CYSE 368 INTERNSHIP

BY: BRYANT WATKINS

AUGUST 4, 2025

VIRGINIA DEPT OF STATE POLICE

SUMMER 2025

Table of Contents

Introduction

The journey to obtaining this opportunity with the Virginia Department of State Police was by no means an easy one. While looking for work in the summer of 2023 – a friend of mine referred me to an entry level data center position through an information technology staffing agency known as TEKsystems. I was fortunate to be able to receive a contract offer that was designed to last three months, and this was very short but the path it would create for me was incredibly valuable. In my time there I excelled and learned a lot in networking and telecommunication processes. My time eventually came to an end sadly following the three months.

Once again looking for work – TEKsystems once again granted me a new opportunity as a contractor with the Virginia Department of State Police. I was tasked with installing and programming the telecommunication devices found in the fleet vehicles. This was an exciting opportunity for me that gave me a glimpse first-hand of the environment of this employer. I once again excelled in my role, receiving high marks from many in upper management on my swift learning and performance. Unfortunately, my time came to an end once again as the contract concluded.

This was only the beginning, however. In the last weeks in my contractor role, I observed a job posting for a direct role with the Virginia Department of State Police. I quickly submitted my resume, and weeks later I would go on to interview for said role. I performed well during the intensive interview, and the high marks I received from management during my time as a contractor only further added prestige. Weeks following the interview, I finally received the call of which I had dreamed. I was officially presented a direct-hire role with the Virginia Department

of State Police, and thus I felt that my pathway to a cybersecurity career had finally begun with this opportunity.

Already being accustomed to the environment of the Virginia Department of State Police – I knew that this was the place for me. This is an organization that has been around for nearly a century, as they were founded in 1932. They have arguably the most expansive networking and cybersecurity infrastructure in the Commonwealth of Virginia. I also knew that many of the information technology employees are amongst the most skilled and experienced in the Commonwealth. I found a combination of these factors to be perfect for fostering a learning environment that would teach me the necessary skills for a future in cybersecurity.

Many obviously associate law enforcements with the Virginia Department of State Police, but there is an entire division dedicated to information technology services as well. The system that my position manages is known as STARS – Statewide Agencies Radio Systems. The STARS program ensures the functioning of communications, and with this comes a vast network of devices and infrastructure that facilitate this. This expansive information technology infrastructure entails programming along with many cybersecurity measures. My role oversees these programming and cybersecurity tasks.

As my role began, I participated in an orientation that was conducted through Zoom. There is no initial training, as the entirety of the role entails continuous training exercises. My initial impressions of this company are that there is a strong sense of structure as well as collaboration. I also quickly noticed a culture of professionalism that I found to be very impressive and inspiring. The prevalence of security measures at every turn, from authentication and authorization methods to alarms, was incredibly noticeable. I felt as though I have finally

found a place to cultivate my skills and expand upon them as well as my knowledge pertaining to networking and cybersecurity.

From the very beginning, I worked with my supervisor to craft at least three attainable goals for myself in this role. The first goal was to establish firm understanding of the software programming of telecommunication devices. The second goal was to Gain operational insight on the Information Technology hardware and the processes that they provide for the Virginia State Police. The third goal was to Establish firm understanding of alarm security installation and troubleshooting. We felt that these goals would help to advance my knowledge in networking as well as cybersecurity.

Management Environment

While in this role, the management environment was one that was completely conducive to accelerating my learning. My supervisor is by my side for many of the new tasks that I participate in, often there to provide extensive coaching as well as to directly observe my performance in certain areas. Every month of my employment also entails the filing of performance indicator forms; these forms oversee my accomplishments as well as certain areas needing improvement. These forms are essentially a performance review with any relevant constructive criticism, and they prove incredibly beneficial as I can receive input from my supervisor and adjust my performance as necessary.

The management structure also establishes a chain of command, as my direct supervisor has supervisor he answers to. His supervisor then answers to the information technology department supervisor who then answers to the division captain at the top of the hierarchy. I enjoy the structure; I engage with all levels, and no level is beyond providing direction or

assistance for me. There have been times when I have been teamed up with both my direct supervisor and his, and both have provided me with hands-on experience and passed on their expertise.

