Internship Final Paper

Jaden Walker

TIAG

CYSE 368 Internship

Fall 2025

12/1/2025

TABLE OF CONTENTS

1. Introduction

I chose this internship because I wanted real experience in cybersecurity and system administration. I also wanted to place myself in an environment where the learning was constant and where the responsibility felt meaningful. TIAG supports government driven operations and that level of structure appealed to my long term goals in cloud engineering and DevSecOps. I knew that if I wanted to grow in this field, I needed to understand how large organizations maintain security and stability each day.

Before I started, I set three learning outcomes that would guide my growth during the internship. I wanted hands on experience with enterprise system administration. I wanted a clearer understanding of cybersecurity principles through direct involvement with patching, compliance, and vulnerability management. I also wanted to develop my cloud engineering and automation skills so that I could move closer to the DevOps work I hope to do after graduation.

My first fifty hours showed me I made the right choice. I completed patching tasks, updated hardware and software lists, confirmed workstation naming, and learned how different teams work together. These tasks shaped how I understood responsibility in a real technical environment. Every assignment connected to a larger process. Even small steps like checking device names created better accuracy for audits and planning. This work helped me see how the smallest tasks build the foundation for an entire system.

2. Internship Background and Organizational History

TIAG supports government agencies with infrastructure operations, cybersecurity, patching, system administration, and modernization efforts. The work requires consistency, accuracy, and clarity. Every change must be accounted for. Every deployment must be tracked. Every vulnerability must be addressed. The environment has many moving parts and each part connects back to real missions that matter.

TIAG supports a wide range of internal departments. These include helpdesk operations, network engineering, system administration, and security engineering. Each team has its own responsibilities, but they also depend on each other. Changes in one area always affect another, so communication is important. The organization works closely with government civilians who provide structure and history for the environment. This mix of contractors and government staff creates a professional atmosphere where the mission stays at the center.

What stood out to me early was how structured everything was. The organization expects accuracy in documentation and expects discipline in operations. The security posture of the environment affects every individual and every department. Because of that, TIAG works with a mindset focused on reliability and clear procedures. This type of organization teaches you how to think long term and how to understand the impact of each technical decision.

3. Orientation, Training, and Initial Impressions

My orientation introduced me to the server architecture, the vulnerability checking tools, the patching methods, and the database systems used by the environment. I learned how ACAS identifies vulnerabilities and how Tenable provides the IAVA information needed for patching. I also learned how MCEM deploys software across large numbers of devices.

During the first week, I attended meetings where teams updated leadership on their progress. These meetings explained the responsibilities of each group and helped me see how taskers move through the organization. Understanding these structures made it easier for me to ask questions and to see how my assignments fit into the larger mission.

My early impressions of TIAG were positive. The environment felt professional and focused. People communicated clearly, and everyone seemed aligned with the goal of supporting users and keeping the environment secure. My initial tasks involved patching, updating hardware and software lists, and verifying user information in Active Directory. These tasks taught me how important accuracy is in an environment with many devices. I realized quickly that small mistakes create large problems, so attention to detail became a priority for me.

4. Management Environment and Supervision

The management environment at TIAG focuses on accountability and support. Supervisors communicate expectations clearly, and they encourage questions instead of discouraging them. I always felt comfortable admitting when I did not understand something. Leadership explained processes step by step and helped me build confidence in my work.

Every department has leads who guide the flow of information. System administrators oversee deployments. The network team handles connectivity and stability. The security engineers track policies and compliance. The helpdesk manages user tickets and immediate support. This structure allows each person to understand their role and work efficiently.

Throughout my internship, supervision helped me grow. Leadership trusted me with tasks and offered feedback that shaped my skills. Their willingness to let me learn through real assignments helped me become more prepared for the technical roles I hope to pursue after graduation.

5. Major Work Duties, Assignments, and Projects

My assignments grew steadily throughout the internship.

During the first fifty hours, I learned about server patching, workstation patching, and vulnerability checking. I updated hardware and software lists and verified workstation names. I also gained experience with ACAS, Tenable, and MCEM. These early tasks were important because they helped me understand how an enterprise identifies and resolves vulnerabilities. They also taught me the value of accuracy.

During the second fifty hours, I worked on in processing users and assigning M365 licenses. I added users to the correct OU, ran scripts to create profiles, and entered the fields needed for new accounts. I also learned about license replication times and how delays can affect user onboarding. I worked with Splunk to build dashboards and attended meetings about network upgrades and pilot programs. These assignments helped me understand the operational side of system administration.

