Description

The State Information Technology Services Division (SITSD) is responsible for managing and protecting the network used by all State agencies in support and service to Montana's citizens. The Montana Cybersecurity Enhancement Project (MT-CEP) consists of multiple initiatives to protect citizen's data through investments in the people, processes, and technology protecting the State's information assets.

Scope

The "Montana CAREs" initiative will benefit local and tribal governments, K-12 schools, and other public institutions across Montana. The other initiatives in this project will benefit State agencies and the citizens they serve.

Risks

If the State suffers a large cyber incident or cyber breach without this funding to limit the scope and impact, then we run the risk of exposing our citizen's most sensitive information, interrupting critical State services to our citizens, harming the State's reputation, decreasing the State's credit rating, and increasing the State's insurance costs.

Benefits

These initiatives will enhance the State's resiliency against inevitable cyber incidents and potential cyber breaches. No amount of funding can guarantee full protection against all cyber attacks, but purposeful and strategic investment in the people, processes, and technology protecting our State's information assets will limit the scope and impact of cyber incidents and cyber breaches.

Initiatives ($4,969,307)

In selecting these initiatives, we considered the current threat environment, ranked the risks, analyzed the gaps, identified potential solutions, weighed the solutions, distributed investments across security layers, and sought synergies with other strategic initiatives for additional benefits to the enterprise.

1. Upgrade internal firewalls ($1,130,000)

The internal firewalls are approaching End of Life and require upgrading to remain eligible for vendor support and patches. This initiative is to upgrade the internal L4 network firewalls to L7 application firewalls that will give us better visibility of traffic, finer granularity of control, and additional protection against sophisticated cyber attacks. Additionally, this initiative will enable us to scale infrastructure and bandwidth to keep pace with agencies' growing network needs.

2. Backup and classify data ($400,000)

Failure to backup important data could lead to unrecoverable data loss due to hardware failures, misconfigurations, data corruption, disasters, ransomware, etc. This initiative is to identify all data that should be backed up, to backup that data, and then to classify that data to ensure appropriate

security and privacy controls are applied. Additionally, this initiative will enable the State to perform full disaster recovery test, validating the State's backup and recovery capabilities.

3. Implement third-party patching solution ($100,000)

Applications that are not patched in a timely manner can be exploited to harm the State's information assets or compromise our citizen's data. This initiative is to implement a third-party patching solution to simplify, standardize, and automate patching third-party applications, reduce the time it takes to patch third-party applications, and to gain better visibility of our third-party patching status to achieve a better understanding of the our risk posture.

4. Implement enterprise password manager ($250,000)

Every employee develops their own method to manage their passwords, leading many employees to use weak passwords or reuse passwords at work that they use at home. Poor password habits lead to cyber attacks such as credential stuffing that utilize weak, compromised, or stolen credentials. This initiative is to implement an enterprise password manager to securely store passwords, increase password strength, and ensure individual accountability for shared accounts.

5. Implement SIEM data stream processor ($350,000)

Charges for the SIEM tool are based on the amount of data that is processed, decreasing how much data we can process or increasing how much we need to pay for that data. A SIEM data stream processor does not charge by data throughput, so it can be used to determine which data should be sent to the SIEM tool. This initiative is to implement a data stream processor to reduce the amount of data sent to the SIEM tool and reduce related ongoing costs of the SIEM tool.

6. Implement offensive security tools ($300,000)

To protect data in today's sophisticated threat environment, security teams must develop offensive security capabilities to identify vulnerabilities before cyber threat actors exploit them. Offensive security looks at the organization with an external perspective just like a hacker. This initiative is to implement threat hunting and penetration testing tools to validate the State's security controls are implemented and functioning as expected to protect our data.

7. Implement CASB solution ($500,000)

As state agencies increasingly adopt different cloud solutions, it becomes increasingly difficult for the State to keep track of where its data is located and what type of data is in each cloud. This initiative is to implement a Cloud Access Security Broker (CASB) to serve as a policy enforcement point to identify all the State's data in every cloud service and ensure the State's security policies are enforced based on data classification and regulatory requirements.

8. Implement DMARC solution ($200,000)

Email is a State employee's primary communication tool, it is also a cyber threat actor's primary hacking tool; many states and local governments have been losing large sums of money where a hacker spoofs a vendor's email address to commit fraud that costs more than this initiative. This initiative is to implement a DMARC (Domain-based Message Authentication Reporting and Conformance) solution to protect against email cyber attacks by validating the sender of emails.

9. Joint Security Operations Center ($800,000)

Managing massive amounts of security information from multiple systems and taking risk-prioritized actions on that data is overloading security and technology teams with repetitive analysis and exhausting our limited resources. This initiative is to continue participation in a Joint Security Operations Center in partnership with other states to combine security operations resources and to share intelligence, playbooks, and augment specialized security expertise in each state.

10. Fund cybersecurity training ($464,307)

Technology is quickly evolving, and security staff need continuous training to keep up. Internet of Things, Cloud Computing, and emerging technology present the greatest risks to organizations because they are funded and adopted without consideration for how they will be secured. This initiative funds security training for staff in Security Services, NOSC, National Guard, and agency security teams so they will be able to adequately secure new and emerging technology.

11. Implement application security tools ($225,000)

Application security is critical because programs interact with data and unsecured code can be exploited to harvest credentials and steal data. Detecting vulnerabilities early in the software development lifecycle is necessary to reduce development costs and increase application security. This initiative is to implement code analysis tools to thoroughly analyze source code and test applications to identify misconfigurations or other errors that create security vulnerabilities.

12. Fund Montana CAREs ($250,000)

Local, tribal, and territorial governments, schools, and other public institutions in Montana are frequently targeted by hackers deploying sophisticated tools to lock or steal sensitive data or interrupt their services. Many public institutions lack the communication, assessment, response, and enhancement capabilities to protect their organizations in today's quickly evolving threat environment. Recognizing that cybersecurity it not a state government problem, but a statewide problem, this initiative takes the first steps to implement the Whole-of-State cybersecurity approach to utilize state-local partnerships to combine our resources and become "Stronger Together". Montana CAREs (Communication, Assessment, Response, and Enhancement services) is a multi-agency organization consisting of the Fusion Center (MATIC), the National Guard, DOJ IT, and the CISO's team that provides information sharing, security assessment, emergency response, and program optimization services to reduce risks in the public sector across the State.

Justification

Public sector organizations are favorite targets for hackers because we process, store, and transmit our citizen's most sensitive information and we are underfunded and understaffed compared to our private sector counterparts. This purposeful and strategic investment in cybersecurity will limit the scope and impact of costly cyber attacks and reduce the recovery costs needed after a cyber incident or cyber breach.