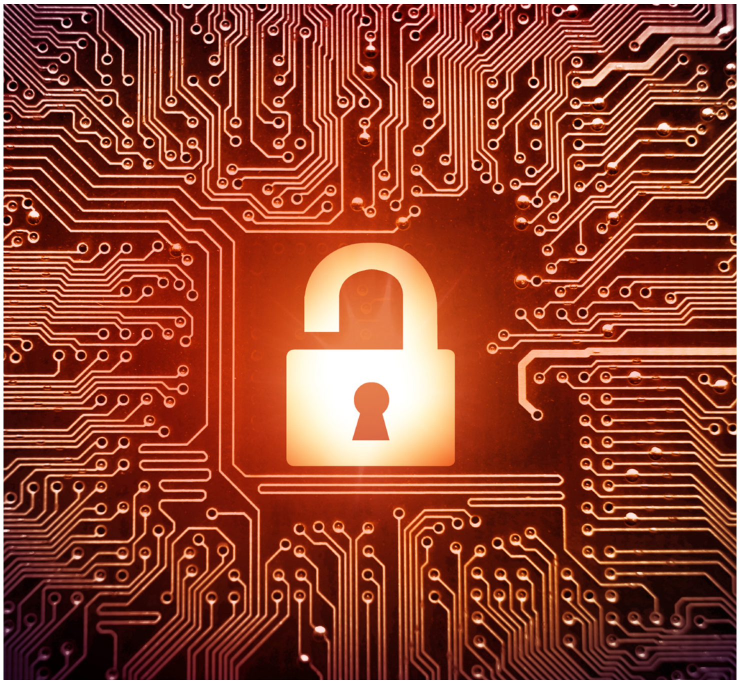
State of Iowa
Cybersecurity Strategic Plan



JULY 2019

Since the launch of the 2016 Iowa Cybersecurity Strategy, the Office of the Chief Information Officer continues to lead the Governor's Cyber Working Group to sustain Iowa's strong cybersecurity posture. The recommendations in the 2016 Strategy have provided a foundation for this multi-agency partnership to further define and fulfill their critical role in protecting state government from constant cybersecurity threats.

We continue to work together to promote and develop solutions to address all the cyber-related challenges we face in Iowa.

To develop this strategy, we surveyed a select group of individuals with security responsibilities in both Iowa state agencies and counties. This group of stakeholders were invited to participate in the development of this strategy. We collectively explored the following components that make up this strategy: Mission, Vision, Purpose, 9 Core Values, 25 Objectives and 9 Goals.

The focus of this engagement was to identify current needs and to strategize objectives designed to mitigate current trends in cybersecurity. By doing so, we improve identification, protection, detection, response and recovery as it relates to the protection of Iowa's critical infrastructure and citizens.

Stakeholders

These groups were identified and invited to participate in the development of this strategy.

Office of the Chief Information Officer

Iowa Department of Human Services

Iowa Vocational Rehabilitation Services

Iowa Department of Revenue

Iowa Communications Network

Iowa Homeland Security & Emergency Management

Iowa Secretary of State

Iowa Economic Development Authority

Iowa Lottery

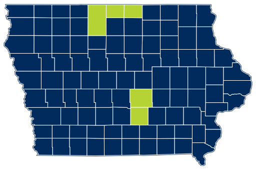
Iowa Adjutant Generals Office

Iowa Department of Transportation

Iowa Department of Public Safety

Iowa Public Employees Retirement System

Iowa Department of Public Health



Jasper County
Kossuth County
Marion County
Winnebago County
Worth County

Index: Table of Contents

Introduction

Mission

Securing and improving Iowa through effective cybersecurity practices by providing a framework for identification, detection, protection, response and recovery from threats.

Vision

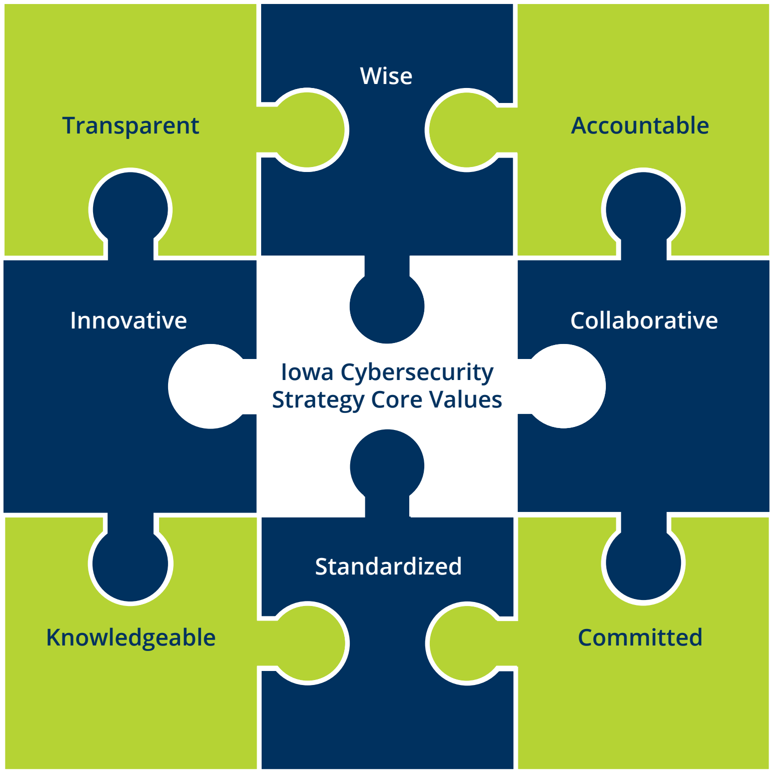
Iowa will be the leader in cybersecurity best practices through collaboration and innovation to meet the challenges of the future.

