Keller Beacham

CYSE 368

Spring 2026

Professor Teresa Duvall

TA Joshua Russell

SharePoint Specialist

Reflection #2

During my internship as a SharePoint Specialist at the Mid-Atlantic Regional Maintenance Center (MARMC), I have continued to gain practical experience working with enterprise information systems and data management. My role involves maintaining SharePoint sites, managing permissions and access controls, supporting users across the command, and ensuring that information stored within our systems follows proper governance and security standards. Being able to work in a real operational environment has helped me understand how many of the cybersecurity and information management concepts I learn in school actually apply in practice.

One of the main parts of my job is maintaining the MARMC SharePoint Home Site and its subpages. This includes keeping information up to date, making sure the pages function correctly, and maintaining proper permissions for users who need access to different areas of the site. Because SharePoint acts as a central hub for information across the command, organization and accessibility are extremely important. If pages are not maintained properly or permissions are incorrect, it can slow down workflows or expose information to people who should not have

access to it. Managing these permissions has helped me understand how important access control is in cybersecurity. Even something as simple as assigning the wrong permissions can have serious consequences in an organization that handles sensitive operational information.

Another large part of my work involves managing shared area permissions and assisting with data organization after a major data migration to SharePoint. The team migrated over three terabytes of data from legacy shared drives into SharePoint, which was a huge project for the command. Since that migration, there has been a lot of follow-up work to make sure the information is organized properly and that users can access what they need. Many people across the command rely on SharePoint daily, so when they cannot find files or do not have access to a system, it becomes our responsibility to help resolve those issues. Recently I have worked closely with Tyler Johnson to manage access requests for the PMS Viewer system for personnel in several departments as well as external commands. Handling these requests has helped me develop stronger problem-solving skills and a better understanding of how user access is managed within a large organization.

One of the responsibilities I take most seriously is managing the command's 90-day Personally Identifiable Information (PII) audit for SharePoint. Every quarter we must verify that no sensitive personal information is improperly stored or exposed within our SharePoint sites. This process requires going through different site areas, reviewing stored files, and making sure the command remains compliant with security standards. Conducting these audits has helped me better understand how governance and compliance work in real cybersecurity environments. It also showed me how much responsibility comes with managing information systems, because even small mistakes involving sensitive data could create serious problems.

I have also recently started working with Power BI, which has been a new learning experience for me. I created a spreadsheet that tracks gains and losses for civilians and contractors within MARMC and turned that data into a dashboard that can be displayed on the command's SharePoint site. This allows leadership to quickly view workforce data in a more visual and organized way. I am also helping build a SharePoint page that allows new personnel to track where they are in the onboarding process at the command. Working with Power BI has helped me see how data analysis and visualization tools can support decision making and improve communication across an organization.

As I continue working in this role, I have also started thinking more seriously about whether this is a field I see myself growing in long term. Before this internship, most of my experience with cybersecurity was from coursework, labs, and my Marine Corps occupation. Being able to work with real systems and support real users has given me a much better understanding of what the job actually looks like day to day. I have realized that I enjoy working in environments that combine system administration, cybersecurity, and information management. It is rewarding to know that the work I do helps support the command's operations and keeps systems running smoothly.

This internship has also helped me grow professionally in ways that go beyond technical skills. Many of the tasks I perform require attention to detail, patience, and communication with users who may not be very familiar with technology. I have learned how important it is to explain things clearly and help people understand the systems they rely on every day. I believe the main strengths I bring to my role are organization, reliability, and the ability to work through problems step by step. These are skills that will continue to be valuable as I move forward in my career.

Overall, my experience at MARMC has been extremely valuable for my personal and professional development. It has allowed me to apply concepts from my cybersecurity studies to real situations while gaining experience with enterprise systems, governance practices, and data management. The work can sometimes be challenging, but it is also meaningful because the systems we maintain support the entire command. This internship has helped me gain confidence in my technical abilities and has reinforced my interest in pursuing a career in cybersecurity and information systems.