

Final Internship Reflection Paper

Zineb Crowe

Endpoint Transport Cloud Engineer

AERMOR LLC / Naval Network Warfare Command (NNWC)

Professor: Dr. Teresa Duvall

Teaching Assistant: Joshua Russell

Course: CYSE 368

Old Dominion University

Spring 2026 Term

Table of Contents

1.	Introduction	3
2.	Management Environment	5
3.	Major Work Duties, Assignments, and Projects.....	7
4.	Use of Cybersecurity Skills and Knowledge	10
5.	ODU Curriculum Preparation	12
6.	Fulfillment of Learning Outcomes	14
7.	Most Motivating or Exciting Aspects	16
8.	Most Discouraging Aspects	17
9.	Most Challenging Aspects	19
10.	Recommendations for Future Interns	20
11.	Conclusion	21

1- Introduction

My decision to pursue an internship aligned with my role as an Endpoint Transport Cloud Engineer at AERMOR LLC, supporting the Naval Network Warfare Command (NNWC), marked a pivotal step in my transition from a background in logistics at Renault to a career in cybersecurity and cloud engineering within a Department of Defense (DoD) environment. Although I am employed in this position, the responsibilities and hands-on technical experience directly align with the learning objectives of the CYSE 368 internship course, allowing my role to be formally recognized as an internship. As a Bachelor of Science in Cybersecurity student at Old Dominion University, holding certifications such as AZ-900, MS-900, Security+, and SC-900, I recognized the importance of gaining practical experience beyond the classroom. This opportunity allowed me to apply theoretical knowledge in a real-world setting while preparing for advanced certifications such as AZ-104 and CISSP, all while balancing full-time work, academic responsibilities, and family life.

AERMOR LLC is a contractor dedicated to providing DoD with engineering and cybersecurity expertise to support installation and maintenance of critical networks to ensure warfighters have reliable access to the data they need. It supports NNWC and was assigned to PEO Digital. NNWC evolved from earlier Navy network warfare capabilities that supported communication modernization initiatives required to address growing cybersecurity threats. The command manages the Navy's enterprise transition from NMCI to the Nautilus platform, providing secure, reliable transport to and management of endpoints at install sites around the world. Users of these systems include Navy military, DoD civilians and contractors from every

branch of service stationed around the world. They require secure and reliable access to networks every day to execute their mission. AERMOR LLC supports FlankSpeed, a cloud-based collaboration and secure transport capability, VPN endpoint transport, Nautilus Virtual Desktops (NVD), and Microsoft Intune-based endpoint management. All services are managed in a NIST SP 800-53 compliant environment, with CMMC Ready and FedRAMP High coverage to protect Controlled Unclassified Information (CUI).

To guide my development, I established three specific learning objectives in my Memorandum of Agreement (MOA). The first was to gain the necessary skills to perform advanced hybrid network troubleshooting, with specific focus on determining how to properly troubleshoot routing on legacy NMCI infrastructure in conjunction with Nautilus Endpoints (NEP) and Nautilus Virtual Desktops (NVD). The second was to apply DoD policies and guidelines for cybersecurity compliance to both the configuration of endpoints and access to sensitive information as well as the access controls in place should a cyber incident occur. The third was to improve my ability to effectively communicate professionally within a secure, multi-team environment whether it be through ticketing systems, with users, or through the creation of technical documentation related to found issues and resolutions. These objectives were set to help bridge some of the academic learning with real world military operations where precision and accountability are paramount.

Upon arrival, I was given a comprehensive orientation and on-boarding process. During this time, I learned about the different tools and systems the team utilizes such as Microsoft Azure, Microsoft Intune, our VPN setup, and the FlankSpeed tool. I also went through training for BMC Helix, the ticketing platform we use, as well as training for handling sensitive and classified information. My first impression of the set-up for the internship was exciting and

challenging at the same time. The structure of the workspace is built to be mission-focused, emphasizing accuracy, accountability, and teamwork among not only the DoD Military, Civilian, and Contractors but also other organizations around the world. It takes a lot of patience, flexibility, and critical thinking to successfully complete the tasks assigned to an intern in this environment.

