Iowa Communications Network

A State-of-the-Art Fiber Optic Network

Network Facts

Secure Network

The ICN operates a private (closed) state-of-the-art fiber optic Network that provides telecommunications services to authorized and certified users.

- **DDoS Mitigation Platform:** Services include high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors that if needed can be mitigated.
- **Disaster Recovery Site:** Established an additional disaster recovery site that further enhances network redundancy, provides a diverse fiber path, and enhances disaster recovery operations for all users.
- **Carrier-Grade Testing Lab:** A telecommunications technology test facility, that allows ICN to operate efficiently as a carrier and establish a standards based approach to evaluate new technologies.

Common Carrier Designation - E-Rate Funding

ICN began its participation in the Universal Service Fund program in FY 2001, as a common carrier.

As a result of ICN's status as a common carrier, education and healthcare users can access federal funding that subsidizes the costs of eligible telecommunications services.

- ICN's education and healthcare users received approximately $6.3M in federal USAC funding for FY19.
- To receive discounts, users are required to use competitive bidding and award based upon best value (primarily cost).
- ICN's Common Carrier status is in part based on the autonomy of the Commission (ITTC) in the oversight of the Network.

Public Private Partnerships

ICN managed services incorporate premium partnerships with the private sector.

- Fiber Network Services, network maintenance provider (Iowa based).
- CenturyLink, managed voice provider.
- LightEdge, managed firewall provider (Iowa based).
- Pratum, managed security provider (Iowa based).
- Private Sector Telecommunications, ICN partners with the private sector for leased fiber connections.
  - In Fiscal Year 2019, ICN reinvested $9.6M of revenue for private telecom services.

Authorized Users

Education

Locations Served:

- 348 Public & Private K-12 locations
- 9 Area Education Agencies (AEA) (45 sites)
- 15 Community Colleges (30 sites)
- 3 Regents
- 20 Private Colleges

Healthcare

Locations Served:

- 101 Hospitals
- 178 Clinics and other Healthcare Providers
- ICN manages Iowa Hospital Associations' healthcare broadband network (IRHTP).

Government

Locations Served:

- 133 Judicial Branch locations
  Connections to all county courthouses.
- 265 Dept. of Transportation locations
  Connections to maintenance garages, driver's license stations, and construction offices.
- 158 Dept. of Human Services locations
  Connections to DHS offices across the State.
- 59 Workforce Development locations
  Connections to satellite offices.
- 231 additional State, Federal, miscellaneous government locations

Public Safety

Locations Served:

- 113 Iowa Homeland Security & Emergency Management PSAP locations
  Public Safety Answering Point (PSAP) for NG911.
- 179 Dept. of Public Safety and Homeland Security locations
- 38 Iowa National Guard locations

For additional information: Mark Johnson, Chief Operating Officer | Office: 515-725-4608 | Cell: 515-554-2787

Major Initiatives

Network Redundancy / Core Network Upgrade

Efforts continue to increase redundancy for the protection of critical users and uses, as well as provide disaster recovery functionality that will benefit all authorized users.

- **Core Upgrade Details**: 100GB native core with all counties currently connected with a 10GB capable backbone.
  - Scalable capacity to meet increased demand for services of up to 200GB as needed.
- Enables the ICN to proactively manage the increasing current and future bandwidth needs of our users.
- Sufficient capacity at the Core to securely carry the State's data traffic, without degradation.

Healthcare Dedication

Healthcare facilities are connected to either the ICN network or the Iowa Hospital Associations' (IHA) network.

- Serving 279 hospitals and clinics; providing critical broadband and Internet services.
- Iowa Hospital Association Partner (since 2008).
  - Technical, engineering, and maintenance provider of the Iowa Rural Health Telecommunications Program (IRHTP).
  - Project management and deployment of a complete network upgrade on behalf of the IHA. The ICN is upgrading equipment at 191 locations.
    - Enhances redundancy to hospitals and clinics.
    - Increases bandwidth availability to enable improved access to specialists and records.

911 Partnership with Iowa Homeland Security & Emergency Management (HSEMD)

- Providing a closed secure network for 911 wireless calls.
- Providing infrastructure and services for merging the existing wireline carrier network, consisting of all the State's wireline service providers, onto HSEMD's Next Generation 911 (NG911) IP network.
- Providing colocation facilities and transport services for a Hosted Public Service Answering Point (PSAP) solution. Results in the consolidation of equipment expenses.

Managed Voice Service (MVS)

ICN provides MVS to authorized users on the Capitol Complex and Statewide, as well as to education users.

- 153 active user groups, with over 7,600 seats.
- Provides relocation benefits during disaster recovery, no long distance or 800 expenses, and call encryption.
- Eliminated approx. $1.1M appropriation that supported telecommunications services on the Capitol Complex.
- Voice services on the Capitol Complex transitioned to the ICN during the 1990's.

