CYSE368 Cybersecurity Internship Final Paper – Patrick Bays @ ANVIL Systems Group

Student name: Patrick Bays

Employer: ANVIL Systems Group, Inc.

Instructor Name: Professor Teresa Duvall (TA Joshua Russel)

Class Name and Term: CYSE 368/Spring 2026

Table of Contents

1. Introduction

My motivation for joining ANVIL Systems Group was based mainly around my previous internship experience with the company. In Summer 2019, I interned there for a period of 6 months as a Computer Science intern. During that time, I gained an understanding of what it would be like to work as an employee of ANVIL Systems Group, and got acquainted with the company's CEO, VP, and COO. I also got to work extensively with the computer scientists and mechanical engineers on staff there at the time, and learned about the projects they were working on. Every bit of information that I learned during that time intrigued me, so much so that I decided to work for them circa 2023. Since then, I have been working there as a Network Engineer and loved every second of it. Although next to nobody from my internship days 4 years prior worked there anymore, the environment was still tight-knit and as agile as ever. It really excited me for what came next.

The ANVIL I've come to know and love is a specialized organization with approximately 26 employees, focusing on providing critical RF (Reference Frequency) solutions to sites around the globe. My role is to provide critical network and field engineering services, particularly for environments requiring high levels of security and compliance. The company serves a niche demographic that includes the Department of Defense (DoD) and other companies contracted by the federal government of the United States. A primary focus of our operations is maintaining rigorous security standards such as CMMC Level 2 to ensure the integrity of mission-critical communications.

Learning Objectives: During this time, I aimed to achieve the following specific objectives:

1. Learn how to incorporate my existing network knowledge into a fast-paced, small company environment.
2. Learn how the CMMC accreditation process works, and what must be overcome to achieve it.
3. Gain experience with Virtual Machine software like Proxmox and VMware ESXi, as well as NAS software in Synology.
4. Learn about hardening systems for government use in secure environments.

2. Management Environment

The management structure at ANVIL Systems Group is characteristic of a small company. With

only 26 employees, the hierarchy is relatively flat, which creates an environment of raw communication. Unlike larger corporations burdened by heavy red tape or multi-layered approval processes for every task, our team operates with extreme cohesion. This means that, regardless of team (Mechanical, Electrical, Software, QA, Network, etc.), there is a camaraderie there that allows us to simply walk into each others offices if a question needs to be answered or if there is a problem to be solved.

Supervision at ANVIL is direct and task-oriented. Upper management generally trusts the engineering teams to have the ability to take initiative and pioneer themselves, which is **great.** It allows our smaller teams to have their own mini-hierarchies, and shows that our C-Suite is confident in our abilities and direction. Furthermore, this creates a kind of “lock-step” approach when crises arise, like hardware failures or emergency communications needs. The team can work regardless of external force to pivot immediately towards what demands attention without any bureaucratic delay. This effectiveness is by far the most valuable thing when it comes to operating in high-pressure, time-sensitive, high-security environments.

3. Major Work Duties, Assignments, and Projects

My role as a network engineer involved several critical projects that are foundational to the company’s operational security and continuity.

The first project I worked on during this time frame was Blue Team Remediation and STIG Compliance. One of my primary responsibilities was executing remediation steps following a blue team investigation conducted by a DoD contractor. This involved using Ansible scripts with DISA STIG roles to alter system files and configurations across multiple sites. This task is vital to the business as it minimizes the attack surface, closing ports and patching services that could be exploited by malicious actors. An unfortunate but not unexpected part of this process was debugging some issues that arose when executing those Ansible scripts. A lot of the machines that we’re running the STIG on were put into these environments long before any of us worked at ANVIL, so it was kind of a toss-up on whether a machine would accept or reject some select rules.

Post-STIG, I had to use Tenable Security Center to verify that the STIG took properly. Because of the fact that some of these rules didn’t stick on older hardware, there were a lot of vulnerabilities that were kicked back by the scanner. I had to SSH into each machine and individually check each finding to either mark it as a false positive, or fix the issue and then re-run the scan. This was grueling work, but it’s all in service of the mission. During this whole process, I was also assigned a POA&M (Plan of Action and Milestones) to disable zone drifting on a few hosts that still had it on – this was a finding from our Blue Team investigation.

