7/29/2025

John C. Creger UIN 01154971

MARMC Internship

US Navy

CYSE 368 Summer 2025

Table of Contents

Introduction

Internships are an excellent opportunity to gain valuable professional experience in a career field. These positions are often unpaid and require very little experience. I was fortunate to find an internship opportunity at Mid-Atlantic Regional Maintenance Center (MARMC) in Norfolk Va. I am currently active-duty Navy and am stationed at MARMC. I am a Navy Diver, and I mostly work on the waterfront of Naval Station Norfolk, fixing ships underwater and transitioning into a cybersecurity role is a different and challenging atmosphere and working environment. Overall, I learned a lot about the industry and different roles of cyber security professionals working under the MARMC umbrella. While completing my internship my goals were to gain experience in understanding various cybersecurity threats, develop hands on, incident response skills, enhance knowledge of securing networks, and apply cybersecurity best practices in operational environments.

MARMC is a Navy command dedicated to fixing and maintaining naval ships under the 2nd Fleet. The 2nd Fleet is responsible for securing naval operations in the Atlantic and the Mediterranean Sea. MARMC is a large organization with over 1500 active-duty Sailors and civilian employees. There are two main facilities, both located at Naval Station Norfolk, building CEP-200 near the waterfront and building LF-18, located on the opposite side of the base near the airfields. The cybersecurity division is located in building LF-18 along with the majority of the administrative staff dedicated to the command. MARMC's primary customers are the ships and submarines assigned to the 2nd and 5th fleets. When these ships require maintenance that the crew of the vessel cannot accomplish, they request services provided by my MARMC to keep them fully functional. MARMC also supports ship repair and maintenance while ships are deployed to the Persian Gulf and operating under 5th fleet. Additionally, MARMC has assets in Rota, Spain and Souda Bay, Greece. MARMC is a global organization and is a valuable asset to the Navy and to national security.

The cybersecurity office within MARMC is a much smaller cog in the wheel, of the larger MARMC machine. The division falls under code 1100 and is appropriately designated 1100X. There are six full-time employees including the Division head, ISSM, two ISSOs and two cybersecurity analysts. The cyber team works closely with the IT department, but strict lines are drawn for job roles and areas of responsibility. The main focus of the cybersecurity division, at MARMC, is the security of a LAN housed with MARMC called RMC-NET. RMC-NET is an in-house standalone network that was originally designed and built for all the RMCs to connect to provide a shared network. The network is air gapped and now has very low threat assessment. It is rumored that RMC-NET is going to be shut down completely and will be replaced with a cloud-based solution. That system hasn't been fully decided on, but I think Amazon Web Services (AWS) has presented a solution for the replacement of RMC-NET. An additional responsibly of the cyber office to review System Authorization Access Request (SAAR) forms to ensure personnel at the command have the appropriate access and privileges. The last major function of the office is to

manage Secret Internet Protocol Router Network (SIPR) tokens to qualifying personnel. The MARMC cyber security office has many roles and serves several customers daily.

My initial orientation to the role was non-traditional. Historically, when new people are hired on, they attend a weeklong indoctrination class. This class introduces all the departments of the command and gives a brief overview of what they do to keep the machine rolling. This is a valuable time to learn these people's names contact information because, without a doubt, I will need them for something in the future. I was able to skip this portion of the "hiring process" because I checked into the command three years ago completed indoctrination. The first day was a bit of a whirlwind. I arrived at the cyber security office at 0700 and was meet with a confused look from a man in the MARMC SOC, apparently the supervisor had not informed his team that I was going to be helping over the next several weeks. After the introductions were completed, I was sent down to the IT department to get issued a laptop, and ancillary equipment. I got my workstation organized, computer updated and configured and was now ready for tasking. One of the cyber security analysts, Maurice, pulled me over to help with conducting network scans. The program he used was Tenable in conjunction with ACAS and he explained that this software is used in nearly every federal agency. Everyone in the office was welcoming and treated me professionally. My initial impression was positive, and it seemed like this was going to be a successful and educational experience.

