

CYSE 368 INTERNSHIP FINAL PAPER

RFK Solutionz

Jason Carter

Supervisor: Jadira and Dr. Frost

Company/Agency: RFK Solutionz

Instructor: Professor Teresa Duvall

Course: CYSE 368

Term: Summer 2026

Date: August 7, 2026

Table of Contents

1. Introduction.....	3
About RFK Solutionz.....	4
Orientation and Initial Impressions	4
2. Management Environment.....	5
3. Major Work Duties, Assignments, and Projects	6
IT Deployment Work	6
CMMC Compliance Research	7
Offensive Security and Presentation Work	8
Cyber Academy Program	8
4. Application of Cybersecurity Skills and Knowledge.....	9
5. Connections to the ODU Curriculum	10
6. Fulfillment of Learning Outcomes.....	11
Outcome 1: Practical CMMC Compliance Experience	11
Outcome 2: Hands-On IT Infrastructure Skills	11
Outcome 3: Applied Security Skills and Presentation Delivery	12
7. Most Motivating and Exciting Aspects.....	12
8. Most Discouraging Aspects	13
9. Most Challenging Aspects	13
10. Recommendations for Future Interns.....	14
11. Conclusion	15
Appendix A: Internship Work Sample Inventory	17

1. Introduction

I decided to pursue my internship with RFK Solutionz because it offered a combination of technical information technology work, cybersecurity compliance research, and opportunities to communicate security concepts to other people. As a cybersecurity major at Old Dominion University, I wanted an internship that would move my learning beyond isolated classroom assignments and laboratory exercises. I wanted to see how cybersecurity decisions are made when there are actual systems, users, operational requirements, and business priorities involved. RFK Solutionz provided that opportunity by allowing me to work with IT deployment tasks, CMMC compliance research, offensive-security-related projects, and the Cyber Academy program.

My internship was also important because I entered it with a particular view of cybersecurity. Before the internship, much of my interest was directed toward technical and offensive-security subjects. I had earned the CompTIA Security+ certification and had developed hands-on familiarity with tools including Nmap, Metasploit, Burp Suite, Wireshark, Nikto, and Hashcat. Those experiences gave me confidence in my ability to learn technical security concepts, but they did not give me a complete understanding of how cybersecurity operates as a professional discipline. In particular, I had limited practical experience with compliance, governance, infrastructure deployment, documentation, and explaining technical material to people who were not cybersecurity students. The internship gave me a chance to broaden that understanding.

At the beginning of the internship, I established learning outcomes through the Memorandum of Agreement associated with the internship. The first objective was to gain practical, supervised experience applying cybersecurity compliance frameworks, particularly CMMC Level 1 and Level 2 requirements, to a real organizational environment. The second objective was to build hands-on information technology infrastructure skills through hardware deployment, workstation configuration, and operating system administration. The third objective was to develop and practice professional security skills, including vulnerability assessment, privilege escalation testing, and security-awareness presentation delivery. These objectives became the framework I used to judge whether the internship was successful.

A fourth, more personal goal developed as the internship progressed. I wanted to use the experience to determine what areas of cybersecurity I wanted to pursue professionally. I had previously been drawn strongly toward offensive security because of my interest in penetration testing, exploitation, and security tools. I had not had enough professional exposure to compliance, infrastructure, education, and broader security operations to know how those areas would fit into my long-term plans. By the end of the internship, that question had become one of the most important outcomes of the experience. The internship changed my cybersecurity career goals by showing me that my professional interests are broader than I had originally assumed.

This paper describes my internship experience at RFK Solutionz and evaluates it against the requirements of CYSE 368. It discusses the organization, orientation and management environment; explains my major duties and why those duties mattered to the business; examines how I applied cybersecurity knowledge and learned new skills; connects the internship to my ODU education; evaluates each learning outcome; and reflects on the most motivating, discouraging, and challenging parts of the experience. It concludes with recommendations for future interns and an assessment of how the internship will influence the remainder of my education and my professional plans.

Overall, the internship met the central purpose I had for it: it gave me an opportunity to experience cybersecurity as a working profession rather than only as an academic subject. Some assignments were more technical than others, and some tasks were delayed by infrastructure problems, but those realities were themselves part of the education. The experience showed me that successful cybersecurity work depends not only on technical knowledge, but also on documentation, communication, patience, adaptability, infrastructure awareness, and the ability to teach or explain concepts to different audiences.