A spur-of-the-moment project I worked on was recovering a failed Synology NAS and creating a backup source for data redundancy. Following a significant failure of our primary Synology NFS share (the host for all project documentation, 3d models for our mechanical design, and Altium files for our electrical design), my coworker and I worked to diagnose the hardware failure and implement a temporary backup solution using a non-compliant Synology DiskStation. This was essential to prevent data loss and maintain business continuity during the period we were awaiting replacement hardware. We had no choice but to keep the unit that failed as the production unit, as we had no other devices on hand that could use Full Volume Encryption (FVE) as mandated by CMMC Level 2 controls.

The third project I worked on was an emergency communications deployment. In response to equipment damage at a remote site, I was tasked by our CEO with preparing emergency communications boxes. These units contained LTE modems, SATCOM modems, and Layer 3 switches designed to route traffic in the event of traditional signal loss. This project required intensive testing of salvaged and previously "yellow-tagged" equipment to ensure failover reliability. It also provided insight into the previous way of doing things in regards to these comms boxes – whenever a device failed in one of them, it would just be yellow-tagged and shoved on a shelf in the warehouse. Because of this “eject and replace” mentality (mainly due to time constraints), a lot of those tagged modems and switches were actually perfectly fine – they just needed a bit of TLC and a firmware update or two. While the other two members of my team checked out each comms box and conducted failover tests, I took the time to check if each of these devices was actually broken or not. In the end, we ended up with only two of our 9 modems being un-salvageable, so it was a worthwhile effort. Those boxes are now fully tested and awaiting shipping if they’re needed.

The Fourth project I worked on throughout my time with ANVIL was an Infrastructure Refresh (VMware to Proxmox Transition). To prepare for an upcoming CMMC Level 2 audit, I participated in replacing End-of-Life (EOL) VMware ESXi hosts with a new Proxmox cluster utilizing HPE ProLiant DL325 Gen11 servers. This project also involved transitioning from older Fortinet hardware to newer Cisco hardware, applying existing VLAN configurations and controls to the new architecture. This was necessary to ensure our hypervisor solution met modern compliance and stability standards.

4. Use of Cybersecurity Skills and Knowledge

This work served as a bridge between theoretical classroom knowledge and previous knowledge from prior roles into practical, high-stakes applications. Prior to this role, I possessed foundational knowledge in networking, including experience with Fortinet appliances, VMware, and Nutanix environments. I also had a baseline understanding of Ansible for automation and the principles of Defense-in-Depth.

On-the-job, I learned several important things as the work required me to rapidly acquire expertise in a plethora of new areas. I learned the intricacies of DISA STIGs and using Tenable Security Center for credentialed vulnerability scanning, I gained hands-on experience with Proxmox clustering to enhance my experience with using hypervisor software, I gained an understanding of various firewall operating systems like Cisco FXOS and Juniper JunOS, and I increased my understanding of the specific technical requirements that government certifications such as CMMC Level 2 involve.

Change in Understanding: The most profound change in my understanding was moving from a "theoretical" view of security to a "resilience" view. In class, we discuss the importance of Defense-in-Depth, but actually seeing a system go offline and realizing that "there are no lines of defense" without proper backups changed my perspective on risk management. I learned firsthand that security is about ensuring that the system can recover when hardware inevitably fails. Actually playing a part in that diagnosis and remediation process is what changed my understanding the most.

5. ODU Curriculum Preparation

The ODU Cybersecurity curriculum provided a vital foundation, though the work revealed gaps between academic theory and the realities of the job.

My Software Engineering course was directly applicable when debugging Ansible scripts and managing automation tasks. Furthermore, my Digital Forensics course provided the necessary mindset for understanding the implications of the blue team's investigations and the importance of audit trails. The concept of "Defense-in-Depth" learned in class was reinforced daily as I applied STIGs to reduce attack surfaces, and implemented CMMC controls to hopefully pass our future audit.

