John C. Creger

CYSE 368

7/7/2025

UIN 01154971

Mid-Atlantic Regional Maintenance Center (MARMC) Reflection Paper 2

I have completed my second 50 hours of the internship and have once again learned a lot. It's interesting how much you can learn about an organization in just a few weeks from not only a technical perspective but also from an inter-personal perspective.

The director of cyber security at MARMC is Mr. Fitzsimmons, a GS-13 and he is technically savvy and well credentialed professional. He took a few hours recently to explore different areas of cyber and how to deep dive and analyze job listings. Being a former Sailor and a current government employee, he gave me good insight into navigating USAJOBS.com. He helped me corelate different aspects of my current position, showing that I am actually more qualified than I originally thought for a government position. His insight was helpful and gave me a little hope on possibly getting hired in a government position.

David is one of the cybersecurity analysts within the department and has nearly 20 years of experience in government, government contracting and the private sector. I laid out the pros and cons of each. Government work will be much more routine, the pay is ok, but job security is much better as a government employee. Government Contracting is much like being a government employee however the pay is usually much better. The downside in your contract isn't indefinite, meaning if another company under bids the contract you could either be let go or have your salary reduced. David's advice for the private sector is that you will probably be exposed to multiple roles and have the best chance of learning the most in the field. But once

again pay is often higher and job security can be uncertain. Taking Davids advice, I am going to pursue a position in the private sector because I want to be exposed to as much as possible and feel I take a risk because I have my navy benefits to act as a safety net.

From a technical standpoint I have been assigned to process all the SAAR forms that filter in through the IT help desk portal. It's an easy job that is redundant and helps the team focus on other problems. One of the responsibilities of the office is to reset SIPR tokens, however I am unable to complete that specific task because the command doesn't want to elevate my privileges on the high side. David spent some time with me explaining accreditation boundaries within systems and the AO works, taking responsibility for that network with the accreditation boundary. It was also explained that all these networks and systems work together to accomplish a task or mission. There could be several AO's and boundaries withing an organization and it's the job of ISSM to make everything work together and function properly.

I was finally able to perform my first site visit to Navy Cyber Defense Operations (NCDOC). This facility is located over in Suffolk across the street from Commander, Naval Information Forces (NAVIFOR) and home of the 10th fleet cyber command. I had to make a lot of phones calls to get in the door. An official visit request was sent from MARMC to NCDOC security with the applicable Security Management Office (SMO) code. My clearance was verified with DISS, and I was assigned a liaison, Cyber Warfare Technician Senior Chief Thrasher. To enter the building I had to leave my phone and any smart devices in the car and go through a metal detector and x-ray. After a few official greetings with members of the Triade, I was introduced to members of the Red Team. They gave me a good overview of what they try and accomplish. They are "hired" by commands to perform security assessments and then they go forth to see what they can get away with. This is super interesting and I love the idea of

performing social engineering and phishing techniques to gain unauthorized access. It was made very clear they operate within the boundaries of what the commands want and establish limits to prevent unintentional spillage. I was then given access to the N3a watch floor. That was super cool to see, in real time what the true capabilities of the systems they employ. Unfortunately, the majority of what I was exposed to was classified and writing about it will get me in trouble and compromise OPSEC. I enjoyed my visit and learned a lot about the different roles that exist in an enterprise level organization.

These last 50 hours have been educational at the office at MARMC and for my visit to NCDOC. I am hopefully that I will be invited back to NCDOC for further experience. I am also still planning a site visit or Teams meeting the Navy Expeditionary Combat Command SOC at Little Creek, to gave further information.