Major Work Assignments, Duties, Projects

Upon my entry into this internship opportunity, I was immediately thrust into major assignments spanning the entire commonwealth of Virginia. My team was tasked with installing power inverter devices for 48V DC plants across all Virginia Department of State Police sites. The installation process entails the programming of the device software as well as the setting of alarms. I was specifically tasked with the alarm setup and software programming aspect of this major project. This task provided me with an immediate opportunity to establish hands-on experience with networking software and security alarms.

The Virginia Department of State Police has a cybersecurity alarm system across all sites that is established through direct device connection to phone punch-down blocks. These connections are established through the use of cat 5e cables, as these cables enable the transmission of signal. The inverter devices installed required this same process, and I was tasked with doing so. Establishing the cable connection was only the first step in the alarm setting process, however.

The installation of the alarms also entailed direct collaboration with the network operating center to have the alarms properly assigned to identifying numbers. The network operating center is a team that we must collaborate with to ensure that the entire communications department is made aware of the establishment of any new alarms. The identifying numbers for the alarms in question refers to both the phone punch-down as well as a Motorola MOSCAD

SDM 3000 Remote Terminal Unit device. There was an establishment of both “major” and “minor” alarms for the inverter devices, and both alarms were identified on the phone punch-down blocks as well as the MOSCAD devices.

The Motorola MOSCAD devices were the critical backbone of the cybersecurity alarm system. These devices visually display lights pertaining to every alarmed device at the site. They also play a critical role in data collection and remote monitoring capabilities. The remote monitoring capabilities enable the communications team to remotely monitor the alarm status of any device. Considering the vast number of sites and locations, including many of which are extremely difficult to travel directly to, remote monitoring of alarms is an important operation necessary to the cybersecurity of Virginia Department of State Police networking devices.

Another major duty of mine was to then program the software for these inverter devices. Communication with these devices requires a direct ethernet cable connection. Inserting an ethernet cable was the first step, as I then would need to alter the internet protocol address of my laptop to ensure that it was within the internet protocol range of the device in question. Every inverter device we installed was already assigned default internet protocol addresses. Once I ensured that my laptop was within range and connected, I proceeded to enter the device’s address into a web browser’s address bar. Undertaking these steps finally allowed me direct access to the inverter device’s software.

Once the software was accessed, I was specifically tasked with altering the default internet protocol address as well as the setting of a password. Each site had preassigned addresses and passwords that pertain to its location. Establishing a new address allows the device to be remotely monitored and altered as needed through the use of Command Prompt. The default passwords for these devices were very generic and simplistic, so it was imperative that I

changed them to more complex passwords that would prove to be much more difficult conduct any attack against – such as dictionary, rainbow, brute force, etc. Overall, programming these inverter devices was the last critical step in the installation process for this project. I was able to successfully set alarms, program device software, and manage passwords at dozens of sites for this project.

All of my completed tasks were incredibly necessary to the operations of Virginia Department of State Police. Setting alarms establishes a first line of defense for State Police communication devices. The alarms I set are not only for alerting the communications team to attempted tampering, but the alarms also notify the communications team to any operational issues that arise with the inverter device. The Virginia Department of State Police must be aware of any issues that arise, as these devices are critical to the establishment of statewide communications.

My programming of the inverter devices' software was also a task that proves necessary to successful operations for the State Police. These inverter devices are preassigned default values upon first installation. It was imperative that I programmed these devices, which included establishing a new internet protocol address. Setting a new internet protocol address is what allows the State Police communications team to communicate directly with these devices remotely through Command Prompt and further conduct any changes or observe data as necessary. Without establishing the new address, the State Police would have no way to remotely monitor or alter the software to these devices.