My time at ANVIL Systems Group revealed several practical complexities not fully covered in a classroom setting. The chief of these is the actual physical challenges that come with field engineering (i.e. managing hardware failures, and even flying out to sites in order to diagnose issues that laymen on the ground can’t access). Last year, I flew out to a couple remote sites to install some systems there, and going through those experiences provided me a ton of insight into how my role, especially at a small company where everyone wears a lot of hats, means that I can be sent overseas to perform any number of things. Unfortunately due to my clearance, those operations are not something I can put in text to submit.

Another thing that ODU’s curriculum didn’t adequately prepare me for was the logistical difficulty of maintaining connectivity in regions outside of the US, specifically when using SATCOM and LTE. This isn’t something I expected ODU to cover, as SIGINT (Signals Intelligence) is not covered in most cybersecurity programs, but it was still a challenge to learn about all of that stuff on the fly. On a different note, ODU did help me prepare for this role in terms of time management. I

cannot describe the intensity of time management required to both balance high-level technical tasks with my academic workloads, especially when I can be on a 6-10 hour time difference from the college itself.

6. Fulfillment of MOA Outcomes

I feel like my first MOA outcome, incorporating my existing network knowledge into a small company environment, was fulfilled. Through both the emergency comms box project and the Synology failure, I learned to work within a highly cohesive, three-man team where communication is direct and immediate. I had ample opportunities during troubleshooting of these devices to flex my proverbial network muscles, and my approach to diagnosis often provided differing but valuable insight when the rest of my team was stuck in a certain way of thinking.

My second outcome, to learn CMMC accreditation processes and challenges, was also fulfilled. The Synology failure highlighted the difficulty of maintaining compliance (FVE requirements) during hardware transitions. There were also a lot of other miscellaneous CMMC tasks that our team had to work on that didn't end up making it into my reflection papers. The company we were partnered with to assist in our CMMC journey, Summit7, began not holding up their end of the bargain, so we had to swap partners in the middle of satisfying POA&Ms. It gave me a lot of insight into how organizations work with these companies to achieve their certifications, and being a part of that process helped me gain a deeper understanding of what all goes on under the hood.

My third outcome, to gain experience with Proxmox, VMWare ESXi, and Synology NAS was fulfilled. The process of decommissioning the EOL VMWare host and the implementation of the HPE/Proxmox cluster provided direct, hands-on experience with these technologies. Given that my only prior experience was with Nutanix and self-hosting VMs using VirtualBox and other, free, consumer-grade softwares, it was great to finally get some experience with enterprise-level hypervisor solutions.

My fourth and final outcome, to learn about hardening systems for government use was absolutely fulfilled. My work with DISA STIGs, Tenable scanning, and the remediation of the resulting findings directly addressed this goal. By debugging those scripts and peering into what actually makes a hardened system for the United States government, it moved my understanding of defense-in-depth from a theoretical view to one that I have to work with on a daily basis.

7. Most Motivating or Exciting Aspects

The biggest motivator during my time at ANVIL has been the tangible sense of purpose derived

from our mission-critical work. Unlike a lot of academic or entry-level IT roles that feel somewhat removed from real-world consequences, the tasks I performed had direct implications for national and operational security in high-risk environments. Being tasked with preparing emergency comms boxes, knowing that these LTE/SATCOM units might be the only lifeline for remote sites during conflict, provided a level of gravity that is incredibly motivating. I feel a little silly saying this, but there's actually a bit of an adrenaline rush in knowing that the reliability of the network I configured could impact the safety and communication capabilities of personnel operating in volatile regions.

I also found immense satisfaction in the high-stakes problem-solving that a small company environment demands. In a larger corporation, a hardware failure like the Synology outage might be treated as a routine ticket, but at ANVIL, it was a sudden, all-hands event that required immediate diagnosis and decisive action. The autonomy I was granted to take initiative, like identifying the need for a backup system and then configuring said backup system, was very empowering. The work involved in troubleshooting network issues and debugging complex Ansible scrips provided a continuous stream of intellectual stimulation that kept me engaged the whole time.

Lastly, the level of professional cohesion and the lack of bureaucratic restrictions were major highlights of my experience. I found it incredibly motivating to work in an environment where communication is pure and raw rather than buried under layers of corporate formalities and red tape. The ability to collaborate directly with members of the other engineering teams created a dynamic that made even the most grueling all-nighter feel like a shared victory.