About RFK Solutionz

RFK Solutionz is a cybersecurity and information technology services organization. During my internship, the work I encountered included IT infrastructure deployment, cybersecurity compliance research, security-related technical activities, and educational outreach. A major area of relevance was the Cybersecurity Maturity Model Certification, or CMMC, framework. The organization's work therefore sits at the intersection of technology implementation and security requirements, particularly for environments connected to the Defense Industrial Base.

The materials and experience available to me did not provide a detailed founding history or a complete corporate timeline for RFK Solutionz, so I do not want to invent dates or milestones that I did not personally verify. What I can describe from my internship is the practical role of the organization. RFK Solutionz operates in a setting where organizations need reliable technology, secure systems, and an understanding of cybersecurity requirements. That combination made the internship particularly useful because my assignments were connected to both the technical and administrative sides of cybersecurity.

One notable part of the organization was its Cyber Academy program. During my internship, RFK Solutionz hosted a week-long Cyber Academy program from August 3 through August 7, 2026, involving approximately fifty students. The program used interactive and game-based activities to introduce younger students to foundational cybersecurity ideas. This outreach work demonstrated that the organization's activities were not limited to technical services. It also involved workforce development, education, and community engagement.

The variety of work also meant that the organization served different types of audiences. Technical tasks were relevant to the organization's internal infrastructure and client-facing capabilities. Compliance research was relevant to organizations that need to understand and meet cybersecurity requirements. Educational activities were designed for students who were not yet cybersecurity professionals. Working across these different audiences helped me understand that cybersecurity professionals must be able to change the way they communicate depending on who is receiving the information.

Orientation and Initial Impressions

My initial orientation introduced me to the expectations of the internship and to the types of work I would be completing. Jadira served as my direct supervisor and became the primary person responsible for helping me understand assignments, reviewing my work, and providing direction when I needed clarification. The beginning of the internship was a transition from the predictable structure of university assignments to a setting where tasks could depend on the condition of real systems and the priorities of the organization.

One of my first impressions was that the internship would require me to be more adaptable than I had expected. In school, an assignment normally has a defined start point, a set of requirements,

and a deadline. At an internship, a task can be affected by equipment availability, system outages, changing priorities, or the need to coordinate with other people. I experienced this directly when the Domain Controller and File Server experienced recurring problems that affected my CMMC Level 1 assessment work. Instead of treating the interruption as simply an inconvenience, I began to understand it as part of the environment in which professional cybersecurity work occurs.

I also quickly recognized that my existing technical knowledge was useful but incomplete. My familiarity with security tools gave me confidence when dealing with offensive-security-related work, but CMMC research required a different kind of discipline. I had to read requirements carefully, organize information, understand scope, and maintain documentation. The internship therefore challenged me to become comfortable with work that did not always produce an immediate technical result. A well-organized compliance document or work log may not feel as exciting as running a security tool, but it can be equally important to an organization.

Another early impression was that professional cybersecurity includes a significant communication component. I expected to spend most of my time working with systems and security concepts. Instead, I eventually had to explain security ideas through presentations and teach activities to a class of younger students. That experience became especially important later because I discovered that knowing cybersecurity and teaching cybersecurity are two different skills. I could understand a concept technically and still need to change my explanation, examples, pacing, and expectations in order for another person to understand it.

2. Management Environment

My direct supervisor throughout the internship was Jadira. She was responsible for assigning or directing my day-to-day work, reviewing my compliance research, and providing feedback on my technical and professional activities. The management environment required me to take responsibility for completing assignments while also being willing to ask questions when I encountered something unfamiliar. This balance was important because the internship was designed as a learning experience, but the work still had to be useful to the organization.

One of the most valuable parts of the supervisory relationship was the opportunity to work independently without being completely disconnected from supervision. Many internship assignments required me to research a subject, organize my findings, and develop something that could be reviewed. This encouraged me to develop professional judgment rather than simply wait for instructions for every individual step. At the same time, having a supervisor available meant that I could receive direction when an issue went beyond my current knowledge.

The management structure also demonstrated why communication is important in cybersecurity. A cybersecurity assignment may appear straightforward from the outside, but its completion can depend on people responsible for infrastructure, systems, documentation, or scheduling. The recurring Domain Controller and File Server problems were a good example. My CMMC assessment work depended on systems being available and functioning. The situation reinforced the idea that cybersecurity management involves coordinating technical priorities with operational realities.

