

Jason Carter

June 28, 2026

RFK

Reflection #2

CYSE 368 Internship Reflection Paper 2

The second fifty hours of my internship at RFK Outreach have been both productive and technically demanding, building directly on the groundwork laid during the first half of the experience. My responsibilities have spanned hardware deployment, system security hardening, compliance research, and cybersecurity education — a breadth that has pushed me to apply classroom knowledge in a genuinely operational environment.

A significant portion of this period was devoted to completing the hardware deployment in the Olympus room. The process of refreshing these workstations proved more involved than anticipated: two machines had to be swapped out entirely because their RAM was below the minimum threshold required for the organization's workload, and compatible replacement sticks could not be sourced in time. This required triaging the deployment schedule and prioritizing the machines that could be brought up to standard, which reinforced the importance of asset inventory accuracy and procurement planning in any IT environment.

Once the hardware was stabilized, I shifted focus toward security hardening at the user account level. Specifically, I began testing basic-level user accounts for any unintended privilege escalations — checking whether standard users could access resources, execute binaries, or modify configurations beyond their assigned role. This kind of least-privilege auditing is directly relevant to CMMC Level 1 requirements, which mandate that access to Federal Contract Information be limited to authorized users only. Identifying and remediating privilege

misconfigurations before formal assessment is exactly the type of proactive hardening that positions an organization well for compliance.

Progress on the CMMC compliance front, however, remains gated by infrastructure. The Domain Controller and File Server are still not operational, which blocks the next major phases of the assessment — particularly the access control and configuration management domains that depend on Active Directory being in place. I have continued my independent research on CMMC Level 2 in the meantime, using that time productively to deepen my understanding of the controls that will need to be addressed once the servers come online.

I also took the initiative to gather detailed information about the organization's key fob access logging system. Understanding how physical access events are recorded is relevant to both the audit trail requirements under CMMC and to the broader physical security posture of the facility. Documenting how this system functions — what it logs, how logs are retained, and who has access to them — will be useful when the organization formally addresses the physical protection domain of the framework.

Another issue I identified and escalated was the operating system on the workstation tied to the server room. That machine is currently running Windows 7, which reached end-of-life in January 2020 and no longer receives security updates from Microsoft. I formally recommended upgrading this system to Windows 11 to eliminate a significant attack surface and bring it in line with basic security hygiene. An unpatched workstation physically adjacent to server infrastructure represents a meaningful risk, and addressing it should be a near-term priority.

Finally, I created and rehearsed an offensive security presentation intended for the upcoming Cyber Academy summer camp, which will serve approximately fifty students. This presentation, co-developed with my partner Daniel Cobb, covers foundational offensive security concepts in a

way that is accessible to a student audience while remaining technically grounded. Building this material required synthesizing everything from basic reconnaissance methodology to ethical and legal boundaries around penetration testing — a process that deepened my own understanding even as I worked to make the content clear for others.

In conclusion, the second half of my internship has reinforced that real-world IT and security work rarely proceeds on a linear path. Hardware constraints, infrastructure delays, and legacy system issues all require adaptability and the ability to find productive work within whatever constraints currently exist. I leave this phase of the internship with a stronger grasp of compliance auditing, security hardening methodology, and technical communication — and a clearer picture of how much organizational context shapes what security work actually looks like in practice.