8. Most Discouraging Aspects

By far the most discouraging aspect of this job has been the psychological weight associated with holding a TS/SCI clearance. While being granted access to higher-value networks is a significant professional milestone (in my opinion), and that carries a motivational aspect to it, it also carries an inherent sense of responsibility that's incredibly taxing. There is a deep sense of isolation that stems from the inability to speak candidly about my work without having to think about ways to generalize it such that I don't expose information that can be detrimental to national security. Although I can share general accomplishments like in-house diagnosis and repair of systems and comms box creation, it has to go through a bunch of internal filters before I can even dream of writing it down or speaking it out loud. When major projects are completed, I can't celebrate those wins in any of my social circles because the work must remain confidential. This creates a disconnect between my professional identity and my personal life. I often find myself unable to explain sources of stress or reasons for sudden absences during critical incidents, which can lead to a feeling of being siloed from my own support systems. The most harrowing aspect of it all is that I cannot tell another soul on the outside about the scope of my work for the rest of my entire life.

9. Most Challenging Aspects

The greatest challenge was undoubtedly managing the intense demand of my academic workload alongside high-staked engineering responsibilities. The nature of network engineering is often unpredictable, as seen during the Synology failure. “Drop everything” moments are common and require immediate, focused attention. This created a significant logistical challenge when these professional emergencies collided with the responsibilities of my five ODU courses. The challenge wasn’t just the loss of study time, but the pure exhaustion that was caused by the rapid switching between modes of mentality. Transitioning from preparing for a DoD-level audit to deep-diving into software development or forensic analysis was tough to do multiple times a day, and maintaining my performance in both domains while navigating these frequent disruptions required an extreme level of discipline.

10. Recommendations for Future Interns

I recommend that incoming interns prioritize building a foundational level of technical expertise before applying. While much of the hands-on training occurs on the job, having a baseline familiarity with our specific technology stack, especially JunOS, FXOS, and Hypervisor software, will significantly reduce the initial learning curve. Additionally, gaining even a rudimentary understanding of Ansible and Python is highly beneficial, as much of our remediation and configuration work relies on scripting to maintain compliance with DoD standards.

Beyond the technical aspects, it is vital for new interns to prepare for the unique volatility that is inherent to small-scale engineering firms. Unlike larger corporations with rigid scheduling, ANVIL operates in an environment where “drop everything” moments are common due to hardware failures or field emergencies. Interns should foster a high degree of mental agility and be prepared to instantly pivot from routine tasks in the event of an emergency. You must be comfortable with the idea that your primary focus may shift by the hour and without warning to address critical infrastructure needs.

11. Conclusion

Reflecting on this experience, my primary takeaway is the distinction between theoretical security and operational security. Before joining ANVIL I viewed cybersecurity through an academic lens, but witnessing the real-world impact of hardware failure and the sudden loss of critical infrastructure has shifted my perspective. I have learned that while hardening systems and managing vulnerabilities is essential, the true foundation of a mission-critical environment is redundancy and

prepared recovery. The ability to maintain continuity of operations when the primary line of defense fails is what separates a functional network from a vulnerable one.

The work has also fundamentally changed how I will approach my remaining time at ODU. The gap I identified between classroom theory and the reality of the profession has provided me with a new sense of purpose in my coursework. When studying Software Engineering and Operating Systems, I no longer see coding and comprehensive understanding as just an academic requirement, but an opportunity to implement those lessons learned in my career as well. When studying Digital Forensics, I don't see it as a postmortem exercise, but as a vital component of the continuous auditing process required for CMMC compliance. The intensity of balancing five rigorous courses with the agila nature of my role has also forced me to master a level of discipline and time management that will serve me well through my final semesters.

Looking toward my professional future, this experience solidified my commitment to the field of network engineering. The high-stakes environment at ANVIL has provided a sense of gravity and mission-driven motivation that I'd struggle to find elsewhere. While the burdens of a TS/SCI clearance and the pressures of high-level responsibility are significant, the satisfaction derived from my work is unparalleled. Moving forward, I intend to continue my work at ANVIL, expanding my technical repertoire, with the ultimate goal of becoming an even more capable engineer in the secure communications landscape.