Purpose

To protect Iowa from cybersecurity threats by creating a consistent, safe and secure technology environment.

Core Values

Transparent	- Providing honest and accurate threat prevention capabilities
Wise	- Being one step ahead of cyber attacks
Accountable	- Being responsive protecting Iowa’s resources
Innovative	- Implementing unprecedented approaches towards protecting and responding to threats
Collaborative	- Working with our partners to prevent cybersecurity breaches
Knowledgeable	- Consistently educating ourselves and our citizens
Standardized	- Providing a universal platform for cybersecurity prevention and response
Committed	- Providing dedicated efforts to protect Iowa



Strategic Goals

These goals provide a clear direction for addressing how we can continue to ***Detect, Protect*** and ***Respond*** to cybersecurity threats in Iowa. By identifying the needs and objectives to achieve these goals, we can better understand our current state and cybersecurity position. We will foster and ultimately enhance the controls we have in place today to continue to mitigate all potential cyber risks.

- Increase identification of threats
- Provide tools for prevention of threats
- Reduce exposure and risk
- Improve collaboration
- Train and increase awareness
- Explore funding
- Establish analytics and metrics
- Enhance communication
- Develop a cybersecurity workforce

Strategic Goal 1
Increase identification of threats

Objective 1.1 – Review and remediate legacy software and develop future plans

- OCIO working with agency/county application teams will review and remediate legacy software for potential cybersecurity risk and develop plans to replace, upgrade or decommission the software.

Objective 1.2 – Ensure all security risk business processes meet regulatory requirements

- OCIO Information Security Division or the Auditor of the State will ensure that all business processes that involve security risk meet regulatory requirements by providing identification, recognition and remediation of past and current business processes and practice.

"While next-gen technology like Artificial Intelligence (AI) and Machine Learning (ML) are transforming many enterprises for the better, they've also given rise to a new breed of 'smart' attacks. The ability to scale and carry out attacks is extremely enticing to cybercriminals, including use of intelligent malware. The rise in next-gen threats means that security professionals must be extra vigilant with detection and training against these threats, while also adopting new methods of automated prevention methods"
—John Samuel, Senior Vice President and Global Chief Information Officer, CGS

Strategic Goal 2
Provide tools for prevention of threats

Objective 2.1 – Implement an automated notification toolset for agencies

- OCIO Information Security Division should implement an automated toolset to notify agencies and counties of cybersecurity events in real time and provide monthly and annual reports of triggered events as a summary increasing the number of subscribers/clients by 1000 each year.

Objective 2.2 – Develop a State of Iowa Cloud Security Strategy

- Develop a State of Iowa Cloud Security Strategy and publish the strategy along with a master service agreement for identified tool sets.

Objective 2.3 – Provide methodologies and standards for prevention of threats

- OCIO's Information Security Division will provide methodologies and standards for access control, multi-factor authentication, identity management, next-generation firewalls, VPN access, SSL decryption and mobile device management to be verified during the yearly State of Iowa ISD audit.

Objective 2.4 – Develop a framework of standardization of tools

- OCIO or designee will develop a framework providing standardization of cybersecurity prevention tools that is flexible and cost-effective and addresses threats such as ransomware, phishing, spoofing, and malware to include the measurement of security spending, calculation of potential loss and attack analysis metrics.

Objective 2.5 – Establish key performance metrics

- The State of Iowa's Information Security Division Cybersecurity Manager will establish and identify key performance metrics for detecting potential cybersecurity threats and provide for a monthly evaluation of identified metrics.

Objective 2.6 – Develop an automated reporting tool for cybersecurity metrics

- OCIO Information Security Division will develop an automated reporting tool to document identified cybersecurity metrics and key performance indicators.

Strategic Goal 3
Reduce exposure and risk

Objective 3.1 – Conduct annual security risk assessments

- Risk assessors will conduct annual security risk assessments for the counties and agencies to be completed annually.

