USCG AVIATION LOGISTICS CENTER INTERNSHIP EXPERIENCE

Christopher Hossele

USCG Aviation Logistics Center

LCDR Stephen J. Schmid

CYSE 368/Internship Summer 2025

Old Dominion University

August 3rd, 2025

Table of Contents

Introduction to Internship Experience

My experience participating in an internship opportunity was crucial to developing a strong familiarity and skillset within a cybersecurity and information technology work environment, where I was able to observe and contribute to several different tasks as apart of my internship at United States Coast Guard Aviation Logistics Center. These tasks ranged from partaking in team meetings, performing physical security assessments, vulnerability patching, and academic research. Internships allow for a step away from the academic experience and instead a feel for a transition into the employment environment where interns can develop networking connections and potential ideas for determining future jobs of interest. Internships are one of the most important ways for gaining crucial experience while completing an academic degree preceding heading into the workforce, and specifically, an internship in the field of cybersecurity focuses on a rapidly advancing field where hands-on experience is priceless to garnering fundamental knowledge compared to academia where it can potentially become stale after some time. Although with the idea of how crucial cybersecurity internships are, finding an internship position can be quite difficult. When it came to my own experience obtaining one, I surely struggled with my options until I finally landed an opportunity at the United States Coast Guard Aviation Logistics center in Elizabeth City, North Carolina.

To understand how my internship experience tasks were fulfilled and how my overall experience is relevant, it is important to understand a brief history of the organization Aviation Logistics Center. The Aviation Logistics center is located at the United States Coast Guard Base and is a company driven by aviation maintenance, engineering, information services, and logistics who are motivated by their motto “We keep ‘em flying”. ALC’s large customer base is primarily military and coast guard mission operations, deeming the company’s objectives as very crucial to the armed forces as a priority company for them. A significant part of ALC’s tasking is information systems which is a significant part of aviation as a whole in order to keep aircraft running efficiently with communication. ALC was opened in 1947 under a different name until 2008 when it was reestablished to its current name. Overall, Aviation Logistics Center is a particularly well-known organization that supports around 26 of the United States Coast Guard’s aviation air stations within the United States. The journey to officially landing a position as the only intern at ALC was quite difficult and took significant steps.

Initially, starting my search of finding an internship position for myself involved applying to many different places and reaching out to several resources, and without much luck to my favor I never heard back from any employers regarding the next steps. At the time I tried to have the mindset of wanting to take the steps to do everything on my own foot and not utilize assistance in finding one, but after a while my father decided to step in and network for me since he works at the Aviation Logistics Center where there were potential cybersecurity related internship opportunities. When I learned of the opportunities that were offered at ALC as far as a cybersecurity intern, I immediately began the process of reaching out and sending in my resume to see if I would be a fit. Interning at the United States Coast Guard sounded like an amazing opportunity to gain experience as an intern due to the governmental environment which surrounds most cybersecurity jobs, and USCG ALC’s mission as a military organization and their ties to aviation which has always peaked my interest. The reasons although are endless as to how beneficial interning at USCG ALC is overall and surely gives quality opportunity experience with the level of work and importance. I made my overall decision to intern at USCG ALC

Along with the importance of obtaining an internship in cybersecurity at ALC is to identify three key objectives in which I expected to takeaway from my experience. These learning objectives include “Practice multiple aspects of cybersecurity to include physical security and vulnerability mitigation and remediation”, “Develop policies for a system at ALC to include access control, auditing, and awareness and training, among others”, and “Gain experience with systems based on Linux OS”. These learning objectives are important to divert the outcome of my experience and setting myself up for confidence in what I feel most interested in for cybersecurity work. Overall, I feel like these objectives were significantly met through my time at USCG ALC and I was even exposed to different aspects that I felt were as big as my existing objectives. Such tasks included diving into physical security projects and vulnerability mitigation configuration. At the start of this internship, I hoped that the objectives I set for myself would have helped me explore different types of career paths in cybersecurity, helping to branch off to see what kind of work I would want to be doing when it comes time to officially start job searching. I also expected to gain fruitful experience that would help employers differentiate me apart from other candidates as well with the tasks I did to fulfill my objectives during my internship. Having these expectations guided me to enter this internship with an open mind and positive outlook for what I would potentially be gaining from my time here.