My management of the inverter devices' passwords may prove to be the most necessary task for State Police operations. Password management is an enormous pillar of all thing cybersecurity related. The State Police cannot possibly establish a robust cybersecurity system

without having strong and complex passwords that enforce the security for many of their devices. There is a plethora of password cracking methods found amongst the bad actor community. Had I failed to establish proper password management for these devices, then the State Police would find their operations to be incredibly susceptible to many of these attacks that could prove devastating to their cyber infrastructure and communications abilities needed across the commonwealth.

Cybersecurity Skills/Knowledge Used

The tasks and projects that I was assigned to required numerous cybersecurity skills, some of which I learned through my Old Dominion University education and some of which I had to learn from my internship experience. Before taking this internship opportunity, pretty much all of my cybersecurity knowledge and skills were exclusive to my college coursework. Multiple of my courses taken during my junior and senior years entailed plenty of modules, assignments, and projects that allowed me to engage in hands-on exercises to develop knowledge as well as a skill set in cybersecurity tasks. This internship opportunity finally provided me with a chance to experience on-the-job training on certain cybersecurity tasks.

The major cybersecurity skill that I was able to practice and refine, was password management. I had prior knowledge and experience with password management stemming from my college course work. Completing password management tasks for an employer, as opposed to course work, was a new and different experience that I enjoyed. I quickly realized that the same principles and concepts I had learned from Old Dominion University also applied in a real-world environment. Course work taught me the major pillars of any secure password management – password length, a combination of different characters, and uniqueness. I was sure to apply all of

these same criteria to my tasks of managing passwords for some of the telecommunication devices such as the inverters or Sageons.

Another major part of this internship experience was to install and configure alarms for all devices. Alarms are something that was not covered much by my coursework, so getting experience with this skill set was something completely new for me. I was able to gain hands-on experience on both hardware as well as software aspects of the alarm process. Every device we installed or serviced was alarmed, so it was integral to this entire internship experience to grasp a firm understanding of the alarm installation process as well as the management aspect.

Remote monitoring capabilities was also a cybersecurity skill that I learned during this experience, as this was previously something I had not engaged much in during my coursework. Some of the devices that we installed or serviced provided us with the ability to communicate directly through internet protocol address, allowing us remote access to the devices' software. With remote access to the devices' software we could complete numerous tasks, such as password management, user account management, settings management, etc.

The on-the-job experience with the content area has changed my understanding of the subject matter by giving me a new perspective. This experience allows me to see how interdependent many cybersecurity tasks are. I also learned the importance of teamwork in cybersecurity. Many of the tasks that we completed were in direct coordination with the network operating center. I was shown first-hand how a secure cyber environment is only possible with complete cooperation from all. Completing coursework gave me great experience in hands-on exercises, but on-the-job training provides a completely different experience where these same cybersecurity tasks are completed as a cohesive team looking to achieve similar goals.

I also had my understanding surrounding alarms completely changed from this experience. Many people, including myself, think of sirens, horns, and flashing lights when thinking of alarms. Alarms are typically associated with tampering, breaking in, or possible theft. The reality is that there is much more to having alarms, as alarms with information technology infrastructure may very well indicate other issues that may occur with a device or its software. Issues could range from temperature overheating or simple power failure, but it stresses the importance that alarms play in all aspects of life in cybersecurity.

How ODU Prepared Me

While I did experience some new cybersecurity tasks during this internship – I do feel that my Old Dominion University coursework prepared me incredibly well for this internship opportunity. The core principles learned from my course work applied nearly universally. The tasks and projects that I undertook while in the internship opportunity were all built upon a foundation of confidentiality, integrity, and authenticity. My time in completing tasks and projects for the Department of State Police certainly worked to reinforce much of what my coursework taught me.

I certainly made connections between my coursework knowledge and the tasks that I dealt with during this experience. Managing passwords was certainly an activity that I enjoyed from my coursework, I underwent multiple modules and assignments that had me engaged with password management activities. The same concepts from my coursework also applied to my on-the-job experience – adequate password length, a mixture of different characters, and avoidance of common phrases or words. I also used CMD prompt for numerous classes as part of my coursework, so that familiarity helped incredibly whenever I needed to ping devices, view data, or alter device settings remotely for my internship.