Section 2 Management Environment

Management is an essential element of any highly functioning team or organization. There are many different approaches to management and leadership from authoritative, autocratic, laissez-fair, etc. I think the best approach to management and leadership is a combination of everything. Different people respond to different styles of management and there is no set way that guarantees success. I think the key to good management or leadership is consistency, this is also essential for an employee as well. The management within the cybersecurity division is typical of government and most civilian organizations. MARMC cybersecurity hierarchy structure can be seen from the picture presented in appendix one.

My position within this hierarchy would be equal to Ms. Nancy Barcenas, as a cyber analyst. Everyone else in the office had the same pay grade and all answered to Mr. Chris Fitzsimmons as the branch head. Mr. Erim Hamm is the command ISSM and the unofficial office leader that speaks for rest of the employees and reports to Chris Fitzsimmons. Chris Fitzsimmons has been my functional supervisor, and he has some unique management tendencies. It has become obvious that Mr. Fitzsimmons and Mr. Hamm do not always see eye to eye on a variety of issues. This dynamic often boils over and often creates an awkward office environment.

Mr. Fitzsimmons is my supervisor for the internship and has been very helpful, especially when coordinating various site visits. Mr. David Newsome, however, has been more of a mentor and has shown me more of the technical aspects of the role. I think this combination of personnel has been effective from a management perspective.

Section 3- Work Duties and Responsibilities

Working in cybersecurity is a very broad topic and can often mean different things and has various roles. When I first approached Mr. Fitzsimmons and asked for an internship at MARMC, he asked me, well what do you want to do in "Cyber?" He made the analogy that working in cyber is similar to being a doctor, is the aspect of well there are doctors but what kind of doctor are you? This really made me think about what I wanted to do in cyber. Unfortunately, the MARMC cybersecurity doesn't have some the "cooler" type positions like penetration testing, threat hunting, social engineering and other roles associated with red or blue team operations. My daily tasking was more focused on the roles that MARMC needed.

The first task I was given was to validate SAAR forms submitted by military, DOD civilians and contracted personnel. When personnel need to get computer access, they request access through the IT department with a System Authorization Access Request (SAAR) form. The SAAR forms are reviewed sent to the cyber office in order to validate that they have completed the required training and the form is filled out correctly. The proper training is verified through a system called TWMS or Total Workforce Management Systems. TWMS will also retain a copy of the SAAR so that it can be used for future access requests. Common errors on the forms are personnel not selecting the correct job position. There are three choices military, DOD civilian and contractor. This is important because a SAAR form is only valid for the life of a contractor's contract and must be renewed periodically. The length of the contract is also a part of the form to be filled out by the contractors. Once verified, I would send the SAAR form back to IT with either approved or disapproved with amplifying information as to why it was disapproved. This task isn't, in itself a full time job, but MARMC, being a large organization with thousands of employees, processing SAAR forms can take about an hour a day. After processing a few forms, I had become proficient at this task and felt confident I could accomplish the process without supervision.

Once I "proved" myself with processing SAAR forms, I was shown some the basics of the network scanning process. The cyber security office is responsible for the security of the RMC-NET housed within MARMC. This system is an air gapped and running scans and updating is a bit more complicated than if it had internet connectivity. The first thing that is required is updating the scanning program with current STIGs. These STIGS were downloaded from DISA to an external USB hard drive. This hard drive was encrypted and had a digital keypad requiring a password to be entered in order for it to function. Once the updates were downloaded on the hard drive, we would disconnect from NMCI and connect it to a laptop connected to RMC-NET. We would log into the RMC-NET and run an Assured Compliance Assessment Solution (ACAS) provided by Tenable. Before we would start the scan, we would need to update ACAS to ensure the newest STIG had been implemented. After all those steps we were finally read to conduct a full system scan. Scanning the entire RMC-NET network takes about 40 minutes and then produces several different reports. While waiting for the scan to be completed, I was shown some of the different capabilities that Tenable offered. Maurice has already configured many various scan templates. For example, he had templates to only scan the laptops connected to the network

and another template for scanning the servers and routers. We analyzed the reports and found no discrepancies, and everything was good to go. If there were issues, we would have to inform the chain of command to elevate the problem. Once analyzed, scans are saved back to the encrypted hard drive and uploaded to a SharePoint drive for MARMCs parent command Commander, Navy Regional Maintenance Centers (CNRMC) for review and eventual archive.