Objective 3.2 – Create a security standard for outsourced services

- OCIO's Chief Information Security Officer or designee will create a security standard for outsourced services and perform contract reviews to ensure compliance requiring that all contracts contain satisfactory language that meet the minimum legal and security standards established by the State of Iowa.

Objective 3.3 – Supervised penetration testing

- The OCIO Cybersecurity Liaison will supervise penetration testing for all counties and state agencies processing one fourth of participating groups annually.

Objective 3.4 – Perform annual simulations and recovery exercises

- Each agency or county IT director will arrange an annual series of simulations and recovery exercises to determine susceptibility of users to phishing and other schemes through cybersecurity attacks annually.

Improve collaboration/Train and increase awareness

Strategic Goal 4
Improve collaboration

Objective 4.1 – Assist all state and local agencies with cybersecurity reviews

- OCIO will assist all state and local agencies in completion of the MS-ISAC Nationwide Cybersecurity Review providing a yearly benchmarking report.

Objective 4.2 – Streamline and standardize all incident response

- OCIO's Information Security Division will standardize and streamline all incident response processes and procedures to identify and remediate ransomware, phishing, spoofing, and other cybersecurity events.

Strategic Goal 5
Train and increase awareness

Objective 5.1 – Develop a standardized cybersecurity strategy

- OCIO CISO should develop a standardized cybersecurity strategy.

Objective 5.2 – Develop a threat education and awareness program

- OCIO should develop a comprehensive cybersecurity threat education and awareness program.

> "The most important part of the equation alongside IT modernization and treating data as a strategic asset is getting talent to the table, and it is the one that I think is the most challenging because, not only in government, but also in industry, we don't have as much of a pipeline as we would like for cybersecurity specialists or data scientists."
> **- Federal Deputy CIO Margie Graves**

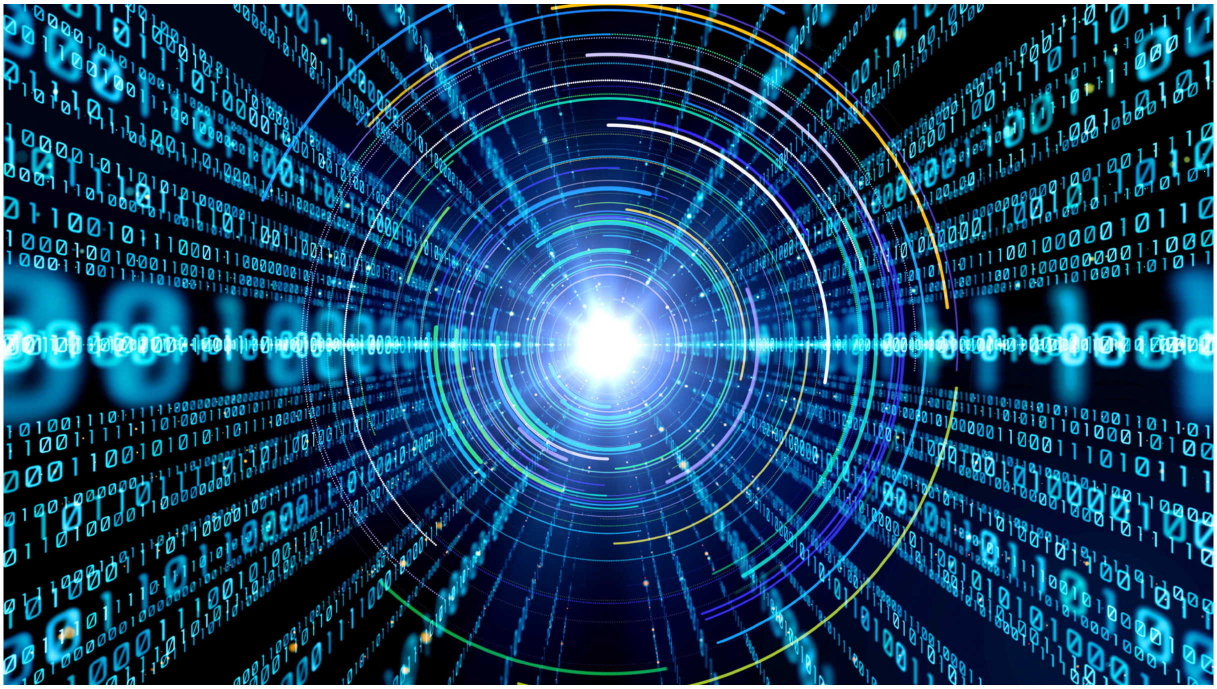
Strategic Goal 6
Explore funding

Objective 6.1 – Develop funding mechanisms to provide cybersecurity identification and prevention

- OCIO CISO will work with stakeholders and lawmakers to develop funding mechanisms to provide cybersecurity identification, prevention and remediation.