There were certainly new experiences not faced with during my coursework. Alarms and collaboration were major experiences that proved different from anything in my coursework. Much of my coursework never really covered much of anything on alarms, from installing them to programming them. This internship gave me an opportunity to do just that, and though I had never experienced alarm management before – I very much welcomed this challenge and even thrived in these tasks. I also did not experience much cybersecurity collaboration through my coursework, I very much do not mind independent work and tasks, so I do not view that as being problematic. Having to work closely with my team as well as the network operating center provided me with a much-needed change in my environment, as it is incredibly important to be capable of working both independently and as part of a larger team.

Fulfillment of Objectives

As the internship would conclude, I strongly felt as though the initial goals That I and my manager had set out for this experience were sufficiently achieved. The first goal was to get hands-on experience in programming the software of some of the telecommunication devices we service, as well as grasp a firm understanding of the process. My manager began this learning process by providing me with written handouts that display and describe the steps. These documents provided me with a great overview of the programming process; it was essentially an extensive introduction. Following my review of the written materials, then came the more important hands-on activities.

Each device had its own respective software site reachable through internet protocol address. The initial connection setup entailed connecting an ethernet cable and entering the default device address into the browser's address bar. Upon successful connection, I was able to begin the programming process. Many of the desired attributes were specific to the needs of the

Virginia Department of State Police, so there was relatively little freedom to customize in that regard. Once inside the device software, I was successfully able to alter data to the desired configuration. Some of the software tasks included initial password setting, alarm threshold configuration, as well as initial internet protocol address setting.

Once the initial setup was completed, I also engaged in further software maintenance through CMD prompt as further programming experience with the telecommunication devices. Some tasks ranged from simple address pinging to ensure connection – to POWERCFG commands to observe system power efficiency. Overall, the tasks I engaged in certainly were satisfactory to our initial goal. I finished my internship experience with the desired knowledge and experience in programming the software of some the telecommunication devices utilized by the State Police.

The second goal of the internship was to gain operational insight into the information technology telecommunication hardware and the processes that they provide for the Virginia State Police. This goal was far less of a hands-on experience, and more so of purely learning and studying an overview of multiple devices critical to the Virginia State Police's communications. Some of the material used to obtain this goal came by way of written material provided in device manuals, but most of my learning experience with this goal was conducted through verbal instruction. My team had many years of experience working with these devices, so they were excellent at being able to verbally explain to me the processes provided by the devices and their importance to not only communications but cybersecurity as well.

I was able to learn about some of the following devices – Aviat RAC70, Nokia 7705 SAR-8, Motorola MOSCAD, and the Cisco ME 3400 to name a few. Some of the processes they provide include tasks ranging from firewall and VPN services to remote monitoring and switch

capabilities. The information learned was incredibly insightful and provided me with essentially a bird's eye view of the networking and security tasks that the devices perform. Overall, I am very confident in saying that this goal sufficiently covered. I left my internship experience with extensive knowledge on networking and cybersecurity functions provided by the equipment of the Virginia State Police. The information gained from this goal establishes critically valuable information for me to take and apply into my future career in cybersecurity upon graduation.

The third goal that was set out in the beginning of this internship experience was to establish a firm understanding of alarm installation, configuration, and troubleshooting. Words truly cannot begin to describe the relevance and importance of alarms amongst all devices serviced by my communications team. Everything at the RF sites was alarmed – from the door to every device inside. I quickly learned of the extensive alarming of devices upon my arrival, so I found that to provide me with an incredible opportunity to gain insight into essentially everything alarms related – from the initial installation to configuration and troubleshooting.

Alarms play a critical role in cybersecurity, as they are essentially the definition of security. Many cybersecurity jobs will entail complete management of alarms. In knowing that fact, I found it highly valuable to undertake extensive learning on the alarm process. Gaining this sort of knowledge and hands-on experience with alarms at such an early stage in my career will undoubtedly prove extremely valuable. Upon my arrival, I quickly began my journey to achieving this goal. One of my very first tasks was to install an alarm for an inverter device that my team would go on to install across the entire commonwealth.

