

David Seliquini

CYSE 368

Summer 2026

Professor Teresa Duvall

TA Jade Hines

Wise Technical Innovations LLC

Reflection #1

I just wrapped up the first 50 hours of my cybersecurity internship at Wise Technical Innovations (WTI). Instead of a normal, slow orientation where you just sit in a breakroom filling out HR paperwork, I was thrown right into the deep end. My supervisor, Koren M. Wise, had me sit through a 50-hour intensive training boot camp for the Certified CMMC Professional (CCP) certification. This was a great way to start because it knocked out my first two learning objectives from my MOA right away: understanding the CMMC ecosystem and finishing the required training hours so I can actually sit for the CCP test later on.

The main focus of the week was figuring out exactly how the Department of War tracks and enforces cybersecurity for its civilian contractors. We spent a lot of time digging into NIST SP 800-171, which is basically a master list of 110 security rules that DOW contractor companies have to follow. Since my background is in military operations and not standard corporate IT, learning how to actually grade a company's network was pretty challenging at first.

Honestly, the hardest and most discouraging part of these first 50 hours was just the sheer volume of information. There are so many acronyms, policies, and scoping rules to memorize. You have to know the rulebook inside and out to decide if a contractor actually meets the security criteria. When we did practice scenarios in class—like looking at a fake company's network diagram and trying to find the security holes—it felt a bit overwhelming. There is zero room for guessing. Thankfully, sitting down and breaking these scoping exercises out with Koren during my Thursday shift really helped it all make sense.

As the week went on, things really started to click. I realized that managing digital risk is basically the exact same concept as the procedural compliance I enforced in the military. For 14 years in the Navy Submarine Force and working as a Test Director at the Norfolk Naval Shipyard, physical safety and quality assurance were non-negotiable. We used strict boundaries and needed hard, objective proof that a system was safe before we moved forward.

At WTI, I am doing the exact same thing, just with computer networks instead of high-pressure pipes. Instead of checking a physical tag-out boundary on a submarine, I am learning how to check a company's digital boundary to make sure their Controlled Unclassified Information (CUI) is locked down securely. When I look at a System Security Plan (SSP) now, I am looking for the same type of hard evidence I used to look for on the deckplate. This was easily the most exciting part of the internship so far. It proves my fourth learning objective—that my veteran experience translates perfectly into civilian cyber auditing.

Now that the classroom training is out of the way, I am moving into my regular office schedule at the WTI headquarters on Tuesdays and Thursdays. For my next 50 hours, I will be focusing entirely on my third learning objective, which is getting hands-on experience with practical compliance auditing. I am looking forward to working with the rest of the team to look at real client evidence and figure out where their vulnerabilities are. Overall, these first 50 hours were intense, but they set a really solid foundation for the rest of the summer.