Infrastructure Appropriations for the Equipment Project

Description:

The Iowa Communications Network (ICN) has received appropriations to replace and upgrade equipment that is reaching its end of functional life. The following is an explanation of the multi-year equipment replacement project funded by the appropriation. The ICN currently provides Firewall and DDoS (Distributed Denial of Service) protection at no cost to the Executive branch and for the benefit of a number of Judicial, and Legislative branch agencies.

State Firewall Equipment / DDoS (Distributed Denial of Service) Mitigation System:

System designed as a tightly integrated, multi-layered cyber defense for Legislative, Judicial, and Executive Branch agencies. Designed to prevent unauthorized access to or from their networks.

- All traffic entering or leaving passes through the state firewall which examines and blocks the traffic that does not meet the specified security criteria.
- Protects confidential information from those not authorized to access it.
- Protects against malicious users and incidents that originate outside users' networks.

DDoS Mitigation services are based on software and hardware that provide high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors that if needed can be mitigated on designated DDoS appliances.

1. **Detection**: Continuously monitor the number and size of packets and flows as they navigate (traverse) the ICN network going to and from customers' networks.
2. **Mitigate:** Traffic is remediated by being routed through ICN infrastructure that filters out the DDoS attack traffic allowing customers' Internet connection or other web-connected targets to focus on legitimate traffic.
3. **Report:** ICN can provide information to customers including attack duration, protocols and ports attack traffic is utilizing, all source (attacker) IP address', and the number of packets and connections making up the attack.

Progress:

ICN has moved forward and replaced our legacy centralized firewall. The new Next-Generation Firewall provides a decentralized platform that allows a single plain of glass for support that WILL tailor security services based on individual agency's needs. This is a 2-phased approach. This first phase is to upgrade the security infrastructure followed by a second phase that takes all the customers from behind the state firewall and moves them to their own individual appliance.

Phase 1 is complete. Now Judicial, DHS, ICN and OCIO/State firewalls are all operating independently on new Next-Generation firewalls. Phase 2 is moving forward, and new facilities are being designed and will be implemented by December 2023.

In addition to the firewall solution, the ICN is redesigning/upgrading the DDoS/Security platform. The platform is being moved out to the edge of the network to leverage network efficiencies, reduce bandwidth utilization, increase speed to respond to DDoS events, and reduce the attack surface associated with DDoS attacks. This allows for better failover and improves detection, mitigation, and reporting.

The DDOS upgrade requires a redesign of the network. This includes the purchase of additional devices that range from mitigation equipment, optical taps, routers, and security software. This should be completed over the next 3 to 5 months. The end goal is to deliver security services that provide confidentiality, integrity, and availability of information throughout Iowa.

Total Estimated Cost of the Projects:

Table 1. Appropriations and Spending for the Equipment Project

Revenue Sources	Fiscal Year	Appropriated Amount	Expended	Encumbered	Balance	Percent Complete	Est. Completion Date
09439223	2023	$1,510,724	$0	$ 0	$1,510,724	0%	6/30/2024
09439221	2021	$2,071,794	$ 1,735,237	$ 299,699	$336,557	85%	06/30/2022