I was given a "project" to conduct research and validate whether the dive locker needed an RMC-NET asset. One of the functions of the RMC-NET is to provide stand-alone computers for legacy applications that are unavailable or restricted to being used with standard NIPR NMCI machines. The diving hyperbaric recompression chamber has an atmospheric monitoring system called a Sub Aspida manufactured by Analox. This device ensures proper amounts of oxygen and carbon dioxide are maintained when divers are in the recompression chamber. The Sub Aspida needs periodic calibration and requires proprietary software to complete the calibration. Additionally, the Sub Aspida needs to be connected to a computer via USB cable to complete the calibration. The software is currently unavailable on the Navy's Software center and it's unauthorized to be connected to an NCMI asset. This is specifically what RMC-NET provided a solution for. Unfortunately, RMC-NET is going to be decommissioned and dismantled and possibly replaced with an AWS solution. The dive locker needs the capability the Sub Aspida provides, but MARMC soon won't have to infrastructure to keep the device calibrated. My assignment was to explore if the software was IOS compatible and if they provided any application compatible on iPads. The command has a set of iPads that have been authorized to connect to NCMO via VPN so if Sub Aspida had an IOS application it could be updated with the iPad. I emailed the company to inquire about where the device could be updated via iPad. They did respond and informed me that the software is not compatible with IOS and must be updated on a Windows platform. The next step is to route an exception to policy to be able to connect the Sub Aspida

The duties and responsibilities that I was given in the MARMC cyber security office were on par for an entry level position. Processing digital forms by verifying accuracy and requirements were completed was the majority of my daily tasking. I was also encouraged to enroll in computer base training hosted by DC3 to build my skills. Additionally, running scans on the RMC-NET provided experience on networking monitoring and analysis.

Section 4- Cybersecurity Skills

Prior to the start of the internship at MARMC my cyber security skills were limited to a purely academic setting. I have taken a full course load on in most areas related to cyber security, to include, RMF, penetration testing, Linux fundaments, cryptography and digital forensics to name a few. I enjoyed most of the classes and was looking forward to applying what I learned into a real-world setting.

The biggest use of a specific skill was NIST RMF. The ACAS scans I ran with the Tenable environment all had to be updated with the STIGs downloaded from the DISA site. When these

STIGs could or could not be easily implemented, a Plan of Action and Milestone was created to set a timeline for completion. I have academic experience with the NIST RMF 800 series, allowing me to understand the processes that need to take place. The most beneficial knowledge that helped me with my internship was just having the appropriate vocabulary and being able to speak the language. The terms and acronyms associated with cyber and information technology are unique and being able to under a conversation without having to stop and ask what stuff means if very beneficial.

Section 5- ODU Curriculum Application

Old Dominion's Cybersecurity degree is an interdisciplinary course of study and has a broad scope of classes that will be accepted for credit. This course being a 300-level course, I feel is best taken as summer class prior to a student's senior year. I am completing my internship as the last class before graduation as I have completed 97% of my degree prior to my internship. I took classes what prepared me for my internship; however, I took a lot that did not. With traditional logic I think having completed all my classes prior to an internship would be a good thing but with how specific cyber security can be I think it was not. If I had completed the internship prior to senior year, I would have a taste of what is going on in industry and would have tailored my classes to a more specific cyber role. The curriculum that helped me the most were classes that incorporated penetration testing skills like CYSE 450 Ethical Hacking and Penetration Testing, CYSE 301 Cyber Techniques and Operations, and CYSE 270 Linux for Cyber Security. These classes allowed me to understand what the personnel stationed at NCDOC were talking about. They allowed me to speak their language and ask smart questions about the mission and capabilities. Over all the curriculum prepared me for the internship, but could have been tailored based on the skill sets MARMC required for daily tasking.

