Bryant Watkins

Reflection Paper 4

Date: 06/26/2025

ODU Summer 2025

Professor Teresa Duvall

TA Ashley Robinson

Internship Reflection Paper: Fourth 50 Hours

Virginia Dept of State Police

This most recent 50-hour span has provided me with an opportunity to learn an in-depth overview of more of the networking devices and the services that they provide for the State Police. There are many key devices that are valuable in providing networking and cybersecurity capabilities, the two I gained more insight on were – the Aviat IRU 600 system and the Nokia 7705 Service Aggregation Router. While we do maintenance the hardware aspect of these devices, we also conduct a review of their functionality as to gain a complete understanding of their processes and importance to cyber operations across the commonwealth. Gaining a complete understanding of our communications network environment further enhances our capabilities and knowledge to service these devices in time of need.

Aviat Networks is a very well-renown company, known for providing many high performance network and security infrastructure to many governments across the United States. The Commonwealth of Virginia is one of those customers, with the Department of State Police utilizing Aviat Networks devices across nearly all RF communication sites. The device most found at these sites are the IRU 600 systems – which possess an additional component known as the Eclipse RAC70. These devices prove to be powerful work horses for the networking and security of State Police communications.

The RAC 70 device is what allows there to be Synchronous Optical Network (SONET) and ethernet traffic for communications. Most consequential, is the fact that this device is capable of providing FIPS 140-2 Level 2 validation. FIPS 140-2 Level 2 validation is a major component to cybersecurity, as this is one of the most robust security standards for telecommunication devices across the United States. This standard entails a requirement for tamper-evidence as well as role-based authentication. Overall, this incredible security standard validates cryptographic module devices' security state.

The other device, the Nokia 7705 SAR, is another networking and security powerhouse that provides many services for State Police communications. The main function of this device is to provide router services. It operates by forwarding packets with internet protocol and multiprotocol label switching data. This device has the capability to perform in adverse agricultural terrain, of which many sites are located, as well as provide some remote services as well. The Nokia 7705 SAR also provides dynamic routing as well as recovery services, proving incredibly reliable and fast-acting.

The cybersecurity capabilities of the Nokia 7705 SAR are also increasingly robust. The quantum-safe networking component ensures the cybersecurity triad is fulfilled for all data crossing the network – confidentiality, integrity, and authenticity. DNS and ICMP replay attacks face an enhanced application-aware firewall that works to repel such attacks. The Nokia 7705 SAR also possesses Trusted Platform Module 2.0 security, allowing for enhanced hardware security through cryptographic keys amongst other functions. The device also only performs boot tasks with the use of trusted software networks, this is done through its use of SR OS secure boot technology. Overall, learning the networking and security capabilities of these devices provides

me an incredible overview that further enhances my understanding of the cybersecurity environment used by the State Police.