Early in the internship, I was working on troubleshooting a routing issue where users were unable to access .mil sites. Through a series of route traces and analysis, we discovered the root cause was due to an unexpected behavior of one of the endpoint transports. Through the troubleshooting and analysis, I got a real-world sense of how our interconnected systems function in practice and the degree to which even small issues can have broader operational consequences.

My experience with NNWC has been unique and has been provided with an opportunity to work within an environment where cybersecurity, cloud engineering, and compliance intersect with communication on an ongoing basis. This paper explores my internship experience through the lens of the management environment, tasks tackled by me, the application of my existing knowledge of information and cybersecurity, and my professional growth.

2- **Management Environment**

Management at AERMOR LLC is structured and collaborative. We adhere to a strictly militarized management style which enables personnel to perform at their highest levels. This framework further includes contractor oversight and an established technical mentor role that ensures technical proficiency. Leadership at AERMOR manages administrative tasks such as contractor compliance and performance metrics, business and financial management, time and

effort tracking, pay management, policy administration, adherence to all relevant employment laws, development and oversight of administrative procedures, managing required training and implementing all business wide support functions. Meanwhile, NNWC leadership provides mission objectives and technical direction for all day-to-day activities.

As an Endpoint Transport Cloud Engineer, I have dual management which means I have organizational support and technical guidance. My day-to-day work is guided by a technical lead, Ryan Foster, who manages our team in a style that I find to be highly effective. His leadership approach is more than handing down instructions and Ryan encourages problem-solving through critical thinking and independent research to solve customer issues. For example, when a user is reporting website access issues on their Nautilus machine, I would first look at the findings from trace routes and monitoring tools such as Azure Monitoring and then discuss the findings with Ryan and the rest of the team to drive towards a resolution. Overall, my experience at NNWC enabled me to become more confident in my work.

All leaders within the company stress accountability, precision, and documentation. With the environment of cybersecurity being highly compliant and audit driven, it is key to take actions seriously and work diligently. Strong communication within the team including our military, civilian, and contractor personnel were vital to successfully meeting team objectives. Additionally, Endpoint Transport team held weekly team syncs and continuous communication through collaboration tools like Microsoft Teams.

A similar management structure exists to support our users and address any issues they may have with website access. Three levels of support are in place: Tier I addresses initial user inquiries, Tier II performs website testing and gathers detailed information such as connection

types and error messages to support troubleshooting, and Tier III handles more advanced issues related to endpoint transport and routing. Roles and responsibilities were clearly defined within the management structure, allowing for efficient issue resolution and smooth progression through levels of support.

AERMOR's project management incorporated several aspects of agility to include a streamlined workflow, prioritization of tickets, and an emphasis on ongoing training such as current DoD Cyber Awareness Training, processing of Controlled Unclassified Information (CUI), and Privacy Act requirements. Although at times, outside coordination introduced delays, including escalations, overall, the project management environment remained highly effective throughout the effort, maintaining focus on mission critical objectives.

My experience in this management environment was invaluable as I was able to grow as a professional. The environment allowed for critical thinking and fostered camaraderie while maintaining a culture of full accountability. This operational environment, driven by strong leadership, and a well-defined structure, combined with open lines of communication contribute directly to mission success in cybersecurity operations and prepared me to operate confidently in complex, critical environments.

3- Major Work Duties, Assignments, and Projects

The work of an Endpoint Transport Cloud Engineer is critical in resolving connectivity, endpoint and access to Navy systems issues occurring during the NMCI to Nautilus transition. The types of issues solved are on a network to end user level, requiring the ability to resolve routing issues, configure endpoints to operate correctly and enforce Navy compliance using tools such as Microsoft Azure. Many of these issues that are in a live environment and time sensitive

in nature, requiring the Engineer to work with users to resolve tickets submitted through BMC Helix to ensure end users have timely resolution to their issues. This is critical as users requiring connectivity to .mil websites, logistics systems and other enterprise applications require timely operationally effective support to meet their Navy mission.