Section 6- Learning Objective Success

When I signed my original Memorandum of Agreement (MOA) with Mr. Fitzsimmons, I had four primary learning objectives. I went aggressive during my approach to the learning objectives and knew that achieving all these tasks was going to be a large undertaking. The four objectives were, Understand Cybersecurity Threats & Defense Strategies, Develop Hands-on Incident Response Skills, Enhance Knowledge of Secure Network Architecture and Apply Cybersecurity Best Practices in Operational Environments.

Understanding Cybersecurity Threats & Defense Strategies was goal to specifically gain insight into threats faced by MARMC and analyze security incidents happening within MARMC. This goal was partially met because I did learn about potential threats that MARMC faces such as insider threat and spillage of classified or sensitive information. On the other half of that task, I couldn't analyze a real-world incident because I wasn't given enough privileged access to truly analyze a real-world event. Developing Hands-on Incident Response Skills was a goal to participate or observe in simulated threat scenarios. This goal was not met for the same reason as before because I wasn't given escalated privilege, however I was able to visit NCDOC red team

and was provided a brief overview of their mission and capabilities. Enhancing Knowledge of Secure Network Architecture was a goal to observe network security implementations which I think was a success. Learning how to implement security updates with RMC-NET met the requirements of this objective. Appyling cybersecurity best practices in operational Environments was a goal to Identify vulnerabilities and risk mitigation strategies at NCDOC, and this goal was not fully met because, although I visited NCDOC I wasn't able to fulfill an operational role.

The internship at MARMC provided a lot of educational benefits. As for the specific objectives laid out in the MOA, I think I might have missed the mark on about half. If I were given privileged administrative access both at MARMC and NCDOC, the objective would have been much easier to accomplish.

Section 7- Motivating Moments

The cybersecurity department within MARMC is not a large organization and has a limited scope of responsibilities. I knew this fact prior to the internship and Mr. Fitzsimmons wanted me to conduct site visits at various locations around the Hampton Roads area to gain more experience and see different aspects of cyber. One of these visits was to Navy Cyber Defense Operations Command (NCDOC) in Suffolk, Va. I had never heard of NCDOC prior to Mr. Fitzsimmons telling me about it. NCDOC is the U.S. Navy's primary command for Defensive Cyberspace Operations (DCO). It plays a critical role in safeguarding Navy networks and enabling global power projection through proactive cyber defense. This trip was extremely motivating and gave me deep insight into some of the most sophisticated and powerful cyber assets.

The road to getting a visit was not an easy task. I began by emailing some of the public contacts listed on the website and didn't hear back. I was slightly discouraged after not hearing back for a few days, but I then leaned on a valuable asset at my disposal, the Chiefs Mess. I emailed the Command Master Chief (CMC) of NCDOC, plead my case and within a day got a response and was given a point of contact, Cyberwarfare Technician Senior Chief Thrasher. He was the operations (N4) Leading Chief Petty Officer (LCPO) and was glad to help me coordinate a site visit. The first thing he asked me about was my security clearance. I have a Top Secrete/SCI with polygraph from a previous command I was stationed. This made the site visit much easier. Without a high-level clearance, I would not have been let into the building at all. Of course, NCDOC isn't going to take my word for it and would need to verify my clearance level. I then coordinated with the MARMC security department, giving them NCDOC Security Management Office (SMO) Code to submit a visitor request with a program called Defense Information System for Security or DISS. After a day or two I got confirmation that the requests had been processes and my site visit was approved. The next step was to coordinate with Senior Chief Thrasher to set up a time and day to make the trip to Suffolk.

I arrived at the Department of Defense Compound Suffolk on July 1st to engage in the site visit with NCDOC. The first step was clear security. This command had an airport level, TSA style security station that must be cleared prior to entering the facility. I had to go through a metal

detector and x-ray machine to ensure I wasn't carrying any unauthorized items such as phones, laptops or other personal electronic devices. After clearing security, I met my contact at the quarter deck, we exchanged greetings and then we made our way to the CMC's office. An Interesting thing about the CMC is that he is not a cyber warfare tech or even an information technology trained Sailor. After a brief introduction and me, thanking him for the opportunity for the visit, we made our way to the first stop of the tour, NCDOC's Red team.