During the first couple weeks at the start of the internship, I was allowed the opportunity to familiarize myself with both the base and Aviation Logistics Center itself. ALC is composed of many different buildings that support many different tasks, such as aircraft mechanics, network management, and coast guard security and support laboratories that altogether support the Coast Guards missions.

As part of my orientation and familiarization, I sat in on a few meetings with the team that I would be working with for the duration of the internship experience, coordinating with the LCDR and the team of cybersecurity professionals on different tasks throughout the several weeks there. The meetings that were held revolved around getting to know my colleagues and also introducing myself to the company as well. Overall, everyone was super friendly from the start and continued to be for the entirety of the internship, learning that they all wanted me to succeed to the best of my ability. I was also brought on a tour of the base where I was shown the multiple different buildings for ALC operations along with the top-secret classified workspace building that I would be spending majority of my time in doing physical security assessments for the company. My schedule for the internship was also notably flexible which I enjoyed, bulking my hours in the beginning of the internship so there was no need to scramble for hours towards the end. If I ever needed to take a day off for important proceedings it was no issue as well, considering I have had a relatively busy summer on top of the internship. One notable characteristic about ALC that is quite fascinating is how close proximity the organization is to the Pasquotank River, where I would sometimes step outside and stand by the water when it was nice out. I immediately found myself to be settling in quicker than I expected to, having my own assigned desk space and time to sit down and research the sole components of the Coast Guard and ALC’s mission. Another part of my familiarity was visiting the laboratory and information services division building. The laboratory is a significant source for vulnerability testing and mitigation, communication center for the aviation control tower and aircraft, and network configuration. During my internship I visited this place a few times to participate in STIG configurations or SCAP scans among other tasks.

As far as any training had went, simple research tasks were assigned to me to familiarize myself with certain topics that are frequently directed as daily business operations, such as studying the risk management framework. I was also allowed the opportunity to participate in Continuous Processing Improvement (CPI) training where I was rewarded a certification for my completion in the training. Since the Aviation Logistics Center is a huge product service, Continuous Process Improvement training is crucial to ensuring that the workflow is performed with the most efficient methods. Overall, there wasn't much to necessarily be trained on due to my internship experience being notably research oriented to familiarize myself with my tasking.

My initial impressions of the internship were relatively positive while slightly intimidated by the work flow that felt so real to me. Being in an actual cybersecurity employment environment for the first time ever was definitely a lot to take in at first but it immediately didn't seem too intimidating after a while.

Management Environment

The overall management of USCG Aviation Logistics Center wasn't too clear to me as there were so many different departments within so many different buildings. I did notice that there is a significant amount of collaborative efforts between the different departments, such as the information service division, electronic services division, and laboratory among others. Ideas and plans were always discussed during meetings, many of which I had sat in on. For the most part, it seems that mostly everyone had their own team and would provide their efforts to the commanders. For example, my team consisted of cybersecurity analysts or a rotary technician who would answer to the lieutenant commander of the department, who was also my internship coordinator. He had served in the United States Coast guard for several years before pursuing a master's degree in cybersecurity at Old Dominion University, which I found to be pretty interesting. He was always very knowledgeable about subjects and often gave me helpful advice on my tasking and personal goals towards my relationship with cybersecurity as a career. I noticed that most of the time, meetings would be held with the different teams within the building I stayed in, most likely building an agenda and discussing findings and predicaments.

There would often be other meetings that would take place to discuss collaborative efforts and plans with the higher-ups who were most likely from the different buildings such as the laboratory, ISD, or ESD. Since the Aviation Logistics Center is ran under the United States Coast Guard, there is of course collaboration between members of the armed forces who would guide the operations that took place within ALC as well. I never really saw much supervision there within the cubicle area where I sat most of the time, but overall everyone seemed to be extremely focused on getting their daily operations and tasks done.