I spent a lot of time in my new role analyzing traffic through different connections like FlankSpeed Edge (FSE), VPN East and West, Nautilus Virtual Desktop (NVD), and Ubiquitous networks. Many of the challenges that Nautilus users faced were related to differences in how their system routed traffic, how they resolved DNS, or how their gateways were set up in comparison to how legacy NMCI systems had been configured. I would have to pull and examine routing tables, perform long trace routes, and pull detailed Azure Monitor and PowerShell data to determine where something was failing. I would then use that information to identify where misrouted packets were traveling and work with users to configure their computers to send the packets over the optimal connection.

A large amount of my time went into just getting people access to TTMS, DLA and other enterprise applications and external web sites that people needed to use for their work. That required quite a bit of analysis to determine where traffic was being routed in the internal network, and then how that traffic was being interpreted by external systems. At first glance, internal routing and DNS looked to be set up correctly. It required some more in-depth research to find out that traffic was being NAT'd differently than I had been told by our internal routing team. Once I was able to identify the correct external CIDR ranges, I worked with site admins, DISA, and our external partners to get those whitelisted, which took a lot of back and forth, but in the end all users (regardless of connection type) were able to access the sites correctly.

A particularly challenging project was identifying the root cause of users being unable to access systems, often encountering permission errors despite all indications that system configuration and internal settings were correct. After methodically investigating and testing routing, firewall rules, and coordinating with other external parties to verify correct recognition and control of IP addresses, I was able to identify the underlying causes of each issue. Similar collaboration and troubleshooting took place across different network paths to determine why users were unable to access certain systems. Often, seemingly small misconfigurations at the network edge impacted end users' ability to complete critical mission tasks.

In addition to addressing individual complaints, I also worked on ways to enhance the performance and scalability of the network. I analyzed and repaired several instances of websites not being able to be accessed, and categorized sets of scenarios to test optimal routing and verified fixes on different stacks. By establishing a consistent pattern of access, the number of occurrences of these repeat issues has significantly decreased and the overall performance of the network has increased.

Also, I worked in collaboration with other teams and components to resolve issues. This included working with network teams, site admins and external organizations to diagnose and troubleshoot issues that involved multiple components and systems. The troubleshooting involved identifying and testing different connection paths and ways to route around failures and verifying fixes before they were considered closed on any tickets.

Throughout these duties, assignments, and projects, my work has continued to support the NNWC's mission of reliable endpoint transport. Each project not only resolved immediate connectivity needs but also contributed to the NNWC's long-term goals of improved network

stability and performance. Through these tasks, I have also continued to gain insight into how endpoint transport, cloud infrastructure, and cybersecurity issues can be best addressed in support of military and intelligence community mission requirements.

4- Use of Cybersecurity Skills and Knowledge

This internship was an excellent way for me to apply the knowledge gained from my time at Old Dominion University and my Security+, AZ-900, MS-900, SC-900 certifications in a dynamic, mission critical environment. Prior to this internship, I had only studied and gained knowledge of various forms of cybersecurity. However, this experience allowed me to translate that knowledge into a practical application and function as a supporting role to maintain a Department of Defense (DoD) information technology network in an adequate, secure, and reliable state.

I was able to consistently apply the basic skills that I learned throughout my internship while working to resolve endpoint transport and connectivity issues on a day-to-day basis. Much of the analysis required to resolve these issues involved looking at the routing path of messages, identifying potential failures within a network, and verifying that endpoints have the proper secure access to our organization's systems. I was able to apply my knowledge of IP addressing, routing, and network design concepts including segmentation while analyzing access issues for systems such as the TTMS system to determine if the issue was related to the local routing configuration, firewall rules, or limitations on the external system. This further solidified my belief that security is not solely the responsibility of one system and often requires a holistic view of how systems interact with other systems in multiple environments.

