest part is trying to manage client expectations when we do not even have all the answers yet ourselves. We know the 110 basic security controls are not going anywhere, but the exact timing of how they will be certified is suddenly back in a gray area. Navigating that confusion with clients has been a real lesson in how to communicate risk.

The most exciting part of finishing these last few hours was realizing how much my understanding of cybersecurity has changed since May. Before this internship, I thought cybersecurity was mostly about offensive hacking and network defense. Now, I understand that the foundation of a secure defense network is built on strict compliance

and verifiable risk management. Getting to see the inner workings of an auditing firm like WTI gave me a huge appreciation for the governance side of the cyber industry.

Conclusion

Completing these 150 hours at WTI has been the most demanding but rewarding experience of my time at ODU so far. Getting through the CCP and CCA training requirements while also learning how a federal auditing firm actually operates gave me a massive head start for my transition out of the military. I now have the practical experience and the regulatory knowledge to confidently go after a career in CMMC compliance, even with the current delays in the program.