Reflection Paper 1

Elsie Gonzalez

CYSE 368 Cybersecurity Internship

WTI (Wise Technical Innovations)

Prepared for

Professor Duvall/Josh Russell

September 28, 2025

I have the pleasure of interning for WTI (Wise Technical Innovations) as a NIST SP 800-171 for Compliance. My Cybersecurity internship for this fall semester will include the CMMC (Cybersecurity Maturity Model Certification) program, where assessments are conducted for DoD (Department of Defense) contractors. This internship will provide an opportunity to learn about the governance and compliance side of the Defense Industrial Base Cybersecurity and take a career path in this sector. With my military background and experience, I hope to be able to contribute to quality work and achieve an important qualification in this Cybersecurity sector. I will be working with another Cybersecurity student under the guidance of a qualified assessor and the owner of WTI. I feel privileged to learn from the best in this industry and look forward to vital training.

I am interested in specializing in learning and expounding my knowledge on the governance and compliance side of Cybersecurity. In the military, I conducted many audits, enforced, and practiced compliance. Compliance is a tenet for most, if not all, organizations, and when it comes to the defense of our national assets and sensitive information. With WTI, services provided are as a C3PAO (CMMC Third-Party Assessor Organization) that assesses defense contractors in meeting the cybersecurity standards of the DoD, specifically with the NIST 800-171. This NIST delineates the required levels of control for CUI (controlled unclassified information or FCI (federal contract information).

During the initial meeting with the owner Koren Wise, she gave insight into what our internship training would consist of. The objective of the training is to learn and navigate through risk analysis and compliance. Some of our training will consist of building enclaves with Azure, GCC, and audit practices. There will be an opportunity to gain a certification called the CCP

(Certified CMMC Professional), showing knowledge of the CMMC framework and the ability to assess and evaluate the compliance of CMMC standards. This can create a pathway into other certifications like the CCA (CMMC Certified Assessor), which performs the actual audit for the defense contractor. The training will be extensive and worthwhile, as it will expose me to a sector that many Cybersecurity professionals pursue later in their careers.

During our week of training, I learned from Koren and other certified trainers who have done these assessments for many years. As stated before, these trainers have extensive experience with the CCMC assessment process. We were able to go over the ecosystem of the CMMC framework and how other organizations, collectively, contribute to the preparation/assessments/education/training of defense contractors that manage CUI/FCI for the DoD. This training was interactive with discussion questions and conducted scenarios with multiple groups. This training was very well put together; the engagement with the trainees helped with information retention. Quizzes and tests were also provided, aiding in retention and feedback. I was grateful to also hear from other industry professionals who are looking to qualify as an assessor. There was so much knowledge and information that will benefit me in my journey as a Cyber professional.

In conclusion, being a part of this professional organization during my internship will not only benefit my knowledge and practice, but I will also get to apply my own experience of handling CUI or sensitive information. It is important to safeguard our national assets to protect our safety and freedoms. Learning and applying CCMC concepts are part of the overall experience that I will gain from this internship.