In the last few months, I have grown in my ability to apply knowledge of cybersecurity to technical problems that would normally be viewed as purely network related. Viewing problems from a CIA (confidentiality, integrity, availability) perspective has helped me look at issues in a more well-rounded fashion, instead of focusing only on connectivity. This perspective has particularly helped when dealing with boundary controls, identifying if users or systems have the proper identity, and how different networks are segmented. In our GEMSIS project, what started out to be a simple permission issue, had to do with an external system not properly understanding NAT-translated IP addresses. We had to expand our thinking on how access control is not just a local configuration but can also involve external systems that are trying to enforce certain security policies.

In addition to applying existing knowledge, I developed some new technical skills within the project scope. Some of these skills had not been previously utilized in academic or previous work environments. I became familiar with Microsoft Azure platforms and used the Azure CLI within scripting automation. I learned how to manage endpoint security and how Network Address Translation (NAT) impacts external access control and IP whitelisting. In addition, I became proficient in diagnosing and resolving issues within complex hybrid environments consisting of cloud, on-premises and external entities.

When working to resolve endpoint issues, concepts from compliance and security frameworks were constantly at play. References were made to NIST SP 800-53, CMMC, and FedRAMP High requirements when ensuring that endpoint configurations were properly set and aligned to validate secure access and documentation for future auditing. Intune provides robust role-based policy enforcement which allows for implementation of secure configuration and hardening practices to meet baseline security requirements for endpoints. Furthermore, proper

documentation of all actions in BMC Helix allowed for proper traceability, accountability, and audit readiness within a highly regulated environment.

My experience from the internship has completely changed my perspective on how I see cybersecurity. Before I started the internship, I had a theoretical understanding of cybersecurity. I knew how to protect individual systems and components, but my new experience has shown me how a true cybersecurity strategy is complex and multi-layered. It involves network security, cloud security, endpoint security, and security of any external systems or data that are integrated with the system. Moreover, I have realized that having a deep technical knowledge is not enough, one needs to be able to think critically, pay attention to minute details, and analyze complex systems to identify potential threats.

5- ODU Curriculum Preparation

I gained a solid theoretical and technical foundation in a well-rounded cybersecurity curriculum at Old Dominion University. With this preparation, I entered my internship as a Cloud Engineer with some prior knowledge of networking, security principles, and cloud engineering fundamentals. Through the ODU's courses and certifications, I gained in-depth understanding of topics such as subnetting, routing, network access control, and risk management principles that I successfully applied to my duties as a Cloud Engineer.

I made good connections between what I was studying and my work during the internship. In the networking classes, I studied IP addressing, routing behavior, and went in depth looking at different protocols and how to analyze them. Much of what I studied for endpoint transport issues on the Nautilus side translated directly. My understanding of topics like

IPsec and general concepts related to secure communications also translated well to the VPN configurations and general secure access solutions that we utilize in Azure.

Additionally, my understanding of different cybersecurity frameworks, including NIST SP 800-53 and a general understanding of zero-trust principles translated to what I saw implemented in the different environments that we worked in, namely Intune compliance policies and FlankSpeed access controls. In addition to learning the general concepts and principles of technical writing at school, I was able to implement some of the experiences throughout my internship. Completing technical writing projects at ODU involved creating, revising, editing, and proofreading documentation that helped me become proficient in documenting certain aspects of and reporting on incidents found within the BMC Helix product suite. Certain security policy topics covered such as security and privacy controls related to Managed Protected (MP), Use, Sharing, Disclosure, Access & Authentication for Controlled Unclassified Information (CUI), Data Protection and Critical Data Asset Protection, as well as Identifying and Mitigating Risk were highly relevant to the DoD mandated training provided to all DoD personnel. I was able to understand the general implementation of these practices and policies within the industry, especially in the government sector as utilized within the office.

In addition to material I had studied in class, the internship also exposed me to additional tools and processes that I would not have learned about in school. Working off a partially NMCI migrated Nautilus network introduced issues that the school's network does not have, such as NAT translation and external IP whitelisting. There were also issues involving coordinating with different organizations, which can be time-consuming, especially when there are many variables at play and not all the information that we need is available. Each of these real-world problems involved incomplete data, a time crunch, and dependencies on other groups. I also benefited

from exposure to a variety of enterprise-level tools and technologies such as Microsoft Azure, Microsoft Intune, and Large-Scale Endpoint Management.