Security Services

A top priority is creating and deploying security services for our users, to assist in protecting their networks.

DDoS Mitigation

Mitigation solution allows Internet traffic to be "cleaned" and returned to user with little impact on service.

During the Last 12 Months:

- Detected 8,860 DDoS attacks on the State's Network.
- Longest DDoS attack was 11 hrs, 31 mins, 29 secs.
- Largest DDoS attack was 4.38TB (Terabyte).
  - Sustained 2-3 Gbps for 6 1/2 hours targeting a high school in October.

Firewall

All Network traffic entering or leaving passes through the State Firewall which examines and blocks the traffic that does not meet the specified security criteria.

- State Firewall: Hosted and Managed by the ICN.
  - Protects confidential information from those not authorized to access it.
  - Protects against malicious users and incidents that originate outside users' networks.
- Managed Firewall Service.

For additional information: Mark Johnson, Chief Operating Officer | Office: 515-725-4608 | Cell: 515-554-2787

Iowa Communications Network

FY 2021 Appropriation Request

Fiscal Year 2020-21 Appropriation Request

$2,071,794 (Governor's Budget Recommendation) – Firewall & Distributed Denial of Service (DDoS) Mitigation Services

The ICN currently provides Firewall and DDoS protection at no cost to most state agencies, but the protection provided ultimately benefits all State government entities. To ensure the continuation of these critical cyber protection services, the ICN seeks an appropriation for the costs of those services. Specifically, the requested funding will be used for the following activities:

- Redesigning current network architecture, as necessary, for improved security.
- Upgrading existing network security equipment to maintain carrier grade services.
- Ongoing maintenance of the security equipment.

The total funding request is based upon costs incurred by the ICN in providing the current level of security.

Background

- Need to assure State government agencies have a baseline level of protection from cyber-attacks.
- Currently utilizing funds intended for necessary network equipment replacement and network upgrades.

Service Information

State Firewall

- ICN has operated/maintained the State Firewall since the 1990's.
- Additional installations and upgrades have been implemented over time to insure operational integrity.
- 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 these networks.
- All traffic entering or leaving passes through the state firewall which examines and blocks the traffic that does not meet the defined 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

- A second part of a layered cyber defense.
- DDoS Mitigation system inspects the Internet traffic and filters out any malicious packets.
- *During the Last 12 Months:*
    - Detected 8,860 DDoS attacks on the State's Network.
    - Longest DDoS attack was 11 hrs, 31 mins, 29 secs.
    - Largest DDoS attack was 4.38TB (Terabyte).
        - Sustained 2-3 Gbps for 6 1/2 hours targeting a high school in October.

For Additional Information:
Mark Johnson, Chief Operating Officer | 515-725-4608 | mark.johnson@iowa.gov
Deb Evans, Chief Financial Officer | 515-725-4698 | deb.evans@iowa.gov

Critical DDoS Mitigation Functions

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. **Mitigation** >> 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. **Reporting** >> ICN can provide information to customers including attack duration, protocols and ports the attack traffic is utilizing, all source (attacker) IP address', and the amount of packets and connections making up the attack.

Equipment Descriptions

Firewall

A firewall is recognized as the first line of defense in securing sensitive information by using software to maintain the security of a private network. A firewall is a hardware or software-based appliance that prevents unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the Intranet (the local network to which you are connected) must pass through the firewall, which examines each packet and blocks those that do not meet defined security criteria.

- ICN has operated and maintained the State Firewall since the 1990's.

Gigamon: DDoS Mitigation

Network software/appliance that sends a copy of traffic from Internet routers to Flowtraq and other security tools including the OCIO. This allows the ICN Network's minimally invasive solution to monitor without added disruption to the production Network.

- Initial installation: 2011 with additional installations and upgrades implemented over time.

Flowtraq: DDoS Mitigation

Software that monitors Network flows to detect a range of network behaviors that identifies and provides alerts on DDoS attacks. When traffic thresholds are exceeded, Flowtraq will divert the traffic from the Internet routers to the A10.

- Initial installation: 2015 and 2016.

A10: DDoS Mitigation

Network appliance that does the mitigation of DDoS attacks. When attacks are identified traffic is diverted from the Internet routers to the A10. The A10 filters out the bad traffic and returns the legitimate traffic back to the Internet routers to continue on to customer networks.

- Initial installation: 2015 and 2016.

For Additional Information:
Mark Johnson, Chief Operating Officer | 515-725-4608 | mark.johnson@iowa.gov
Deb Evans, Chief Financial Officer | 515-725-4698 | deb.evans@iowa.gov