I generally found the management environment effective for an internship because I was given meaningful assignments rather than being limited to observation. The work allowed me to build artifacts, perform research, participate in technical activities, and support the Cyber Academy. At

the same time, the environment was realistic enough that not every task progressed exactly as planned. This made the management experience educational because I had to learn how to adjust rather than assuming every assignment would proceed without interruption.

The management environment also encouraged professional accountability. Keeping an ongoing work log was especially useful. Because some of my work involved research that continued across multiple sessions, documenting what I had completed helped preserve continuity. It also made it easier to explain progress and identify what remained unfinished. This was an important professional lesson because cybersecurity work often involves investigations, compliance projects, and long-term improvements that cannot be summarized accurately from memory alone.

3. Major Work Duties, Assignments, and Projects

My responsibilities at RFK Solutionz covered several areas, but they can be grouped into four major categories: IT deployment work, CMMC compliance research, offensive-security and presentation work, and participation in the Cyber Academy program. These assignments were different from one another, but together they gave me a more complete view of cybersecurity. The IT work showed me the infrastructure foundation. The compliance work showed me how organizations document and evaluate security. The offensive-security work showed me the adversarial perspective. The Cyber Academy work showed me the importance of communication and education.

Each assignment was necessary in a different way. Technical deployment work supported reliable operations. Compliance research supported organizational readiness and the ability to demonstrate that security requirements were being addressed. Security testing helped identify weaknesses and realistic attack paths. Educational activities supported outreach and workforce development. Understanding the purpose behind each assignment helped me avoid viewing internship tasks as isolated school exercises.

IT Deployment Work

A significant portion of my early internship hours involved IT deployment tasks, including hardware setup, workstation deployment, and operating system configuration. This work gave me practical experience with the infrastructure that cybersecurity depends on. In academic environments, it is easy to focus on the security layer and overlook the physical and administrative work required before a system can be secured. At RFK Solutionz, I saw that a security program begins with knowing what systems exist, configuring those systems correctly, and maintaining them in a usable condition.

Workstation deployment is necessary because poorly configured endpoints can create operational and security problems. A workstation has to function for the user, but it also has to fit within the organization's security expectations. Operating system configuration affects patching, support, security features, compatibility, and the ability to maintain a consistent environment. My work researching an operating system upgrade recommendation required me to think beyond the question of whether a newer operating system was technically available. I had to consider support lifecycle, compatibility, security implications, and the practical effect of an upgrade.

That experience helped me understand the relationship between IT administration and cybersecurity. An operating system decision can affect security for years. A system that is no

longer supported can create risk even if the user behaves responsibly. Conversely, upgrading immediately may create compatibility or operational problems. Cybersecurity professionals therefore need enough IT knowledge to understand the systems they are trying to protect.

The deployment work also reinforced the importance of process. Physical setup, configuration, and troubleshooting may not be the most visible cybersecurity activities, but they create the foundation for security controls. Monitoring, patching, access control, and compliance cannot be implemented effectively if the underlying systems are unknown, unstable, or incorrectly configured. This was one of the first places where the internship expanded my understanding of what it means to work in cybersecurity.

CMMC Compliance Research

The core of my internship work centered on CMMC Level 1 and Level 2 compliance research. I built and maintained structured notes in Obsidian covering scoping methodology, External Service Provider and cloud service provider considerations, individual domain requirements, and a six-phase compliance action plan. I also maintained an ongoing work log. This work was necessary because compliance requires more than simply knowing that security controls exist. An organization needs to understand which requirements apply, what evidence is needed, what gaps exist, and what sequence of actions makes sense.

One of the most important lessons from the compliance work was the importance of scope. Before an organization can meaningfully evaluate compliance, it needs to understand what systems, services, people, and data are included in the environment being assessed. The work surrounding external service providers and cloud services reinforced the idea that an organization's security boundary can be affected by services it does not physically own or operate. This was an area where I had to develop knowledge through research rather than rely only on previous coursework.

The six-phase compliance action plan was another important assignment. The purpose of the plan was to translate a large set of requirements into a sequence that could realistically be addressed. This required prioritization. An organization cannot treat every requirement as an isolated checkbox without considering dependencies between controls. Foundational access, configuration, and system-management practices can influence the ability to implement more advanced monitoring and response capabilities. Building the plan taught me to think about compliance as a project rather than a list.