Through these tools, I gained better insight into how a full cybersecurity implementation would operate, especially around the concepts of compliance, monitoring, and secure access. I also recognized additional knowledge and education in the areas of cloud security operations, hybrid environment, and large-scale system integration.

Throughout my time in the ODU Cybersecurity bachelor's program, the curriculum provided a strong foundation that prepared me for success in my internship. In addition, gaining experience in the real world, the program has helped strengthen my skills as a Cloud Engineer while increasing my overall knowledge of cybersecurity. It has also reinforced key concepts related to the field and shown me that it is an ever-changing field that continues to grow at a rapid pace and helped solidify my desire to continue learning and to be adaptable throughout my professional career.

6- Fulfillment of Learning Outcomes

At the start of my internship, we established specified three main goals in my Memorandum of Agreement (MOA). Those goals were to become proficient in advanced hybrid network troubleshooting, apply cybersecurity compliance standards in a real-world setting, and to enhance my professional communication skills within a multi-team environment, all while maintaining the highest level of security. All the goals were met, and in some cases exceeded, as I completed my internship.

First, I strove to improve my ability to troubleshoot hybrid network infrastructure components within even more complex operating environments such as NMCI and Nautilus. In

each instance, I went from structured, step-by-step walkthroughs to independently researching and solving complex problems for various vantage points within the production network. Every day, I applied the insight I gained through attempting to understand and describe how multiple paths of connectivity interact to troubleshoot routing issues at several key points within the network, including connections over FlankSpeed Edge, the VPN East and West connections, and within the Nautilus Virtual Desktop environment. I applied similar reasoning to troubleshoot and resolve access issues to web-enabled systems such as GEMSIS, TTMS, and Treasury.gov (among others), including evaluating routing and NAT translations and discovering external components such as the need for IP whitelisting. In this way, I refined my critical thinking skills to tackle and resolve more complex incidents alone.

The second objective focuses on applying cybersecurity compliance to endpoint configurations and processes. Our work with Microsoft Intune allowed us to ensure endpoints followed regulatory requirements, verify correct security configurations, and confirm adherence to DoD guidelines. Additionally, correct documentation and record-keeping for auditing and compliance were necessary. This allowed the team to go beyond a theoretical understanding and practice implementation of secure configurations and compliance processes in a controlled environment.

To reach my third objective I aimed to enhance professionalism in communication within a collaborative multi-team environment. This goal was met by engaging with our internal teams and site administrators, as well as external organizations to discuss tickets and develop solutions. Throughout the last few months, I have worked to ensure that all incidents, their resulting resolutions, and any learned information were documented within BMC Helix and properly relayed to users. By engaging with leadership and team members, I better organized, detailed,

and solution-focused my communication to reach a full range of technical and nontechnical recipients.

Throughout the internship I was constantly evolving from depending on guidance and mentorship in the beginning to independently troubleshooting, creating solutions and assisting other team members as needed towards the end. The stages in which I grew as a Cloud Engineer in a real-world cybersecurity environment aided in my completion of the objectives I set for myself.

The internship was great and met all my initial goals for learning. I became more confident and proficient in breaking down complex systems and learning new technologies. I also became more competent in both technical and communication skills, as well as gained a better understanding of how security principles are put into practice in daily operations, as well as how to design and operate cloud-based systems. This has helped me grow and be ready for other cybersecurity and cloud engineering roles.

7- Most Motivating or Exciting Aspects

The most motivating aspects of this internship were the real-world application of the skills I learned and the personal growth I experienced. Knowing that my work helped resolve issues affecting the Navy personnel and their mission critical systems was very motivating. The problem-solving aspect of this internship was also very encouraging. Each problem presented a unique challenge to troubleshooting and repair and each solution required detailed analysis, patience, and creativity. Seeing the result of a problem fully resolved, after days and sometimes months of troubleshooting and collaboration with other teams, was very rewarding. Additionally, the feeling of confidence as a Cloud Engineer was also a motivating aspect of this internship.