When it came to the management environment in regards to my internship experience. Every morning I would always immediately head to my internship coordinators office where we would do recaps of things that I learned days prior and discuss the many things that I now know. After that I would be assigned tasks to complete for the week and allowed the opportunity to ask questions to my fellow colleagues from my team. Typically once I would complete a task, which ranged anywhere from researching topics in cybersecurity, physical security assessments, or participating in duties at the lab we would discuss how I felt about my work and decided if I would continue to go down that route for experience purposes. Although, most of the time I

would be let off to complete my tasking on my own, only periodically stopping in for questions or clarification. I noticed I never really had any issues with my ability to complete tasks on my own and I enjoyed the independence I had quite often. The offices were always very quiet and allowed me to focus most of the time until I had the urge to put on some music. Never any conflict arose in the workplace and I noticed that there was always a significant amount of communication that would ensue, excluding outside sources where there was minimal conflict. Issues were always resolved in meetings that I would typically sit in on, where presentations were given to bring the teams back on track to avoid any confusion or error.

My internship coordinator, Mr. Schmid was always extremely encouraging when it came to wanting to branch out into trying different things during my internship. He always reminded me that if I am feeling “comfortable” within a workplace or opportunity then I am not progressing, because discomfort brings progress. I found this to be extremely helpful advice which helped me decide on wanting to perform tasks such as physical security assessments by myself and even considering jumping on obtaining my first cybersecurity certification as soon as possible. I was always nervous about the idea of having to tackle huge important projects by myself during the internship, but I had to understand that it would be a great learning opportunity for me and I eventually did not hesitate as much. If my internship was a couple months longer I would have been able to partake in a drone project as well. Overall, when it came to the management environment for my internship experience I never seemed to have a problem with building a weekly agenda or having my questions answered.

Work Duties, Assignments, and Projects

During my internship timeline, I had many tasks and projects that ranged from taking a couple days to a couple weeks to complete. My tasking included; researching topics in cybersecurity such as classified information levels, risk management framework. certifications, CVE’s, ACAS, SCAP, STIGs, roles of cybersecurity jobs, partaking in physical security assessments of top-secret spaces, participating in lab activities such as vulnerability patching and system scanning, and sitting on multiple team meetings where we would discuss different topics of company operations and even discussing security efforts and errors. A lot of these tasks that I completed were unheard of to me, finding that I learned a great amount of new things compared to my academic studies.

When it came to my researching tasks. Most of the things that I was advised to learn about were crucial to the company’s operations. Topics such as classified information levels and cybersecurity roles were important because of the level of sensitivity that takes place when it comes to information handling within the company. There is a significant amount of company secrets and government information that I was not even allowed to know during my internship, but I completely understood that.

Researching topics such as Security Content Automation Protocol scans (SCAP), Security Technical Implementation Guides (STIG), and Assured Compliance Assessment Solution (ACAS) scans were important to know as they are crucial for typical business operations. Participating in the lab for a few days showed me how these topics are used very frequently. I learned from this that researching topics beforehand before entering into something is important to starting on the right track.

One of the most fruitful tasking I completed here at Aviation Logistics Center is participating in physical security assessments for top secret rooms. These room assessments were guided by a checklist and my own judgement for compliance. I noted whether specific characteristics of the room's security measures complied with the checklist or not, and noted my findings into a final report which was actually used as an official document for the company. These compliance categories ranged from the structure of the doors to the structure of the inner ceilings and vents. It was a very tedious process overall but with a small amount of guidance and collaboration with the security officer at ALC it was no issue for me to succeed in these project reports. Performing these assessments and finalizing reports took a couple weeks at a time to complete, having to go back and forth between my desk and the security room to make thorough assessments and even fix some mistakes that I overlooked from previous times. Having the opportunity to complete these assessments is crucial for the organization to house top-secret information in the future when it is all said and done.

I also sat in on several team meetings where important information was shared between the different departments in ALC. Many of the team meetings consisted of training measures and recapping of past days discoveries and contingency planning. During one of these meetings, I was given the opportunity to present my reports to a large team regarding my security assessments from the two classified spaces. Having these team meetings are important to the organization by providing information and collaboration.

Some other small tasks I completed involved participating in continuous process improvement (CPI) training which rewarded me a certification along with taking a couple tours of the different parts of ALC. Overall these tasks throughout my internship helped me learn a significant amount while also contributing greatly to the organization as well.

