

Michael Opoku-Arthur

Professor Duvall

CYSE 368

My name is Michael Opoku-Arthur; I am a rising senior majoring in Cybersecurity with a minor in Risk Management. As I near my senior year's beginning, I reflect on my experiences. I am grateful to have obtained an internship every year since attending Old Dominion University. Through these various internships, I have navigated the world of Cybersecurity to discover and establish my niche. The company I am interning for this summer is Leidos; I will be a Cybersecurity/Information Assurance Intern. In this role, I will be on the threat hunting team, monitoring the network and flagging any questionable traffic. I am excited about my Information Assurance role as I can dive into cybersecurity's policy and compliance side. The idea of venturing over to become a cyber risk manager is my current career goal, so seeing what the non-technical side is like is very exciting.

My office is located on the Joint Base Andrews in Maryland. Things are a bit slow right now. So far, I have only been doing training since starting, and the company is still working to obtain all my access and give me a laptop. Due to our level of work, we work in a Sensitive Compartmented Information Facility (SCIF), meaning that no outside technology is allowed—no external laptops, smart devices, phones, smart watches, etc. The issue I am facing right now is that because I don't have access to anything, I cannot receive a company laptop and therefore cannot work on anything in the office, let alone work on anything in general, unless it is training. My time right now has mainly been just training and getting onboarded. For this company, your first week is all orientation on onboarding, which is when you start to ease into your workplace.

During my second week, I met my team lead, Jason, and another member of our team named Kevin. We are the Cybersecurity department, and within it are different teams; my team is Threat Hunting. Already having prior knowledge of threat hunting, it'll be interesting to see the steps that take place for hunting for this company compared to prior ones. I am also excited to see if any standard tools are used universally. The two walked me through what an average day-to-day was like; I did some shadowing, and shortly after, was sent home to finish training since I could not access anything in the SCIF.

My first two weeks with the company have been slow due to access and accounts not being granted and created, but I am very excited for what is to come with the company. I hope for the following reflection journal, I have more to share.

Michael Opoku-Arthur

June 10, 2025

Leidos- Cybersecurity & Information Assurance Intern

Reflection #2

Throughout the next 50 hours with my internship at Leidos, the only thought that was going through my head was, “Am I going to have any information to put on this next reflection?”. The answers to that question are yes and no. The last 50 hours of my experience were an emotional roller coaster for me. Where I last left off in the previous reflection journal was that I still had no user account and no laptop; as I returned from the Memorial Day weekend, my experience was still more of the same in what I had already been experiencing. I still had no user account or laptop, and at this point, I was beginning to grow frustrated with the entire process. Three weeks into my internship, I had no access to the office, no user account, no laptop, and no place to sit! I felt like a stranger in my workspace. Although I was met with these many obstacles, I approached every day in the office as a new one and did my best not to let my prior experiences from the other days affect me on a new day, but unfortunately, the rest of the week was more of the same.

The week of June 2nd-6th is when things started to ramp up, but it wasn’t until the middle of the week that this happened. My account creation process began at the beginning of the week, and I was finally given an account. After receiving the account, I was given a “loaner” laptop. On Tuesday, we met with the program director for the contract I currently work for, Scott Rogers. This was a reasonably productive meeting as we were given company merchandise and were able to meet with the leadership of the AFNCR contract with Leidos; after the meeting, my

Michael Opoku-Arthur

June 18th, 2025

Leidos- Cybersecurity & Information Assurance Intern

Reflection #3

Over the next 50 hours of my internship at Leidos, I continued building on the momentum from where I last left off. Much of my time was still allotted to the frameworks I had just been introduced to, including the NIST 800-37, 800-53, and DODI 8510.01. I continued completing the required computer-based training (CBT) and reading through documentation to strengthen my understanding of the Risk Management Framework (RMF). I was okay with the current pace of work because I knew that more tedious times were to come, and although I was working on the same task, it was new information to process every day. On top of that, my experience with my team lead and team had been very encouraging, which made me optimistic.

As I progressed in learning the steps in the 7-step RMF life cycle process, I was starting to get confused. I realized that although I was processing the information, I hadn't yet fully pieced together where my role as an employee would come in to fulfill the goals of the framework. I decided to slow down, take a step back, and truly try to understand where I fit in the big picture. After reaching out and asking my team lead and coworkers the necessary questions, I finally gained the clarity I needed. One important concept I've now grasped is that applying RMF to information systems helps us achieve Authorization to Operate (ATO), which is a vital approval component that comes from government heads ensuring that systems are secure, compliant and can operate in an environment.