Another key component fueling my motivation was the mentorship provided throughout the program by the leadership. Their thoughtful guidance and challenging me to think critically, to work independently and solve complex problems encouraged many of those great “Aha” moments. Seeing the concepts I have studied finally come together in practical application is truly rewarding and serves as a constant reminder of my evolving knowledge and expertise. The Department of Defense environment where I contributed, placed a high value on security, reliability, and precision which kept me highly engaged. Managing the substantial workload of the internship while at the same time attending classes and maintaining other activities motivated me to put forth my best effort each day. Seeing my skills grow with each challenge served to fuel my desire to persist in working towards a long-term leadership career in the field of cybersecurity and cloud engineering. The internship experience was highly motivating and rewarding, and I intend on applying all that I have learned at NNWC throughout my career.

8- Most Discouraging Aspects

My internship experience was incredibly rewarding, but there were also some discouraging moments during my time at NNWC. Part of the value of an internship at NNWC is that you get to deal with actual problems, not just idealized examples. Some of these problems took an excessive amount of time to resolve, and many of the seemingly simple problems I got handed in turned out to be complex, multi-layered issues involving things like routing, external dependencies, and overlapping security systems. Some of these involved getting help from other teams or even outside organizations, like gaining access to the TTMS, and as a result took many days to resolve one relatively minor issue. It was sometimes hard to persevere when there were so many different variables involved and little control over external factors.

I was also discouraged by the need to bring in external teams and vendors to help troubleshooting some of the issues. Often, I would have to wait for a site admin, network team, or vendor to investigate and respond to issues that I wasn't able to troubleshoot or resolve on my own. This required a lot of time and effort spent chasing down answers. I found that good time management and persistence were necessary to keep projects on track. Additionally, security and compliance concerns meant that I had to verify and have any changes approved before implementing. While these precautions are necessary and important for keeping things running safely and securely, they often took some of the fun out of making relatively minor changes.

As with any DoD deployment, there were constraints due to classification and security restrictions. While we were able to work with site engineers and operators to troubleshoot and resolve problems, there were a few cases where we encountered limitations due to the classification of certain systems or security restrictions that prohibited us from receiving or disclosing additional information. Additionally, as users and systems acclimated to the NMCI infrastructure and then experienced a forced transition to Nautilus, systems behaved differently, caused unusual errors, or took on unexpected expectations regarding connectivity and access to various resources. These initial transitional problems also manifested themselves in the form of a large volume of repeated questions about issues that had previously been encountered under the NMCI environment.

The internship required significant time and effort, and in my case, it required some balancing with my current job, studies, and family commitments. Managing all the different responsibilities demanded lots of discipline and patience. At times it was disappointing, especially when tasked with repetitive, hard work or stuck in loops trying to resolve tricky problems. However, these challenges provided great value as they were realistic simulations of

some of the difficulties of working in Cybersecurity, and have taught me lots of new skills and patience as I have had to work with different teams, manage dependency, work under tight time pressures and think of creative solutions to problems as they arise.

9- Most Challenging Aspects

The most challenging part of my internship was trying to understand and deal with how the NMCI legacy systems integrate with the Nautilus environment. Most of the troubleshooting I did involve trying to understand how different components interact to create a problem. Often, I was required to analyze several layers at the same time including how DNS was resolving, how SSL certificates were validating, how Network Address Translation (NAT) was working, how routes were propagating, and what external IP addresses needed to be added to a whitelist. As a result, there was often a structured approach to troubleshooting that was required to try and pinpoint the problem.

As we continued to identify and resolve underlying causes of issues, we also had to work within strict boundaries of proper DoD security practices and procedures that must be followed at every step. All actions had to be verified correctly, fully documented and complied with DoD standards. This added an additional layer of responsibility, as solutions could not only be effective but also compliant and auditable.