Unfortunately, much of what NCDOC's Red team does is classified and cannot be written about in this paper. I was able to talk to the teams LCPO and discuss the various processes they use to try to break into a system and see what they can get away with. For me, the most interesting aspect of red teaming is social engineering. The technical side of things is also interesting, using different emulators and tools to hack systems but the human element has always intrigued me. I asked what they do, and they gave me a generic answer. They are charged with trying to exploit vulnerabilities with a targeted command. For example, MARMC could "hire" them to run a penetration test and only the leadership of the MARMC would know that they were hired. During the in brief with the triad, limits are set to ensure the actual safeguard of sensitive information is maintained. The Red team would then begin the reconnaissance of the MARMC to scan for vulnerabilities. One of the interesting aspects of what they do, that I was unaware of, is they test physical security. For example, they may attempt to access the building by piggybacking or searching for unlocked points of entry. Once in the building they continue to see what they can exploit, like seeing if they can access computers, servers or potential classified areas. Learning from the red team was extremely fascinating and has given me a goal to set my sights on future career endeavors.

I left the red team's office and was taken into a different area of the command to meet the LCPO of the Cyber Protection Teams (CPTs). Cyber protection teams defend Navy networks from cyber threats. They are on the opposite side from the red team as they monitor systems for intrusions, respond to incidents, and most often conduct vulnerability assessments. These teams are equipped commercial of the shelf tools distributed by Sealing Tech Inc. These systems have extraordinary capabilities such as the ability to image up to 100 TB of data from a network at one time. These teams safeguard mission-critical data, deploy with Navy ships and to Naval installations globally to enhance resilience. Through continuous defense and innovation, they ensure Navy systems remain secure, reliable, and ready for action. These teams have an aggressive operational tempo and are expected to be deployed nearly 200 days a year. Spending some time with the CPTs was interesting and I was impressed with their mission set and capabilities.

The final feature of NCDOC, that I was given access to, was the watch floor, a true Security Operations Center (SOC). I felt This room resembled NASA's mission control is Houston. The room had close to 30-foot ceilings and one wall completely dedicated to monitors and TVs. The center of the room had a raised platform where the watch captain directed operations. There were 30 desks with three technicians each monitoring two-three large screens with a constant feed of data. This room was responsible for the analyzation of all traffic from every naval network across

the world. I was told if a Sailor downloaded Spotify on USS Neversail, anywhere, in the world they would know about it. They could not give me personal access to act as an analyst, but the experience was still inspiring and left me wanting more.

The field trip to NCDOC was incredibility motivating. Getting out if the MARMC office and experiencing a SOC in real time, talking with threat hunters and learning pen testing from an active red team revitalized my drive to become a cyber security professional. The people I met, the facility, and overall mission were unbelievably motivating. I could see myself applying for any available positions and working at NCDOC as a contractor or even GS level position, if they were hiring.

Section 8-Discouraging Moments

When starting a new venture, most people are excited, bright eyed, bushy tailed, ready to learn and experience new things. This optimism usually fades after time as people settle into a routine. I had this experience. When I first entered the officed I was excited and wanted to do great things. After a relatively short time I became a bit disappointed and discouraged about the position I was filling.

The first thing I became discouraged about was the lack of technical work within the office. I was expecting to come in and be taught about monitoring networks and responding to threats. Although the cyber office does perform those functions it's from a passive posture and is administrative in nature and not happening in real time. The most technical task I accomplished was updating the ACAS scan with the recent STIG files downloaded from DISA. I knew going into the internship that the MARMC cyber office didn't perform the same level of functionality as NCDOC for example, I didn't realize how much less they actually did. Additionally, some of the personality issues that I will discuss later were discouraging. I know this is a micro section of the industry at large but the unprofessionalism that I experienced was extremely discouraging and made me reconsider even working in the industry.

