Background

• December 21, 2015, Governor Branstad issued Executive Order 87 (EO87); a cybersecurity initiative for the State of Iowa.

• Executive Order 87 establishes a multi-agency partnership
  • Office of the Chief Information Officer
  • Iowa National Guard
  • Department of Public Safety
  • Iowa Communications Network
  • Iowa Homeland Security and Emergency Management Department.

• Strategy delivered to the Governor’s Office July 1, 2016.
Scope of Strategy

- Primary focus of the strategy is lifeline critical infrastructure sectors (Communications, Energy, Transportation, and Water & Wastewater) and state government as it relates to the protection of citizens and digital government services.

- The strategy does not include detailed operational plans.

- At the direction of the Governor’s Office and Iowa Legislature, the EO87 Leadership Team will prepare an operational plan, budget, and timelines based on the accepted recommendations.
Iowa Cybersecurity Strategy

1. Protecting Lifeline Critical Infrastructure
2. Risk Assessment
3. Best Practices
4. Awareness Training
5. Public Education and Communication
6. Collaboration
7. STEM (Science, Technology, Engineering, Math)
8. Data Breach

Iowa Emergency Response Plan
Protecting Lifeline Critical Infrastructure

“Address high risk cybersecurity areas for the state’s critical infrastructure and develop plans to better identify, protect, detect, respond and recover from significant cyber incidents.”
“Establish a process to regularly assess cybersecurity infrastructure and activities within the State.”
Best Practices

“Provide recommendations related to securing networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, and destructions of data held by the State of Iowa.”
Awareness Training

“Implement cybersecurity awareness training for State government.”

**Recommendations:**

4.1 - Require general cybersecurity awareness training for all State of Iowa employees and additional specialized cybersecurity awareness training for employees with privileged access. Conduct regular testing to measure the overall effectiveness of the training

4.2 - **Further educate** State of Iowa leadership on cybersecurity risk and their roles and responsibilities.

4.3 - Create a cybersecurity training environment to facilitate cross agency training.
Public Education & Communication

“Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public’s personal information.”

**Recommendations:**

5.1 Institute a public cybersecurity awareness and literacy campaign to improve the cybersecurity awareness of Iowans and promote good cyber hygiene.

5.2 - Facilitate and sponsor an annual public and private cybersecurity conference.

5.3 - Provide cybersecurity awareness and literacy curricula and support materials for K-12 and college students.
Collaboration

“Collaborate with the private sector and educational institutions to implement cybersecurity best practices.”

Recommendations:

6.1 - Improve and enhance current partnerships with educational institutions to identify cybersecurity best practices through internships and faculty expertise.

6.2 - Conduct cybersecurity training exercises across Executive Branch agencies and lifeline critical infrastructure sector partners.

6.3 - Identify, create, review and update legal agreements between collaborative partners to improve information sharing, preparedness and incident response.

6.4 - Expand private sector partnership programs to promote the sharing of criminal and cyber-threat information affecting the private sector in Iowa.
“Recommend Science, Technology, Engineering, and Math (STEM) educational and training programs for K-12 and higher educational programs in order to foster an improved cybersecurity workforce pipeline.”

Recommendations:

7.1 - Incentivize Iowa students to pursue careers in cybersecurity through the creation of scholarship programs modeled after programs such as the Federal Cyber Corps; Scholarship for Service program, the AmeriCorps Model, the Military GI Bill, and others.

7.2 - Provide and encourage pathways to cybersecurity careers from K-12 through higher education.

7.3 - Conduct a review of the cybersecurity workforce requirements for the Executive Branch and recommend necessary adjustments.
Data Breach

“Establish data breach reporting and notification requirements.”
Iowa Emergency Response Plan

“The Iowa Homeland Security and Emergency Management Department shall update the State’s Emergency Response Plan to deal with the physical consequences of a significant cyberattack against the State’s critical infrastructure.”
Alignment with 4E
Enlighten, Engage, Educate, Employ

- 4 pillars that are needed to increase the cyber workforce.
- Iowa State University along with 200+ partners developed methods for each pillar to be successful.
Jeff Franklin
State of Iowa Deputy CIO and Chief Information Security Officer
(515) 281-4820
jeff.franklin@iowa.gov