Many of these issues require coordination with other organizations such as DISA, external vendors, or site administrators to resolve problems more quickly. Working with multiple teams who had different priorities and levels of focus required the team to have a solid technical understanding of the issues as well as the interpersonal judgment to surface the most critical problems to the appropriate users. Along the way, I faced the personal challenge of transitioning

from supported work to independent problem-solving and completion of complex tasks. Initially, I completed tasks with the support of and under the guidance of mentors. However, as the internship progressed, I was forced to grow as a professional by taking ownership of the problems at hand, conducting more in-depth research, and developing innovative, complete solutions with the full confidence of my ability to make technically sound decisions. All these failures and lost hours have taught me a lot. Dealing with a new environment has pushed my analytical capabilities to their limits and given me valuable insights into the daily grind of a cybersecurity team. They also allowed me to approach a problem from multiple angles and think of creative solutions. All of this will help me in my future role as a Cloud Engineer in a high-stress, complex environment.

10- Recommendations for Future Interns

It would be beneficial for future interns to have a good understanding of basic networking fundamentals such as DNS, routing, subnetting, etc. as well as hybrid network configurations and the ability to troubleshoot connectivity issues in such environments. Additionally, having experience with or knowledge of cloud platforms like Microsoft Azure, and a basic certification such as AZ-900 or Security+ would be very beneficial as well.

Effective communication and documentation skills are also necessary to succeed as an intern in this environment. The ability to describe in detail a technical issue encountered, the steps taken to troubleshoot, and provide regular updates via tools like BMC Helix is critical. Accurate and precise documentation is a defining characteristic of the DoD environment, and tracing actions for compliance purposes is a regular task of personnel in these roles. Developing these critical skills is among the organization's top priorities.

Additionally, patience and persistence are key attributes of a successful individual in this role. Many of the current issues with the website are complex in nature, requiring a step-by-step approach to troubleshooting and often involve collaboration with other teams to diagnose and rectify issues. Not all problems will have simple solutions, and the approach will require them to be methodical, thorough and persistent.

Finally, having some experience with tools such as Microsoft Intune, PowerShell and other endpoint management tools can give interns some real-world experience with the tools before they start the internship. Moreover, taking advantage of opportunities to have a mentor and trying to keep a healthy work-life balance will help them in the long term. Overall, preparing as much as you can, being flexible and open to learning as much as they can be, key to a successful experience in this fast-paced field.

11- Conclusion:

My internship was an incredible experience which greatly impacted my understanding of cybersecurity and cloud engineering in a real-world environment conducting real world missions. One of the most important things I learned throughout my internship was that being a “cyber professional” is not just about having a vast knowledge base of the ever-evolving technology and threats in the information technology field, but also how you put that knowledge to use through technical proficiency and adherence to processes, accountability, and a strong sense of mission.

The high standards of the Department of Defense maintain a cutting-edge cyber environment require high precision, accurate documentation, and teamwork. During my internship I gained exposure to several technical capabilities and solidified my problem-solving capabilities as a Cloud Engineer. Additionally, the opportunity to collaborate with and

communicate engineering problems in a straightforward manner to multiple teams was invaluable. Overall, my experiences during this internship helped me to apply the cybersecurity fundamentals learned at ODU and applied my knowledge in a real-world environment.

This internship will allow me to apply my class work to real-world projects and allow me to further develop my skills at ODU. It has also motivated me to obtain additional certifications such as AZ-104 and CISSP to further enhance my knowledge in cloud security as well as enterprise-level security management. Additionally, this experience has solidified my future goals and my focus on the field of cybersecurity and cloud engineering within the DoD, and has furthered my understanding and interest in topics involving endpoint transport, cloud-based infrastructure and network operations within secure environments. Throughout this internship I have gained experience and knowledge that will be valuable in my career and will aid in my development into a more knowledgeable and skilled cybersecurity professional, ready to take on more challenging roles within the DoD as well as a cybersecurity leadership role.

Finally, this experience will continue to influence the remainder of my time at Old Dominion University, as it has shifted my focus toward applying concepts in practical and real-world contexts. It has inspired me to further my skills in cybersecurity by acquiring advanced certifications and real-world training specifically in cloud security and endpoint security. This internship has also solidified my desire to continue working in the field of cybersecurity for the Department of Defense in a long-term capacity supporting and defending the military's missions. Overall, this experience strengthened my passion for the field and provided a strong foundation for my future growth and success.