Christopher Hossele

Reflection Paper 1 for USCG ALC Intern

June 7th, 2025

Old Dominion University

Professor Teresa Duvall

TA Ashley Robinson

CYSE 368

Internship Reflection Paper (First 50 Hours)

Having the opportunity to be a cybersecurity intern at the United States Coast Guard Aviation Logistics Center has so far helped me experience a realistic cybersecurity environment in such a short amount of time already. Within the first fifty hours of my internship timeline, I have already made significant steps in bettering my outlook for cybersecurity as a career by familiarizing myself with research and observation to better understand what to expect from a typical work environment here at USCG ALC.

Apart from my tasking as an intern, being familiar with concepts that I will have to know is key to fitting into a work environment well. I have researched key cybersecurity concepts such as STIGs (Security Technical Implementation Guide), CVEs (Common Vulnerability Exposures), and using ACAS scanning tools. At the Electronic Services Division here at ALC, policy frameworks are an extremely vital component to how they develop their cybersecurity protocols and being familiar with how to read and implement these frameworks is critical. Apart from my tasking here has been to overview frameworks such as NIST's RMF (Risk Management Framework). Within ALC, a huge portion of their cybersecurity infrastructure is based around vulnerability scanning and patching while also providing contingency plans for the networks. Being able to sit in on meetings observe what is being discussed has familiarized me with what typically happens here at ALC's cyber field.

More components of my tasking here at ALC involved sitting in on meetings and conferences. At first, I had absolutely no idea what was being discussed but slowly over the hours I have gained some sort of familiarity with the topics being discussed and I am sure to become even more familiar as time goes on here.

The discussion of obtaining certifications was also a part of my tasking here, realizing how crucial it is to have certifications when it comes to job seeking in the field of cybersecurity.

I have concluded from this that I will be pursuing a certification in CompTIA A+, Security+, and ISC2 cybersecurity certification as a start. Of course, over time I will gain more certifications in relation to my field of interest.

I have also sat in on training as well, such as Continuous Process Improvement training that helped me gain an idea of how business operations work here at ALC. Spending time in ALC's MSSL lab has helped me see further into what they do here, such as going through a STIG SCAP vulnerability scan to see how they patch vulnerabilities. I also observed how they operate mockups, which are control systems that are replicated just the same as the ones that are in the actual planes.

Having the opportunity to assess the physical security of a top-secret room is in the works for me for the upcoming weeks, but I was allowed to tour the room beforehand to get an idea of what to expect when that time comes. I will be going over the security parameters and deciding what routes to take to keep classified information properly secure. I find assessing physical security extremely interesting to me, especially with how thorough it is.

For the first section of my hours here as an intern I have already learned a huge amount of what to expect from a work environment like this and how I can apply it to my future fields of interest. Within the next few weeks, I will be branching from research and observation and will be doing more hands-on tasks.