Final Reflection Paper

Elsie Gonzalez

CYSE 368 Cybersecurity Internship

WTI (Wise Technical Innovations)

Prepared for

Professor Duvall/Josh Russell

December 08, 2025

For my internship with WTI (Wise Technical Innovations), I had a very fulfilling and worthwhile experience. For Cybersecurity students, taking an internship is an important milestone that should be accomplished to get the best hands-on experience to be able to complement all the other training and experience. I decided to do an Internship at WTI because of my interest in governance and compliance. Additionally, I wanted to add my military background and contribute to WTI; ideally, I would like my training, my military experience to meld together and gain a collective skillset and be marketable to the Cybersecurity industry. With WTI, I hoped to learn how the CMMC (Cybersecurity Maturity Model Certification) ecosystem operates, acquire a certification, and continue to network during my internship and beyond.

At the beginning of my internship, I was able to meet with my supervisors and receive an explanation of what would be required and what CMMC would consist of and incorporate. With WTI, they serve as a C3PAO (Certified Third-Party Assessor Organization), conducting official assessments with DoD (Department of Defense) contractors to comply with cybersecurity standards in the protection of sensitive data. WTI also provides training on certifications like CCP (Certified CMMC Professional) and CCA (CMMC Certified Assessor), and I had the privilege of attending these trainings and learning from industry experts. WTI also builds enclaves with Azure, GCC, and GCCH, helping companies stay compliant to meet DoD contract requirements with controlled classified information. During my internship, I was able to see how a CMMC C3PAO organization provides consultation, advisement, and assessments. For my initial orientation, I was given details about what we would be specializing in NIST SP 800-171. There will be risk analysis involved, where you are able to learn how to navigate using tools like Microsoft Sentinel or Defender. There would be opportunities to create audits in reviewing client activity in the enclaves. Additionally, training opportunities and practice exams for the CCP certification would be afforded. WTI is an organization that I strived to be a part of, and I am glad that I was able to be a part of the team.

At WTI, as a small business organization, there were constant training opportunities. With management, I was fortunate enough to have two supervisors who trained us and showed us upcoming information for assessments or pertinent information to enhance my knowledge in the CMMC ecosystem. There is a lot of experience with supervisors with military background and computer science major. As mentioned before, there were plenty of opportunities for training and the owner of the company, Koren Wise, was able to give training to the interns and employees on how to use Microsoft Sentinel and Defender. We were able to see how we can run queries to focus on specific timeframes and look for any anomalies. We were able to write audit reports and see how an organization like WTI would initiate and promulgate these findings to companies that enlist their services. The internship experience and what we could contribute was effective where our different expertise produced different solutions to a problem. For example, our computer science major was able to contribute with his expertise when we had our resume review. He was able to give directions on what verbiage or position our internship experience can provide. Overall, this internship was able to provide the necessary training, support and expertise for an intern gaining experience in the CMMC realm.

With my work duties, I was able to learn how to use Microsoft Defender and Sentinel and perform auditing duties. If there was an issue with the organization, as an intern I was able to spot inconsistencies or abnormal queries where you would report and investigate the findings. One thing that was explained was that when performing these audits, you should possess a level of attention to detail and report all. Even if your findings were on supervisors, it is our duty to detail all findings and brief them for proper guidance on actions to take forward. Most of the queries involved simple explanations like an account being deactivated, or too many logins because of an account deactivation. But the essence of the audit is to report all findings and find proper solutions. A major component of our duties consisted of training for the CCP certification. Initially, like with any other new training, the terminology and the amount of information are foreign. Thankfully, our two supervisors had plenty of knowledge to be able to redirect us or give us advice on how to retain or study the information. Lastly, the duties and responsibilities at WTI were rewarding to learn and to be able to be part of a project that requires real-world experience.

