Title: **Security Operations Center as a Service (SOCaaS)**

Description of Request:

We are requesting SOCaaS to help us detect, identify, report, remediate and protect our network, data, electronic assets and fiscal integrity. Security Operations Centers are financially demanding; consequently, SOCaaS is a cost-effective alternative to protect our systems with real-time security.

Justification:

1. The enterprise network experienced several incidents that could have been averted during the past month. IT&S Staff need to know as soon as possible when anything of a nefarious nature is potentially occurring within our network. We do not presently possess the cybersecurity tools with the required early warning notification capabilities. It is essential that we are able to effectively monitor our network for abnormal activity 24 hours each day and 7 days each week. We must promptly acquire tools that will help us detect, identify, and protect our electronic assets.
2. SOCaaS will address the following IT Assessment items: 1, 3, 24, 32, 34, 43, and 52,
3. SOCaaS will address the following Security Assessment items: 2.1 ID.AM-5, ID.GV-3, ID.GV-4, ID.RA-1-6, PR.AC-1,5,6,7, PR.IP-7,12, PR.PT-1,4, DE.AE-2-4, DE.CM-1-3,6,7, RS.RP-1.
4. This will allow us to implement, provide information, and manage RS.CO1-5, RS.AN-1-5, RS.MI-1, RS.IM1,2 items from the Security Assessment
5. SOCaaS is needed to proactively fortify our security posture.
6. The most recent cybersecurity event overwhelmed our staff as we had to take immediate security action on thirteen machines. Therefore, it is critical the Information Security Officer position be added in conjunction with a new HelpDesk position. Both positions are necessary to bring our security posture to a bare minimum level of safe staffing in order to effectively address future cybersecurity incidents.
7. Local Governments are now a greater target for malicious attacks, hackers, ransom ware and other treachery. A tally by cybersecurity firm Recorded Future -- one of the first efforts to measure the breadth of the assaults -- found that at least 170 county, city and/or state government systems have been attacked since 2013, including at least 45 law enforcement offices.
8. Our network is complex, complicated, diverse, and expansive. We have a significant amount of expensive hardware on the network and many different types of devices that need to be monitored in real time. It is of critical importance that we are able to see what is happening inside the network, identify devices that are not behaving normally, quickly determine what could be compromised, and protect our cyber-assets immediately instead of reacting to preventable incidents after the fact. We do not have the tools nor resources to actively monitor what is happening. SOCaaS is a fundamental cybersecurity tool for monitoring

network activities, alerting us to anomalies, notifying us of problems that need to be resolved, and helping us in our efforts to protect our IT assets.

9. Arctic Wolf offers Security Operations Centers (SOC)-as-a-service via their Concierge Security Engineers and machine learning capabilities. The detection capabilities are recognized as proactive--seeking out threats that have already penetrated enterprises' perimeters and providing actionable remediations.
10. We have evaluated Arctic Wolf's SOCaaS based upon criteria of our current systems, integration with our systems such as Active Directory, Microsoft Office Portal, and future systems such as Okta. This service will also help us apply PCI, HIPAA, and other regulatory requirements to our environment. Arctic Wolf's SOCaaS will connect with our network devices, servers, and workstations. It will allow us to proactively monitor behavior, actively handle threats, and manage/monitor our logs for any anomalies. It will also alert us about additional prevention and remediation tactics.
11. If we leave our cybersecurity as-is, we would be accepting a 99.9% risk event probability that we will remain vulnerable to security incidents that **will be significantly worse in size, scope, and damage than our most recent cybersecurity attacks**. We do not have the tools a SOCaaS can provide, therefore we have to call in outside resources to help us evaluate, investigate and reactively attempt to remediate security events. We will be attacked by ransomware again. We are also a prime target for bad actors based outside of the United States. Iran, North Korea, Russia, and China are at the top of the list with the most active teams of notorious professional hackers focused on breaching and harming US-based municipal government entities such as Lewis & Clark County and City of Helena.

Projected Cost:

Year 1: $49,210.95

Ongoing: $46,717.91

Contact Information:

Chris Sinrud, Operations Manager/Deputy Director – 447.8322

Mike Glass Senior Network Manager – 447.8348

John Ortman Senior Network Manager – 447.8325

Dawn Temple – Department of Justice Cybersecurity team