I gained hands-on experience with the initial installation, with all the devices serviced being alarmed through a cat 5e cable. I would terminate the cable running from the device to a phone punch block to complete the alarm connection, this was a step I felt I had mastered by the

conclusion of my internship experience. The configuration of these alarms typically came during the programming of the device software, as the device software would allow for the configuration of alarm thresholds and other miscellaneous settings. The troubleshooting was by far the most difficult part of the learning process, but after much practice and going through various scenarios, I found it to be a process that I felt extremely comfortable in understanding and practicing in a professional environment.

I feel confident that this goal was also achieved successfully. I came away from this internship experience with great knowledge of alarm installation, configuration, and troubleshooting. Overall, these goals were all pertinent to my future in cybersecurity. With the help of the amazing team around me, I concluded my internship experience in achieving all that I and my manager had set out to. This successful experience provided me with critical tools that will continue to benefit me in my professional endeavors forever.

Motivating/Exciting Aspects

This internship provided me with plenty of motivating and exciting aspects. I found the initial opportunity to work with such a renowned employer to be incredibly exciting. The initial shock that one feels when receiving even just an interview request is immense. Following the interview, going on to further receive the opportunity of employment is an enormous rush of euphoria. Not only was this an opportunity with a highly reputable employer, but I instantly knew that this essentially opened the doors for me to gain critical experience that would catapult me into further cybersecurity opportunities.

Another exciting aspect of the experience was finding out that the team working alongside myself was incredibly experienced. It is very reassuring to know that the people that

will be teaching and leading you have decades of experience in their craft. I certainly comfortable leaning on the extensive experience of coworkers, as they have been through many trials and tribulations that I would soon experience for the first time. I found my team to be incredibly informative and supportive during my time.

An aspect that I found to be highly motivational was that my manager would provide an overview of his thoughts on my performance each month. It is incredibly helpful to receive feedback on your performance on a frequent basis. As part of my monthly performance reviews my manager would include incredible words of encouragement. Members of my team would also provide him with complimentary statements attesting to my performance, as my manager was not able to constantly observe my work directly. These words of encouragement every month would prove incredibly motivating and pushed me to achieve even high adulation during my experience.

Discouraging/Challenging Aspects

While there were numerous motivating and exciting aspects to this internship opportunity, there were also some discouraging aspects as well. One of the exciting aspects would be a double-edged sword, as it had a slightly discouraging aspect to it as well. Having a team around you with decades of experience is great for you if you need to lean on someone with lots of experience, but it can be slightly discouraging to know that you don't have even half of the experience or expertise that they do. There are times where you are concerned about possibly slowing your team down due to lack of experience, as they are experienced enough to complete certain tasks at a far quicker pace than someone with less experience.

Another discouraging aspect to the experience initially was the extensive amount of travel. Before taking this opportunity, I never had to do any real travel for an employer, at least not travel requiring overnight stays out of town. That was something I had to quickly become accustomed to, as nearly every week of the internship entailed travelling. This employer is a department of the Commonwealth of Virginia, so we were responsible for all regions of the commonwealth. Being away from family and friends every week was tough at first, as I frequently lean on them for support. Eventually, I would go on to really enjoy the travel; I even welcomed it and the great experiences it would provide me with getting to see some really beautiful places that I had never seen before. Overall, the traveling experience taught me that not every job opportunity will provide you with the perfect experience. Sometimes, especially for excellent employment opportunities, you will have to engage in certain aspects of the opportunities that are foreign to you and will require some adjustment. In the end, it was certainly worth it.

There were certainly some challenging aspects as well, which was very much expected when taking on such an experience. The first challenge was the pace at which work had to be completed. The inverter installation project was something that had been put off before I had arrived, so upon my arrival it was a project that management was overdue and thus was accelerated. The inverter project gave me my first hands-on experience in alarm installation and device software programming. It was fairly difficult to have to balance completing this project with the speed requested by management, while also having my team guide me through the learning process which can be time consuming. I did not feel rushed though, and I felt that my team did an amazing job of balancing the two tasks' conflicting pace of work.