The work log became equally important. Compliance research does not always result in a dramatic finished product at the end of a single work session. Progress can consist of understanding a requirement, clarifying scope, identifying a dependency, documenting a question, or updating an action plan. Without documentation, those steps can be difficult to demonstrate. Maintaining organized notes therefore became part of the deliverable rather than something separate from the work.

The Domain Controller and File Server outage was the clearest example of the relationship between infrastructure and compliance. The recurring outage became a blocker to completing the CMMC Level 1 assessment. This was discouraging because I wanted to see the assessment progress, but it was also educational. The situation showed me that compliance projects do not exist in a vacuum. A requirement may be straightforward on paper while its practical evaluation depends on whether the underlying systems are available and functioning.

The experience also changed how I think about compliance professionals. Before the internship, I was more likely to view compliance as a governance-oriented specialty separate from technical cybersecurity. After the internship, I see it as a role that requires enough technical understanding to recognize dependencies and enough organizational awareness to document and prioritize them. The best compliance work cannot ignore the condition of the technology it is evaluating.

Offensive Security and Presentation Work

I also co-developed an offensive security presentation with Daniel Cobb. The presentation included a Capture the Flag challenge component. This assignment allowed me to use knowledge that was closer to the offensive-security work I had practiced before the internship. Designing a CTF required thinking about how a participant would approach a problem, what clues would be available, and what technical concept the challenge was intended to demonstrate.

The CTF work reinforced the value of hands-on learning. When a security concept is presented only as a definition, it can be easy to recognize the words without fully understanding the process. Building a challenge requires a deeper level of understanding because the creator has to anticipate how someone will interact with the problem. This made me examine the same security concepts from both the attacker's and the educator's perspectives.

My internship also included privilege escalation testing and research into physical access control systems. Privilege escalation testing was relevant because it allowed me to think about what could happen after an attacker gained an initial foothold. Instead of stopping at the question of whether a vulnerability exists, the exercise encouraged consideration of what additional access could be achieved and what that access would mean for the environment.

The physical access control research expanded my understanding in a different direction. Cybersecurity is often discussed in terms of networks, endpoints, applications, and accounts, but physical access can undermine technical controls. If an unauthorized person can physically reach systems or restricted areas, many logical protections become less effective. Researching physical access therefore helped me see security as a broader system of controls rather than a collection of software settings.

Cyber Academy Program

Later in the internship, I helped plan interactive, game-based activities for RFK Solutionz's Cyber Academy program. The program ran during August 3–7, 2026, and involved approximately fifty students. I selected and scheduled ten activities across two thematic days. This assignment was different from my technical work because the audience was made up of younger students rather than cybersecurity professionals or university students.

The Cyber Academy was important to the organization because it supported community outreach, education, and workforce development. It also challenged me to communicate cybersecurity concepts in a way that was understandable and interesting to students. A technical explanation that works for a college cybersecurity class would not automatically work for a group of small children. I had to think about attention span, instructions, pacing, interaction, and the difference between explaining a concept and helping someone experience it.

One of the biggest lessons from the program was that teaching is a cybersecurity skill when the goal is security awareness. A cybersecurity professional may know how authentication, phishing, passwords, or access control work, but if that professional cannot explain those concepts to a

nontechnical audience, some of the knowledge has limited practical value. The Cyber Academy gave me direct experience with that communication problem.

The experience also required me to take ownership. At one point, I had to teach an entire class on my own. Teaching a full class of small children was one of the most challenging responsibilities I had during the internship because I could not rely on another instructor to carry the lesson if students became distracted or confused. I had to manage the activity, explain instructions, respond to questions, keep students engaged, and make adjustments while the class was happening. This was very different from presenting information to adults or classmates.

4. Application of Cybersecurity Skills and Knowledge

I entered the internship with a foundation that included my CompTIA Security+ certification and hands-on familiarity with Nmap, Metasploit, Burp Suite, Wireshark, Nikto, and Hashcat. These tools represent several areas of security knowledge: network reconnaissance, exploitation, web application testing, traffic analysis, web server scanning, and password auditing. The skills associated with those tools gave me a baseline that I could draw upon during privilege escalation testing, the offensive security presentation, and the CTF challenge.

My previous experience also gave me an understanding of the importance of thinking like an attacker. Reconnaissance, enumeration, identifying weaknesses, and considering possible attack paths were concepts I had already encountered. The internship helped me connect those ideas to a real organization rather than treating them only as exercises. I became more aware that the purpose of offensive security is not simply to demonstrate that something can be broken. The purpose is to produce information that can help an organization make better security decisions.

