

# 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, and for the benefit of, a number of Executive, 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 is in the process of replacing a centralized firewall platform that was end of life. The ICN will provide a decentralize firewall platform to allow state agencies the ability to tailor their security platform based on their individual needs/requirements. The upgrade/replacement of the existing firewall is a 6 to 9 month process to design, configure, and install a NextGen firewall platform to secure all agencies within the State of Iowa. The ICN is currently in the installation phase of the project and is approximately 70 percent complete. Network designs and configurations are complete. The installation phase has 6 to 8 weeks left.

In addition to the firewall, the ICN is reconfiguring the DDoS/Security platform to leverage network efficiencies, while building in network (MPLS) redundancy. Security infrastructure is being moved to the ingresses, where the Internet enters the Network, to address security situations at the point-of-entry. This allows for immediate detection, mitigation and reporting of security events coming from the Internet.

Additional DDoS mitigation equipment, optical taps, and routers are in the process of being purchased and installed. This solution will also assist other agencies with information that assist their security tools as well. This project should be completed within 3 to 6 months.

## 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
09439221	2021	\$2,071,794	\$ 1,081,153	\$ 0	\$990,641.31	70%	06/30/2022