Another challenging aspect of the internship was having to balance the full-time work hours with my coursework here at Old Dominion University. Challenges are not necessarily a bad thing, so this was a challenge I signed up for and willingly accepted. I know that in the professional cybersecurity world there are many positions that require you to complete daily work alongside written assignments and presentations that must be completed at home or off the clock. This internship provided me with that very challenge, I found it to be beneficial for me long-term even though it was difficult in the time. I faired very well in this balancing act and made sure that I gave a complete effort in all that I was tasked with, both professionally and scholarly.

The other challenging aspect to speak of was always being on-call. My team was responsible for servicing equipment that could be compromised at any time, from both internal and external factors. We had to be in a state of readiness in case of any emergency call from upper management. While we never experienced an on-call incident, the potential for it is enough to keep one alert and prepared at all times. Being on-call was also a welcomed challenge, as many cybersecurity jobs entail having to remain on-call in case of an emergency incident.

Recommendations for Future Students

I certainly have a few recommendations for future interns in cybersecurity. My first recommendation is to experience some form of professional employment before attempting to complete this internship. It is extremely important to have at least a little experience in a professional setting before undertaking this internship. This internship should not be expected to be easy, but it will certainly be slightly easier to adjust to if it's an environment somewhat familiar to you. I remember how challenging it was to experience my first job in a professional setting, so I would hate for someone to experience that in this internship.

My second recommendation would be to begin looking relatively early on for internship opportunities in cybersecurity. Cybersecurity is a great field because there are seemingly always job opportunities out there, but that does not mean that they are easy to obtain. While many, including myself, are proud of personal accomplishments and feel as though they have a great resume – there will always be candidates with even more accolades and accomplishments. Entry-level opportunities are even more difficult to obtain, so I recommend starting the search process early. Starting late into your junior or senior year may end up with you getting an opportunity too late or maybe not one at all close to your anticipated graduation.

My third recommendation would be to apply for as many internships as possible. Many people find an opportunity that they feel would be their best-case scenario. Even though you may find certain openings that you strongly favor over others, that opening is certainly not guaranteed. You may feel incredibly confident that you could obtain a certain opportunity, but you must continue applying to other openings as well in case plan A does not work out in your favor.

My fourth recommendation is to ensure that you understand the basic principles of cybersecurity. Old Dominion University does an excellent job with their cybersecurity bachelor's program, so I am confident that if you are enrolled here then this should not be too difficult to attain. Internships certainly are learning opportunities that often provide hands-on experience, but even though they are entry-level opportunities, employers still often expect a baseline amount of knowledge on cybersecurity. If you cannot demonstrate this baseline knowledge of cybersecurity fundamentals, then it can be nearly impossible to obtain an internship opportunity.

My fifth recommendation is to be willing to adapt to environments and factors that you may not find to be perfect or accustomed to. Accepting my internship provided me with

circumstances that were not perfect for me and proved challenging in certain situations. As a professional, however, you will be put in imperfect situations that you must be willing to adapt to. Those that can adapt will prove far more successful than those that cannot. Do not put yourself at a disadvantage by being unwilling to adapt to something different than what you may be accustomed to. No job is perfect, so always put your best foot forward and give your best efforts no matter what the situation is.

My final recommendation would be to look into obtaining professional certifications. A degree is why you are currently at Old Dominion University, and they are certainly very valuable in any profession. They are not everything, however, and you quickly learn that in this profession there are many employers who even give slightly more value to certifications. I take immense pride in achieving my CompTIA Security+ certification, and I have no doubts that having that credential assisted me in successfully obtaining this opportunity. Certifications will set apart from the pact, even after you obtain a degree, as employers will certainly favor candidates with a degree plus one or more certifications versus a candidate with only a degree. Certifications also showcase to potential employers that you not only know relevant material, but that you are also capable of applying this material in real-world situations.

