H.

Vermont Security Operations Center Progress Report

September 27, 2018

Background:

The Agency of Digital Services (ADS) was provided funding, in the budget, to initiate a security operations center or SOC. The goal of a SOC is to detect, analyze, and respond to cybersecurity incidents using a combination of people, process, and technology to provide situational awareness of threats to information systems. ADS recognized that the current workday coverage was insufficient and without a SOC, and the expansion of coverage to 24/7 operations, the State risked an off-hours incident becoming more severe before remediation could begin. ADS opted to partner with the Norwich University Applied Research Institute (NUARI) to leverage their experience, industry connections, and available workforce to provide a quicker and less expensive path to establishing a SOC.

What progress have we made?

It has been a busy three months since we began this project. ADS received notice that the Secretary of Administration's office approved the NUARI sole source waiver. ADS has hired a senior analyst to perform as the SOC coordinator for all the State portions of the SOC partnership. NUARI has appointed a SOC manager, and those key individuals are working through the details on technologies and processes that will be the basis for the SOC. In addition to the hiring progress, ADS has been working on asset verification and assessing the logging capabilities of our current equipment. To date, we have not spent any of the 600,000 dollars allocated for this project. Once we have a signed contract with NUARI, we will have a better timeline of when spending will occur.

Next Steps:

We have started to meet regularly with NUARI to work out contract details. Even though it's taking a little longer than we expected, both sides feel that we are making good progress and that we'll have a signed contract soon. Once complete, ADS can set the training plan and get their employees scheduled for training.

Further Action:

After the start of the calendar year 2019, system setup and initial network and internet traffic analysis will begin. Process evaluation and notification lists will be implemented. NUARI will start incorporating their personnel into our processes and ADS will begin sharing log files. We expect to start slowly and build the volume incrementally until we are in full operation.