Cybersecurity Skills and Knowledge

When it came to utilizing my cybersecurity skills for the duration of my internship, I feel it is important to differentiate between what I already knew and what I have learned after. Before starting my internship experience, I knew a pretty decent baseline of topics regarding cybersecurity policies, hardware development, and minimal physical security measures. I even knew some parts of the risk management framework, many NIST policies, CIA Triad, Linux fundamentals, and very baseline cybersecurity fundamentals. These skills I acquired during my two years of college at Old Dominion University, where I excelled mostly on quite a few of these topics.

When it comes to the skills I had developed during my internship, it came to me by surprise as to what I would be learning and participating in. One of these skills I feel like I developed well is the ability to perform physical security assessments. When it comes to cybersecurity, being able to physically store sensitive compartmentalized information such as laptops, hard drives, files, pin cards, etc. is extremely important in cybersecurity. Also having facilities that harbor operations that require authorized personnel in secured rooms is also extremely important to cybersecurity as well. Human behavior is one of the biggest threats to cybersecurity, and being able to fortify a space to protect these systems is crucial to good cybersecurity methodology. Being able to participate in assessing a top-secret space has given me the ability to spot physical security vulnerabilities, determine the best course of action for

implementing IDS systems, and ensuring proper authentication protocols for key cards and digital pin locks has given me a confident knowledge in physical cybersecurity so far. Of course, it will take much more time to perfect this skill, but my internship has given me a good head start.

Another skill I developed during my internship is configuring STIGs. STIGs are Security Technical Implementation Guides and serve as a tutorial or standard for configuration a system to prevent vulnerabilities. Before entering my internship, I had no idea something like this even existed. Being able to participate in configuring systems using STIGs, I have learned how organizations can prevent vulnerabilities in systems by altering settings that divert adversaries from gaining access.

I also learned more about the risk management framework (RMF) and how it can be applied policy-wise to an organization's systems to keep them secure as well with more reading and research. I have also learned smaller topics as well such as the different levels of classification, becoming more familiar with the differences and how they are important when determining what information falls into these categories. These skills are important to ALC's operational objectives as it is important to keeping systems short of vulnerabilities and to keep their physical assets protected as well. Overall, I feel that physical cybersecurity protection and vulnerability patching are the two biggest skills I have learned within my internship experience.

ODU Curriculum Preparation

I believe that Old Dominion University's curriculum prepared me for a portion of what I endured during my internship experience. It gave me a fundamental understanding of what to expect in the workplace and an idea of how many commercial cybersecurity organizations are. It has prepared me with knowledgeable insight regarding topics of hardware, software, and programming fundamentals while giving me views of how policies impact how these topics are intertwined together to protect sensitive information. I was able to tie a large amount of information from my classes such as CYSE 201s, Social Science Concepts of Cybersecurity, IT 417 Management of Information Security, CYSE 200t, CYSE 425 Cyber Strategy and Policy, and CYSE 406 Cyber Law. All of these classes had subjects that I derived into the things I participated in within my internship experience. When it came to a large portion of the federal side of cybersecurity, I feel like there was a grey area when it came to preparation, but this is most likely due to many topics being classified so teaching it publicly is unlikely. Fortunately, I have determined that I will be seeking certifications in CompTIA A+, Security+, and Network+ to broaden my knowledge and to keep myself current on the ever-changing curriculum of cybersecurity.

Objective Fulfilling

Fulfilling my objectives is determined by the tasks I participated in during my internship. My objectives during the internship were previously identified as "Practice multiple aspects of cybersecurity to include physical security and vulnerability mitigation and remediation", "Develop policies for a system at ALC to include access control, auditing, and awareness and

training, among others", and "Gain experience with systems based on Linux OS". These objectives were very broad when considering how they could be fulfilled as I came into this internship with an open mind and flexible expectations. When it came to fulfilling my first objective, "Practice multiple aspects of cybersecurity to include physical security and vulnerability mitigation and remediation", I can say that I fulfilled this objective in a few ways. One of the biggest ways this objective was fulfilled was my time spent in the laboratory at ALC.