During the third fifty hours, I contributed to a pilot program for an in processing and out processing application. I met with multiple teams to gather requirements. I drafted a pilot document that outlined three stages of development. I presented my idea to leadership, and they appreciated the initiative. A VIP user commented on how the solution would improve efficiency for real users. This project gave me confidence and helped me see how technical ideas become solutions in a real environment.

Each assignment supported the goals of the organization. Patching reduces risk. User provisioning supports operations. Licensing enables access. Pilot planning supports modernization. Every duty connects back to stability and security.

6. Use of Cybersecurity Skills and On the Job Learning

This internship helped me apply my existing cybersecurity skills while also forcing me to learn new ones. Before starting, I understood basic concepts like patching, vulnerabilities, and user creation. However, I had never applied these skills in an enterprise environment. I learned how to identify vulnerabilities with ACAS. I learned how to patch large groups of devices with MCEM. I learned how Tenable links vulnerabilities to compliance requirements.

I also learned about Active Directory structure and how user profiles move through the environment. I realized that small details such as group membership and OU placement affect everything from login access to permissions.

The internship also helped me understand the real meaning of cybersecurity. It is not only about technical tools. It is about process, communication, timing, documentation, and consistency. Seeing these concepts in action changed how I view the subject.

7. ODU Curriculum Connections and Academic Preparation

ODU prepared me by teaching the foundation I needed to understand the environment. My courses introduced me to operating systems, networking, cybersecurity principles, and access management. These ideas gave me the vocabulary and the mental model needed to learn quickly during the internship.

However, some concepts became clearer once I applied them in real work. For example, patching felt like a simple concept in class, but in practice it requires planning, tracking, and troubleshooting. Active Directory also became much easier to understand once I worked with it daily.

The internship reinforced my education and added depth to topics that seemed abstract before. I also gained exposure to new areas like licensing workflows, Splunk dashboards, API planning, and modernization discussions.

8. Evaluation of Initial Internship Objectives

My first goal was to gain hands on experience with enterprise system administration. I achieved this through patching, user provisioning, and workstation management.

My second goal was to deepen my understanding of cybersecurity. I achieved this through vulnerability scanning, compliance reviews, and learning how different tools support security.

My third goal was to grow in cloud engineering and automation. I moved closer to this goal through independent study and through the pilot program work where I drafted a technical solution that used concepts from cloud architecture. I also studied for the AWS Solutions

Architect exam during the internship and passed it. That achievement supported my long term goals and helped validate my knowledge.

9. Motivating or Exciting Internship Experiences

The most exciting part of the internship was working on the pilot program. It gave me a sense of ownership and responsibility. Presenting my idea to leadership showed me that I can contribute to real solutions even as an intern. Hearing positive feedback from a VIP user made the experience even more meaningful.

I also enjoyed studying for my AWS certification and passing the exam. It made me feel like I am on the right path. I connected the cloud concepts I learned with the work I did at TIAG, which motivated me to keep learning and improving.

Working with different teams also felt rewarding. Conversations with system administrators, helpdesk staff, and security engineers helped me see how each role fits into the bigger mission.

10. Discouraging Aspects of the Internship

Some tasks felt repetitive. Patching requires patience and consistency. Updating lists also requires time and accuracy. There were moments when delays in license replication affected onboarding and created slowdowns.

Even with these challenges, I understood that these tasks were important. They taught me discipline and reinforced why accuracy matters in system administration.

11. Most Challenging Aspects of the Internship

The most challenging part of the internship was learning the timing involved with deployments and user provisioning. I learned that changes do not happen instantly. They move through the environment in stages.

Understanding the structure of the OU and the departments also took time. The environment has many users and many specialized teams. Learning who handles what required patience.

The pilot program also challenged me because I had to gather requirements, understand workflows, and communicate ideas clearly.

12. Recommendations for Future Interns

Future interns should prepare by learning the basics of Active Directory, Windows Server tools, patching methods, and cybersecurity principles. They should also practice communicating clearly because questions help prevent mistakes.

I recommend spending time studying cloud concepts to support long term career goals. I also recommend taking notes during meetings so that you do not miss important details about workflows or upcoming changes.

13. Conclusion

This internship shaped my understanding of cybersecurity, system administration, and organizational operations. I gained hands on experience that brought my academic knowledge to life. I learned how to work with different teams and how to support users in a professional environment.

The internship will influence the rest of my time at ODU by giving me confidence to pursue harder courses and deeper technical work. It will also guide my professional future as I move toward roles in cloud engineering, DevOps, or system administration.

I believe this experience will remain a defining part of my growth. It helped me see my potential and gave me a foundation that I can build on for years to come.