Section 9- Biggest Challenges

I'm sure all internships have various challenges and MARMC is no exception. One of the biggest challenges is just getting an internship. I emailed and called several companies and organizations and did not receive a single call back or reply email. I'm not sure why companies wouldn't want potential free work from a college student for a few months, but I guess they don't want the burden. Along the same lines, conducting the site visits was a challenge. I would go for days without response from people. I understand it is a lot of extra work to facilitate someone coming over and asking a bunch of questions but some of the responses I got from organizations were downright rude. I think it's very easy to say, "oh that's not my job" and then just move on. As an active-duty chief, it's in my nature to help people when they reach out and ask, so getting a lot of resistance was a challenge.

Challenges also come in the form of personnel issues. The working environment within the cyber office was often difficult and awkward. This dynamic, I think, was a direct result of leadership and the management style of my supervisor. I don't want to jump to many conclusions, as I only spent a month in the office and was not privy to previous workplace confrontations. It was my opinion that the supervisor tended to micro-manage his team. The team didn't appreciate being treated like children and it would often lead to open hostility in the office in front of the entire workforce. I felt they were being disrespectful to him and undermined his positional authority for the entire team. Coming from a leadership position, I felt the behavior was very unprofessional and it was a challenge for me not to become too involved in the situation. I think this toxic environment has been going on for some time. I think it becomes obvious when I found out that the cyber office has had 5 people quit within the last 18 months. When I started the internship, I wasn't expecting to have issues pertaining to professionalism, but a lesson learned is that unprofessional people work everywhere.

From a technical aspect the challenges I encountered were related to the running of the scans on the RMC-NET. I had never been exposed to that software or the processes that MARMC used to report the results of the scans. The ACAS scans were all completed with a GUI, and it was user friendly and only had a mild learning curve. One of the more challenging concepts was learning about Authorizing Officers (AOs) and Authorized to Operate (ATO). An AO approves an ATO by reviewing the system's security posture and assessing whether the residual risks are acceptable for mission operations. Mr. Newsome spent some time explaining how different parts of a network may have multiple AOs and ATOs and it was the job of the Information Systems Security Manager (ISSM) to coordinate these entities to ensure the network is properly secured. The technical challenges I experienced in my internship were minor compared to the personality and unprofessionalism I encountered.

Section 10- Future recommendations for interns

Internships should be time for learning and possibly even making a few mistakes, as long as you grow from them. I would not recommend MARMC to future students pursuing an internship because of the limited scope of work accomplished within the MARMC cybersecurity office. I decided to complete my internship at MARMC because it was convenient and wouldn't interfere with my full-time job too much. I realized that was shortsighted and I should have attempted to pursue an internship with another entity.

A major recommendation I would advise future students on is to get this internship done prior to your senior year. I had to wait to get it done as the last thing for my degree completion. The purpose of the internship is to learn and to gain exposure to different aspects of cyber. If I had completed this process prior to senior year, I would have varied my course work and geared it towards a more specific area of cyber. The course work offered by ODU in the cyber program does make you well versed in many areas of cyber, but adapting your education to learn more specific skills will make you more valuable in the job market.

Section 11-Summary

An internship at MARMC has been educational experience and has given me a lot to think about both personal and professionally. I feel fortunate that I was given an opportunity to fulfill the requirements of the internship at my current workplace, but I feel I may have shortchanged myself by taking the easy road. I gained experience as an entry level cybersecurity analyst processing basic paperwork and running routine scans of a proprietary network. The time I spent with NCDOC was extremely motivating and gave me better directions. Having to work with difficult individuals is a part of any workplace. Learning how different people deal with difficult people is a valuable skill.

The MARMC internship is going to influence my educational journey. From an undergraduate perspective, it would affect much because the internship was the last requirement I needed to graduate. However, I was considering applying to a master's program and utilizing my Navy G.I. Bill to cover this cost. After talking with many people in the industry, I think the better continuing educational avenues should be in the form on certifications like CompTIA Security plus or SANS GIAC. From a professional standpoint I now know that I will want to work in more offensive aspects of cyber like penetrating testing and other red team activities. The daily grind of ensuring compliance, running scans and analyzing reports is not interesting. In conclusion, the internship at MARMC was an overall success despite the challenges and discouraging moments. I have learned about the MARMC organization and the whole of the cybersecurity industry.

Appendix 1- Command Employee Organizational Chart