Justin Landolina
UID: 01214163
CYSE 368
July 9th, 2022

Journal #2

Now that I have spent some weeks working as an intern in the Virginia Cyber Navigator program I have developed a greater appreciation for the program, and the work we are doing. Talking to the employees who work in elections offices around the state has shown me how much the people working on the ground care about our election system. They, as well as myself, believe that elections are the cornerstone of democracy. The dedication I have seen from election employees has deepened my respect for what the program is trying to accomplish. Hard work and dedication is in no short supply, we are here to assist and provide cyber security guidance where we can. It has been interesting, and challenging at times, to see the different levels of cybersecurity knowledge across the election offices. It has made it so that no two offices are doing the same thing. Which has been a great learning experience for me being that the ODU team was assigned two localities to work.

Over the past couple of weeks I have continued to work on policy writing for Office A. The majority of my time has been spent working on a media protection plan and a continuity of operations plan. As I have been working on these plans one thing I am realizing is how much depth is needed to make a plan that covers everything. The more I peel back the layers of each plan, the more information I discover that should be included. It feels almost like an impossible task to cover every outcome and how one should react under those circumstances. However, having procedures defined could be the difference between keeping mission essential functions running or not. Fortunately, working through the issues of developing all encompassing plans has helped further along one of my learning objectives, which is to understand how policies are written and improve my policy writing.

For Office B we have started to test our pfSense firewall and OpenVPN server before final installation. The team's goal was to get everything working in the Virtualbox virtual environment before attempting the final install. Getting OpenVPN working in the virtual environment came with its own set of issues and turned out to be an interesting challenge. We spent several days trying to get client and sever talking with each other. We did manage to get the VPN operational using a client on my home network and the pfSense/OpenVPN on a virtual network. This required changing some NAT rules in the firewall, and allowing traffic generated on the private network to enter in via the WAN

port. All of the hardware has been purchased so our next step is to schedule a date for the physical installation.