Conclusion

I have a few main takeaway thoughts as I reflect upon this internship experience. My first is that I am confident I can thrive in any professional work environment. This employer is arguably top of the line when it comes to professional standards. While I may not have been perfect, I was very successful in my time in this role. I completed all tasks to the best of my ability, soaked in as much knowledge and experience as possible, and received excellent marks from all members of the communications team as well as management. This experience has

provided me with immense confidence that I can fit into any professional cybersecurity opportunity.

My second takeaway thought is that the team around you matters to an incredible degree. Cybersecurity is as much of a team effort as any profession out there, with everyone having to be on the same page to make things work as desired. I strongly believe much of my success can be attributed to having such a greatly supportive team around me. Having experienced coworkers to lean on in times of need and when learning is incredibly valuable. I can express much gratitude to the Virginia State Police in helping me to become the professional that I aspire to be.

My final takeaway is that this internship provided me with the skills and tools necessary to begin my career in cybersecurity. Essentially all my experience up to my internship was exclusive to my coursework here at Old Dominion University. Completing this internship, however, finally provides me with the much-needed professional work experience necessary in cybersecurity. The skills and experience I gained from this experience are immensely valuable, and something that I will undoubtedly carry with me for the rest of my professional life.

This internship experience will certainly influence the remainder of my time here at Old Dominion University. It motivates me to continue to finish strongly as I inch closer to my graduation time. I have done well in academic performance up to this point in my coursework. The internship experience gave me a small sample of the professional work environment that I aspire to remain in for the foreseeable future. Fulfilling my academic endeavors and obtaining my degree will only make that aspiration even more attainable for me.

The internship also influences my remaining time at Old Dominion University by reinforcing my commitment to cybersecurity. Early on in my coursework I was admittedly

unsure of this field, even after officially declaring cybersecurity as my major. The internship, however, greatly reinforced that commitment. I got to actually experience cybersecurity in a real-world professional work environment. Getting to experience this was amazing, it showed me that this is a field that I truly enjoy engaging in. This internship showed me that this is the right field for me, and one that Old Dominion University will continue to help me refine and strengthen as I finish my remaining time here.

The final influence that this experience provides for my remaining time in my coursework is that it provided me with an insight into my strengths and weaknesses of cybersecurity knowledge. I will take that into strong consideration when enrolling in my remaining courses. Since I now have this insight, I will be sure to select courses that can help to combat some of my known weaknesses as well as further strengthen my known strengths. I am never satisfied with my current body of work, so having this internship provide me with an overview of what needs to be done to improve my experience, and skillset will prove critical to my remaining time in my coursework. These influences will certainly be felt before my pending graduation.

This internship experience will undoubtedly influence my future professional path as well. The first influence stems from the connections that I will attain from this opportunity. Professional law enforcement agencies have plenty of opportunities in the cybersecurity field of work. Having this reputable law enforcement agency on my resume is sure to attract further attention from other law enforcement agencies. I have also met some amazing people with decades of experience that include other law enforcement and state agencies as well.

The other major influence on my future professional path is the enhancement of my resume. Before this internship experience, I certainly had a resume that I felt proud of and

incredibly confident in. Following this internship experience, my resume is sure to be made much stronger. I now have more experience and specifically experience for a professional employer. My listed skills on my resume all pertained to my coursework, but now I have skills and experiences that I can directly attribute to professional work. Strengthening my resume with these attributes will assuredly make myself a far more attractive candidate for potential employers in my future professional path.

The final influence that this experience provides for my future professional path and planning is that I now feel extremely comfortable and confident in seeking employment opportunities that heavily rely on teamwork. Before this experience I was very much more of an independent-minded person when it came to any professional work. Now, having gone through this experience alongside a close-knit team, I am fully prepared to conduct professional work amongst a team. I am no longer reluctant to seek team-oriented employment opportunities. If I earn employment that entails intense cooperation and teamwork, I have no doubt that the influence of this internship will allow me to be fully prepared and capable of successfully doing so in times of need.