

Jason Carter

June 4, 2026

RFK Solutionz

CYSE 368 — Internship Reflection #1

Reflection Paper #1

The first fifty hours of my internship at RFK Outreach have offered a meaningful introduction to the practical realities of IT infrastructure management and cybersecurity compliance work. Spanning three weeks from May 11 through May 28, 2026, this period has allowed me to move between hands-on hardware tasks, systems administration, and substantive research into compliance frameworks — all within the same organizational environment. The breadth of that experience has been both challenging and instructive, and it has consistently reinforced lessons from my academic coursework in ways that classroom learning alone cannot replicate.

The opening week centered on physical infrastructure. I began by testing hardware for desktops and monitors, identifying and labeling faulty components, and relocating computers to the Genesis location. Learning the building's layout may seem like a minor task in retrospect, but it established a spatial and organizational foundation that made subsequent work significantly more efficient. I also began setting up Windows on workstations and configured the initial receptionist computer for a secondary building. These tasks required attention to detail and a methodical approach — carelessness with hardware identification or setup at this stage would

have created problems that compounded downstream. One key takeaway from this week was the importance of documentation. Labeling faulty hardware systematically, rather than relying on memory, is exactly the kind of operational discipline that separates functional IT environments from chaotic ones.

The second week introduced both greater technical complexity and my first exposure to compliance work. I installed and dual-booted Windows and Linux Mint onto all computers in the Guardian Room — a task that required careful partition management and attention to boot configuration. Working with dual-boot environments reinforced my understanding of how different operating systems interact with hardware at a low level. Alongside this, I began researching the CMMC Level 1 (Cybersecurity Maturity Model Certification) assessment process. This required me to think about scoping: identifying which systems, users, and data flows fall within the assessment boundary. I drafted an initial task list for the assessment and subsequently revised it to ensure each section was accurately labeled according to CMMC practice domains. The iterative nature of that revision — drafting, reviewing, correcting — mirrored professional documentation workflows in ways that felt immediately applicable.

The third and final week of this reporting period was the most intellectually demanding. I worked on drafting initial reports for the CMMC Level 1 analysis while simultaneously running into a significant technical obstacle: the Domain Controller and File Server were both offline. I identified this issue and informed my supervisor, explaining that both systems needed to be operational before I could complete server-side configuration checks and deliver finalized recommendations. Communicating a technical dependency to a supervisor clearly — articulating

not just the problem but why it matters and what it blocks — is a professional skill I found myself exercising more deliberately than I expected to at this stage. In parallel, I tested additional laptops for functionality and expanded my research into CMMC Level 2. I created comprehensive reference notes covering the five asset categories used in L2 scoping, all 110 security requirements across the fourteen CMMC domains, rules governing External Service Providers and cloud service providers, and a phased plan of action for an organization working toward L2 compliance. Moving between L1 and L2 frameworks in the same week made the differences in scope and rigor immediately legible.

Conclusion

These first fifty hours have established a strong foundation for the remainder of my internship. I have gained practical experience in hardware evaluation, OS deployment, and systems documentation, while also developing real familiarity with the CMMC compliance framework at both Level 1 and Level 2. Perhaps more importantly, I have begun to understand the rhythms of professional IT work: the way tasks depend on one another, the necessity of communicating blockers clearly, and the discipline required to produce documentation that others can rely on. I am looking forward to completing the CMMC Level 1 assessment once the Domain Controller and File Server are restored, and to continuing my research into Level 2 requirements as the internship progresses.