With cyber major knowledge and background, our initial weeks at WTI consisted of training for the CCP. Not only did the training provide the necessary training, but it also required some Cybersecurity knowledge to be able to contribute to team scenarios. You had to know how network architecture works, and how safeguarding a network requires knowledge of the logical and physical sides. With the training, I was able to differentiate what devices fall into certain categories when it comes to the classification of the types of end system with the specified scenario. With on-the-job experience, I was able to apply the knowledge of knowing when enclaves, for example, are required for certain classifications, which led to the recommendation or requirement of the network setup and architecture. In doing scenarios where you apply your knowledge, it made me realize that studying and doing in-depth research is continual to be able to be proficient in your job.

The ODU courses of instruction have prepared me for this internship. The few courses of instruction that have helped immensely are the networking ones. As a cyber professional, you must have proficient knowledge of various components. What I have discovered is that many terminologies, like hashing, sniffer, or symmetric authentication, are necessary to know so you can understand how to safeguard a network architecture. Not only do you have to conduct assessments in the CMMC ecosystem but advising organizations on how to accurately conduct their setup to remain compliant is part of the required duties. There were many connections between the courses of instruction I took with the internship I attended. With this internship, you had to understand the concepts of cloud-based networks because of WTI's services or creation of cloud-based enclaves. I have had formal training with AWS and am learning about cloud architecture. During my internship, I was able to have more training, but having this prior knowledge made me understand what the instructor was talking about. The curriculum training aided in understanding my job and duties at WTI.

My internship fulfilled the objectives and learning outcomes that I explained in my introduction to this reflection. I was able to see how an organization operates with governance and compliance in the CMMC ecosystem. I was able to apply my military background, my formal training. The most motivating or exciting aspect of the internship is getting to network and learning from other professionals. Besides learning a new aspect of Cybersecurity, and training for the CCP certification, I was able to digest the knowledge of the staff members, the other trainees during instruction, and of course from Mrs. Wise. This internship has far exceeded my expectations, and I am glad I was able to be selected and have had the chance to collaborate with some smart cyber professionals.

When it comes to discouragement, this one is not an easy topic but the only one that comes to mind is not being able to be a part of assessments. Achieving the certification was one thing required, and unfortunately, that depended on our timeline of when we could be ready. In preparation for the course, I was able to learn more than I was expecting, and I am fortunate to have been exposed to many aspects of the CMMC environment. One of the most challenging aspects of this internship is learning and retaining knowledge for the CCP certification. There was plenty of information, training, and avenues to find additional resources. But like any other certification, it is a challenge to become prepared for an exam or certification like this one.

My recommendations for future internships would be to have clear expectations and management. I will say that, for my experience, the expectation and management were reasonable, and it is how I think other internships should be. There should be an initial meeting detailing what the intern is expected to do, what they hope to do, and timelines for any type of certifications that can be afforded. As far as intern preparation goes, the intern needs to free up their time to be able to meet the demands of possible learning or earning a new certification. While life can be demanding, an intern needs to be prepared to earn new skillsets and dedicate, even in their off time, to learning them.

In conclusion, my experience with WTI has made me learn about the governance and compliance side, enriched my understanding and knowledge as a cyber professional, and connected me with other professionals to continue to develop my expertise. Learning the process of the CMMC ecosystem, and how important safeguarding security or sensitive data is crucial to national security. Knowing that the requirements are stringent for a reason makes me thankful that programs and organizations like this exist. With my internship experience, I will be able to be more confident in applying for jobs, and I know that networking is a key component to being successful in the Cybersecurity industry. Additionally, I am thinking of pursuing a master’s program in the governance and compliance side. One of the questions asked was about the niche of Cybersecurity that I would like to pursue. The governance and compliance were an area that I have always had an interest in and continue to do so. I will most likely look for another internship opportunity in this area and further add to my professional resume. Lastly, I am most pleased and thankful to have been a part of WTI and hope to continue to contribute to other organizations that help others to secure assets as best as possible.