In this lab, I spent many days participating in STIG configurations, ACAS scans, and SCAP scans, which are all examples of vulnerability mitigation and remediation techniques. When it came to my participation in physical security assessments, this fulfilled my first two objectives, including "Develop policies for a system at ALC to include access control, auditing, and awareness and training, among others" by providing policies in the form of a report for the security team here at ALC. This is a form of physical security as mentioned in the first objective as it is also a form of policy development. My reports consisted of a guideline for the security team to use when making decisions to further secure their classified rooms using information derived from a checklist.

When it came to fulfilling my third objective using Linux systems, I did not do too much with Linux systems but was given a rundown of some commands and how Linux command prompts contribute to ALC's performance as well. Although, I participated in many things that I found to be far more interesting than Linux systems to me.

Motivating Characteristics

Having motivational characteristics when it came to my internship allowed me to feel excited about heading to base every morning. One of the biggest motivational factors for me was knowing I would be learning something new every time I would head in, such as sitting in meetings to discuss new topics or being assigned new tasking of topics I had never heard of. At the time, being informed about my projects in assessing physical security parameters was extremely motivating to me as well as finding the topic of physical cybersecurity extremely interesting to me. Another factor that was very motivating to me was the environment of the workplace. I felt welcomed there from the start regardless of being the only intern and I didn't feel out of place. It is inviting when the people within a workplace like someone. I was also reminded several times that everyone there wanted me to succeed throughout the entirety of my internship, which I found to be extremely motivating as well. Overall, I always felt motivated to complete and excel in my tasking, regardless of small things that limited my ability to participate in some opportunities.

Discouraging Characteristics

When it came to discouraging characteristics of my internship experience, I can't really say I had a huge number of things that discouraged me. The only thing that majorly made me feel limited in my experience was my inability to have access to the local network for the company. Relying on using a hotspot every day was rather difficult as the service in the area was not very good at all. Sometimes I spent fifteen minutes waiting for a website to load on my laptop, but I

was always motivated to get the website to load for me anyways. I understand the circumstances as to why I was unable to utilize the network as I was not an employee or did not have a clearance to do so. Although with the limiting factor here, it did not stop me from implementing the rest of my tasks that were assigned to me.

Another small discouraging factor that stuck out to me was the commute to and from, as it was over 40 minutes of driving there and over 40 minutes of driving back home. Of course, the commute time is obviously worth the experience that I would be gaining from this anyways, so it didn't matter too much to me. Overall, the discouraging factors were very minimal and insignificant compared to the motivational factors of my internship experience.

Challenging Characteristics

Challenging characteristics, to me only involved the lack of education and experience I had when entered into this internship. I have never been inside an actual work environment for cybersecurity, nor have I really had any education regarding most of what is discussed and performed at ALC. This made it a little difficult when it came to being able to contribute to meetings and discussions, but with my team being very understanding, I was always walked through certain topics and given a better understanding of anything I had felt challenged over. Of course, not having an efficient Wi-Fi network to utilize was both discouraging and challenging to me, but it didn't stop me from getting the information I needed to perform my research tasks.

Recommendations for Future Interns

For future interns, I would recommend brushing up on certain topics in cybersecurity that are relevant to the company to build a better understanding of what to expect. I came into my internship at ALC not really knowing what to expect since I did minimal research beforehand, and I find it very important to have some sort of familiarity. Another recommendation I would ensure for future interns is to do outside reading and research outside of intern hours and when not at the internship facility. This is crucial to me when it came to learning about what was performed and discussed the day prior and helped when it came to the next day's tasking. I also recommend dressing in a professional manner. I came into the first day a little overdressed and a bit too formal but was applauded for my effort in trying to look presentable at a new place.

Conclusion

In conclusion, I feel that this internship was an extremely successful opportunity, not only in gaining experience and knowledge but also in motivating me to keep working towards pursuing a career in cybersecurity. This internship helped me fulfill my objectives and even learn new ones, exposed me to topics I have never heard of or thought to ever experience, and gave me a sense of reality outside of the academic environment. I genuinely feel that internships are a crucial part in gaining both experience and motivation to decide whether or not a career path is right for you. Finishing this internship in my very last semester at Old Dominion University has

shown me how much worth pursuing this field in cybersecurity was and how important participating in an internship opportunity is.