At the same time, I had to learn a substantial amount on the job. My previous learning had been weighted toward offensive security and general security principles, while CMMC compliance was much less familiar. I had to learn scoping methodology, Level 1 and Level 2 requirements, external service provider considerations, cloud service provider considerations, and the process of organizing a compliance action plan. This was a significant expansion of my cybersecurity knowledge.

The internship also required me to learn more about IT administration. Hardware setup, workstation deployment, operating system configuration, and troubleshooting are not always emphasized when cybersecurity is taught primarily through security concepts. I learned that cybersecurity professionals benefit from understanding what administrators actually have to do to keep systems operational. Security controls must work within an environment that has users, software dependencies, hardware limitations, and uptime requirements.

Another new skill was teaching. I had not expected teaching small children to become one of the strongest learning experiences of my internship, but it did. Teaching an entire class on my own required me to translate technical ideas into simple language and to react to the students instead of simply reading from prepared material. If students were confused, I had to change the explanation. If they lost attention, I had to change the activity or pacing. This was a completely different form of problem-solving.

The internship changed my understanding of cybersecurity because it showed me that technical knowledge is only one part of professional competence. I still value technical security skills, and the internship reinforced my interest in them, but I now understand the importance of

compliance, infrastructure, communication, and education. Cybersecurity is an ecosystem. A vulnerability, a misconfigured workstation, an unclear policy, a weak physical control, an incomplete compliance document, and an employee who does not understand security awareness can all become part of the same risk picture.

The CMMC work was particularly influential in changing my perspective. Before the internship, I could understand a security requirement as an individual control. During the internship, I had to think about how requirements fit together, how scope affects the assessment, how infrastructure availability affects evidence gathering, and how an organization can realistically prioritize improvements. This transformed compliance from an abstract subject into an operational activity.

5. Connections to the ODU Curriculum

My coursework at Old Dominion University provided an important foundation for the internship, although the experience also exposed areas that my coursework had not yet covered in depth. The strongest connections came from courses and independent study that had already developed my understanding of security principles, cryptography, network behavior, and offensive-security techniques.

My cryptography coursework was especially useful for reinforcing the importance of understanding the technical foundations behind security controls. The course covered elliptic curve cryptography, including ECC foundations, point addition, and Elliptic Curve Diffie-Hellman key exchange. It also covered $GF(2^8)$ arithmetic, AES, DES, RSA, block cipher modes, and number theory. Although I did not spend the internship performing mathematical cryptography calculations, the course gave me a stronger understanding of why encryption choices matter and why cybersecurity professionals need to understand the mechanisms behind the controls they discuss.

More broadly, my ODU education helped me understand concepts such as access control, authentication, network security, vulnerability, risk, and security architecture. Those concepts were reinforced when I worked on CMMC requirements and when I thought about privilege escalation. A classroom environment can demonstrate how a control should work. The internship demonstrated what happens when that control has to exist in an actual environment with systems and operational dependencies.

My experience with Nmap, Metasploit, Burp Suite, Wireshark, Nikto, and Hashcat also connected to the technical foundation I had developed through coursework and independent study. During the offensive-security presentation and CTF work, I was able to draw upon the same categories of thinking that I had practiced in security labs. The difference was that the internship required me to think about the purpose and audience of the work, not just whether I could successfully execute a technical procedure.

The internship also revealed important gaps. CMMC scoping methodology and the practical treatment of external service providers and cloud service providers were not areas I had previously studied at the same level. I had to learn them through direct research and documentation. The six-phase compliance action plan also introduced me to a more project-oriented way of thinking about security improvements.

The IT deployment work exposed another gap. University cybersecurity courses can provide strong technical foundations without requiring students to spend extensive time physically deploying and configuring workstations. At RFK Solutionz, I learned that endpoint configuration and operating system decisions can have security and compliance consequences. This made me appreciate the value of developing stronger system administration skills alongside cybersecurity knowledge.

The Cyber Academy work revealed perhaps the most personal gap in my preparation: teaching. My university coursework had prepared me to learn and explain cybersecurity concepts at a college level, but it had not prepared me to teach a full class of small children by myself. That experience showed me that communication is not a single skill. Communicating with classmates, coworkers, managers, clients, and children requires different approaches. The ability to adjust communication is something I will continue to develop.

