Keller Beacham

CYSE 368

Spring 2026

Professor Teresa Duvall

TA Joshua Russell

SharePoint Specialist

Reflection #1

Over the course of my internship as a SharePoint Specialist at the Mid-Atlantic Regional Maintenance Center (MARMC), I have gained hands-on experience managing enterprise-level SharePoint environments while supporting a large naval command. My responsibilities have extended beyond basic site maintenance and have included access control, data migration quality assurance, Personally Identifiable Information (PII) auditing, and business intelligence development using Power BI. These experiences have strengthened both my technical skill set and my understanding of information governance, security, and user-focused system design.

One of my primary responsibilities has been maintaining the MARMC SharePoint home site and its associated subpages. This includes cleaning up and managing permissions, ensuring information is current, verifying site functionality, and maintaining a professional and intuitive layout. Strict control of access rosters has been a critical component of this task, as MARMC hosts sensitive operational data that must only be accessible to authorized personnel. In addition to technical maintenance, I have met with civilian content managers to help educate them on SharePoint tools and best practices for web development. These interactions improved my ability

to communicate technical concepts to non-technical users while reinforcing the importance of standardization and governance across enterprise platforms.

Another major responsibility involved shared area permissions control and data management following a large-scale data migration. In September, the SharePoint team migrated approximately 3,239.03 GB of data from legacy shared drives to SharePoint. Since that migration, ongoing quality analysis has been required to resolve access issues, address lost or misplaced data, and correct user errors. A significant portion of my role has involved assisting new personnel with gaining appropriate access to required resources. Recently, Tyler Johnson and I have been responsible for managing access control for users in the C200 department who require PMS Viewer permissions. This experience highlighted the complexity of role-based access control in large organizations and reinforced the importance of accuracy and accountability when managing permissions.

I have also been placed in charge of MARMC's recurring 90-day SharePoint PII audits, which are submitted to PEO Digital. These audits ensure that no unauthorized PII is stored or exposed within SharePoint sites. I recently completed audits of both the Shared Area and the PII Site, verifying compliance and correcting any identified issues. With an upcoming audit approaching, I am currently utilizing a new application to more efficiently identify and sort potential PII across our sites. This responsibility has significantly increased my awareness of compliance requirements, data privacy regulations, and the operational consequences of PII mishandling within government systems.

Most recently, I have begun working with Power BI to support data visualization and decision-making efforts at MARMC. Over the past two weeks, I created a spreadsheet tracking gains and losses for civilians and contractors and transformed this data into interactive Power BI

dashboards displayed on the MARMC main site. Additionally, I am developing a new Power BI and SharePoint page designed to assist new users in tracking their onboarding status within the command. This project has allowed me to combine data analytics with user-centric design while expanding my technical skills in business intelligence tools.

In conclusion, my experience as a SharePoint Specialist at MARMC has been both challenging and rewarding. The responsibilities I have been entrusted with have enhanced my technical proficiency, strengthened my understanding of cybersecurity and data governance principles, and improved my professional communication skills. These experiences directly support my academic goals in cybersecurity and have provided valuable insight into real-world enterprise IT operations within a government environment.