1. Which elements of the project are currently underway? Which elements have been completed since the department last updated the JTC? Is the project on schedule with initial plans?

We have implemented and continue to mature the network segmentation component. This element is fully implemented and live. There is a continuous firewall review as part of our steady state operations, as well as a twice monthly review of all firewall requests and changes. As of the last update the review committee has met 6 times.

The SIEM is live and fully tunned. We are in steady state operations and training operators.

We have selected FirePower 4112, Intrusion Prevention System (IPS) devices to replace our current IPS which are going end of support.

We have hired a new security engineer who will monitor and oversee the SIEM and our student SOC.

2. How much money has been obligated and spent at this point? Please break down amounts and spent separately.

Stealthwatch – $104,253

Stellar Cyber SIEM – $294,445

SIEM Staff / SOC - $170,493

FirePower 4112 - $298,166.02

3. What is anticipated to be completed by the next quarterly update?

We have the replacement FirePower devices.

Training will be allocated to SOC/NOC/Security team members.

4. When does the department/institution anticipate that the project will be complete?

We will have purchased and deployed the replacement IPS devices by June 2024 which is the last of our security enhancement objectives.

5. Are there any important concerns or updates you wish to share with the committee?

Our senior security engineer has retired unexpectedly. We have hired a more junior level position to replace the senior security engineer.

6. For multi-phase projects, has there been any insight gained through this phase of the project that will cause changes in the next requested phase of the project?

This is a single-phase project with many objectives.