Overall, I would describe the relationship between ODU and the internship as complementary. ODU provided the theoretical and technical foundation that allowed me to understand what I was seeing. RFK Solutionz provided the context that showed me how those concepts operate in practice. The internship did not replace classroom learning; it made the classroom learning more meaningful by showing me where it fits.

6. Fulfillment of Learning Outcomes

Each of the three learning outcomes established through my internship agreement was addressed during the experience. Some were fulfilled more completely than others, and some were complicated by circumstances outside my control. Evaluating them individually gives a clearer picture of what I actually gained.

Outcome 1: Practical CMMC Compliance Experience

The first outcome was to gain practical, supervised experience applying CMMC Level 1 and Level 2 requirements to a real environment. I consider this outcome substantially fulfilled. I researched CMMC requirements, organized information about scoping, external service providers and cloud service providers, documented domain requirements, developed a six-phase compliance action plan, and maintained a work log.

The outcome was not fulfilled in the sense of completing every possible assessment activity without interruption. The recurring Domain Controller and File Server problems limited the progress that could be made on the CMMC Level 1 assessment. However, I believe that limitation actually strengthened my practical understanding. I learned that compliance work is dependent on infrastructure and that project timelines can be affected by technical problems. I therefore left the internship with a more realistic understanding of compliance than I would have gained from an uninterrupted classroom exercise.

Outcome 2: Hands-On IT Infrastructure Skills

The second outcome was to build practical IT infrastructure skills. This outcome was fulfilled through hardware setup, workstation deployment, operating system configuration, and research supporting an operating system upgrade recommendation. These activities gave me direct experience with the technical foundation on which cybersecurity controls operate.

The most important part of this outcome was learning to connect IT decisions to security consequences. An operating system is not just a platform for applications. Its support lifecycle, configuration, patching capabilities, and security features affect the organization's risk. This experience made me more interested in continuing to develop system administration skills because I now see them as an important complement to cybersecurity.

Outcome 3: Applied Security Skills and Presentation Delivery

The third outcome was to develop professional security skills through vulnerability assessment, privilege escalation testing, and security-awareness presentation delivery. This outcome was fulfilled through privilege escalation testing, physical access control research, the offensive security presentation and CTF challenge developed with Daniel Cobb, and the Cyber Academy activities.

The Cyber Academy expanded this outcome beyond what I originally expected. I learned that presenting to a cybersecurity audience and teaching small children require different abilities. When I taught an entire class on my own, I had to be responsible for both the technical content and the learning environment. That experience strengthened my communication, adaptability, and confidence.

Taken together, the three outcomes gave me a much broader cybersecurity skill set. I developed technical experience, compliance knowledge, infrastructure awareness, and communication skills. Just as importantly, the internship helped me understand which areas I want to continue exploring after graduation.

7. Most Motivating and Exciting Aspects

The most motivating part of the internship was the variety of work. I did not spend the entire internship performing one repetitive task. I was able to move between IT deployment, CMMC research, offensive security, physical access research, presentations, and educational programming. That variety kept the experience interesting and helped me discover strengths and interests that I would not have recognized through a single type of assignment.

The offensive security presentation and CTF were especially exciting because they connected closely with the technical interests I already had. I enjoyed the challenge of thinking about how someone would approach a problem and how to design an activity that would teach a security concept. The project allowed me to use technical knowledge creatively rather than only following a procedure.

The CMMC research was motivating for a different reason. At first, compliance work was outside the area I was most comfortable with. As I learned more, however, I began to appreciate the complexity of turning requirements into an actionable plan. Understanding scope, documenting requirements, and organizing an action plan required a different kind of problem-solving than running a security tool. I found satisfaction in seeing a large set of requirements become more understandable and manageable through organization.

The Cyber Academy was also a major source of motivation. Teaching younger students showed me that cybersecurity knowledge can have an impact even when the audience is not preparing for a technical career. Helping students interact with cybersecurity concepts made the subject feel more connected to the real world. It also gave me a confidence boost because I had to take responsibility for an entire class and make the material work in real time.

Most importantly, the internship was motivating because it helped answer questions about my future. I entered the internship thinking of cybersecurity career planning primarily in terms of technical security roles. I left with a broader view. I am now more interested in considering careers that combine cybersecurity with compliance, governance, infrastructure, security education, and other areas where technical knowledge and communication intersect.

8. Most Discouraging Aspects

The most discouraging part of the internship was having technical problems interfere with work that I wanted to complete. The recurring Domain Controller and File Server outage affected the CMMC Level 1 assessment and made it difficult to move forward at the pace I wanted. When I had already invested time researching requirements and organizing the assessment process, being unable to continue because of infrastructure availability was frustrating.

The situation also taught me an important lesson about professional patience. In a school assignment, I can generally control when I begin and how I complete the work. In an organization, some dependencies are outside my control. The correct response is not to pretend that the problem does not exist or to work around it in a way that produces inaccurate results. The correct response is to document the limitation, communicate it, continue useful work where possible, and return to the blocked task when the dependency is resolved.

Another discouraging aspect was realizing that some cybersecurity work is less immediately exciting than I expected. Researching requirements and maintaining documentation can feel slow compared with technical testing. However, I came to understand that the slower work has value. Security programs depend on documentation, evidence, and repeatable processes. The experience changed my definition of productive cybersecurity work.

The challenge of teaching also included moments that were discouraging. When teaching a class of small children, it is possible for students to lose focus quickly or to interpret instructions differently than expected. I had to recognize that an explanation that seemed clear to me might not be clear to them. That could be frustrating in the moment, but it forced me to become more flexible.

Overall, the discouraging experiences were useful because they exposed me to realities that cannot be simulated perfectly in a classroom. Delays, dependencies, communication problems, and differences in audience are normal parts of professional work. Learning how to handle them is part of becoming employable, not something separate from cybersecurity skill.

9. Most Challenging Aspects

The most challenging aspect of the internship was learning how to teach small children. I had to teach an entire class on my own, which required me to take responsibility for the lesson from beginning to end. This was difficult because I could not assume that the students already understood cybersecurity vocabulary or had the same level of attention as college students. I had to simplify explanations without making them inaccurate and keep the class moving while still responding to questions.

Teaching also required a different kind of confidence. When performing a technical task, I can focus on the system and troubleshoot if something goes wrong. When teaching, the people in front of me are constantly providing feedback through their questions, attention, and behavior. If

they are confused, I have to adjust. If they are disengaged, I have to change the way I am presenting. This made teaching a more dynamic problem than I expected.

The CMMC learning curve was another major challenge. I had to become comfortable with terminology, scoping concepts, service-provider considerations, and requirements that were not central to my previous cybersecurity experience. The difficulty was not simply memorizing requirements. I had to understand how they related to an organization's environment and how they could be turned into a practical plan.

Balancing different kinds of work was also challenging. IT deployment, compliance research, offensive security, and Cyber Academy planning require different mindsets. Technical deployment requires attention to configuration details. Compliance requires organization and careful interpretation. Offensive security requires adversarial thinking. Teaching requires communication and adaptability. Switching among those modes forced me to become more organized and deliberate.

The challenges ultimately made the internship more valuable. If every task had been identical to something I had already done in school, I would have gained experience but not necessarily growth. The most difficult tasks were the ones that forced me to develop abilities I did not know I needed, especially teaching, communication, and compliance analysis.

10. Recommendations for Future Interns

Based on my experience, I would recommend that future interns prepare for RFK Solutionz by developing both technical and professional skills. The internship is broad enough that a student who expects only penetration testing or only compliance work may be surprised by the variety of assignments.

- Build a baseline understanding of CMMC before starting. Students should understand the basic difference between Level 1 and Level 2 and should become familiar with the ideas of scope, external service providers, and cloud service providers. A basic vocabulary will make the research process much easier.
- Be comfortable with basic IT administration. Students should know how to work with operating systems, configure workstations, troubleshoot basic problems, and understand the relationship between endpoints and security controls.
- Maintain organized notes from the first day. I used Obsidian to organize CMMC research, requirements, scoping information, action-plan material, and my work log. A structured system prevents information from becoming scattered.
- Do not assume every assignment will go according to schedule. Infrastructure problems can delay cybersecurity work. Future interns should be prepared to document blockers and identify other productive work that can be completed while waiting.
- Practice explaining cybersecurity to people who are not cybersecurity students. The Cyber Academy experience showed me how different teaching can be from knowing the material. Future interns should practice simplifying concepts, giving clear instructions, and responding to questions.
- Develop communication skills along with technical skills. Presentations, status updates, documentation, and teaching are all professional cybersecurity activities.
- Come prepared to learn outside your preferred specialty. A student who is primarily interested in offensive security should still be willing to learn compliance and IT

administration. A student interested in compliance should still develop enough technical understanding to recognize infrastructure dependencies.

- Take ownership of assignments. Research the problem, organize your findings, attempt reasonable solutions, and then ask focused questions when you need help. This approach creates more learning than waiting for every next step to be provided.

The most important recommendation I would give future interns is to treat the internship as an opportunity to discover what they do not yet know. It is easy to focus on proving that you already have skills. A better goal is to identify gaps and deliberately use the internship to close them. My biggest areas of growth came from assignments that were outside my comfort zone, especially compliance research and teaching.

11. Conclusion

My internship at RFK Solutionz gave me practical exposure to several different sides of cybersecurity and changed my understanding of what a cybersecurity career can look like. I gained experience with IT infrastructure deployment, CMMC compliance research, privilege escalation testing, physical access control research, offensive-security presentation development, CTF activities, and cybersecurity education. These responsibilities were different, but together they showed me how interconnected cybersecurity functions are.

The most important take-away from the internship is that cybersecurity and IT infrastructure cannot be treated as completely separate disciplines. Security controls depend on the systems being configured, maintained, and available. Compliance assessments depend on infrastructure and evidence. Security testing depends on understanding how systems actually operate. The Domain Controller and File Server outage made this connection especially clear because it demonstrated how an infrastructure problem could directly prevent compliance work from progressing.

The internship also changed my understanding of communication. Before the experience, I thought of communication mainly as presenting technical information to classmates or coworkers. Teaching an entire class of small children forced me to think about communication as a skill that must be adapted to the audience. I learned that a technically correct explanation is not automatically an effective explanation. This lesson will be useful regardless of which cybersecurity specialty I ultimately pursue.

The experience will influence the remainder of my time at Old Dominion University by encouraging me to broaden my education beyond offensive-security interests. I want to continue strengthening my technical foundation while also developing knowledge of compliance, governance, system administration, and security communication. The internship showed me that these subjects are not distractions from cybersecurity; they are parts of cybersecurity that can make a technical professional more effective.

Most significantly, the internship changed my cybersecurity career goals. I entered the internship with a stronger assumption that my future would be centered primarily on offensive security. I still value offensive-security skills and want to maintain them, but I now see myself considering a wider range of professional paths. Compliance and cybersecurity governance became more understandable and more interesting after I worked with CMMC requirements. IT administration became more relevant after I experienced the infrastructure side of security. Education and communication became more important after the Cyber Academy.

This change does not mean that I have abandoned technical cybersecurity. Instead, I now want a career path that allows me to combine technical knowledge with broader security responsibilities. I am more open to roles involving security assessment, compliance, governance, infrastructure security, security awareness, or positions that require movement between technical and organizational perspectives. The internship gave me evidence about what kind of work I enjoy rather than forcing me to choose a career based only on assumptions.

Finally, the internship taught me that professional growth often comes from unexpected assignments. I expected technical work to be the main source of growth, but one of the most important experiences was teaching children. I expected compliance to be less interesting than offensive security, but CMMC research taught me how security requirements become organizational plans. I expected infrastructure tasks to be separate from cybersecurity, but system availability became directly relevant to compliance. These experiences changed my assumptions.

For those reasons, I consider the internship a successful part of my education. It helped me apply what I had learned at ODU, identify areas where I needed additional knowledge, develop practical skills, and make a more informed decision about my professional future. The experience will influence how I approach the remainder of college and how I evaluate cybersecurity opportunities after graduation. More than anything, it showed me that cybersecurity is much broader than any single tool, class, certification, or job title. My goal moving forward is to use the technical foundation I already have while continuing to develop the communication, infrastructure, compliance, and problem-solving skills that I learned were equally important during my time at RFK Solutionz.

Appendix A: Internship Work Sample Inventory

The following work products were part of the internship experience and may be included as supporting materials if permitted by RFK Solutionz and the course requirements. Any confidential client information, credentials, system information, or other sensitive material should be removed before submission.

- CMMC Level 1 and Level 2 research notes and scoping documentation maintained in Obsidian.
- Six-phase CMMC compliance action plan.
- Internship work log documenting research and project progress.
- Operating system upgrade recommendation.
- Offensive security presentation developed with Daniel Cobb.
- Capture the Flag challenge associated with the offensive security presentation.
- Physical access control research.
- Cyber Academy activity schedule and game-based activity planning materials.