Objective 6.2 – Provide cybersecurity response to Iowa agencies and counties

- OCIO's Chief Information Security Officer will develop funding mechanisms to provide cybersecurity response to Iowa agencies and counties to include at least three funding options such as cooperative agreements, internships and outsourcing.



"Cyber attacks can be destructive, debilitating and prevent the distribution of critical government services. It is crucial for Iowa to maintain a clear and precise direction for the protection of our citizen's personal information. This strategy continues to promote our vision and our commitment to secure Iowa."
- Jeff Franklin, Director & State CIO of Iowa

Establish analytics and metrics

Strategic Goal 7
Establish analytics and metrics

Objective 7.1 – Develop an automated reporting tool for analytics and metrics

- The Information Services Division will develop an automated reporting tool with clear escalation pathways for reporting analytics and metrics to executive leadership documenting the toolsets and implementation schedules.

Objective 7.2 – Generate key metrics and comparative benchmarks

- Information Security Division leadership will identify key metrics, KPIs, and benchmarks for all state agencies and counties for detecting potential threats generating comparative benchmarks for improving cybersecurity threat prevention.

> “In the 2014 US State of Cybercrime Survey by PricewaterhouseCoopers, 42% of respondents said security education and awareness for new employees played a role in deterring potential attacks. The financial value of employee awareness also was compelling, the report found, as companies without security training for new hires reported average annual financial losses of $683,000, compared with companies with training that said average financial losses totaled $162,000.”
> **- Paul Armstrong, Security Specialist**

Strategic Goal 8
Enhance communication

Objective 8.1 – Develop a comprehensive cybersecurity communication plan

- OCIO will develop a comprehensive cybersecurity communication plan to ensure consistent and reliable communication for reporting metrics and breaches.

Objective 8.2 – Assist agencies and counties with the development of a framework to improve and develop response plans

- OCIO will develop a response plan template that agencies and counties can use as a framework to improve or develop their own response plans.

Objective 8.3 – Provide monthly reports for cybersecurity events to executive leadership

- OCIO should develop reports designed to document detected cybersecurity events and responses to provide to executive leadership on a monthly basis.

Objective 8.4 – Develop specialized training and awareness of security services

- OCIO should develop specialized training and awareness of available security services and develop an awareness program for agencies and counties to facilitate end-user activity.

Objective 8.5 – Develop a plan to improve response time

- Homeland Security Emergency Management Department in conjunction with OCIO should develop a mutual aid agreement plan for cyber response to reduce response time that is published.

Strategic Goal 9
Develop a cybersecurity workforce

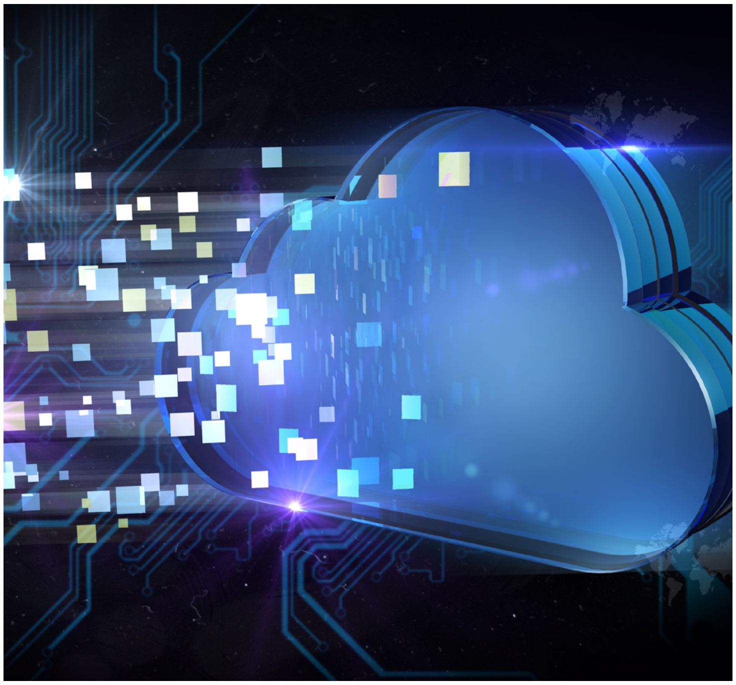
Objective 9.1 – Identify roles and responsibilities for cybersecurity functions

- OCIO's Information Security Division will identify roles and responsibilities for cybersecurity functions for employees within state agencies and counties.

Objective 9.2 – Identify cybersecurity competencies

- OCIO's Information Security Division will identify all cybersecurity competencies for state/local government personnel.

> "Governments operate on procurement cycles that are often out of step with the pace of IT innovation. In the marketplace battle for talent, governments struggle to offer competitive pay for IT professionals. Consequently, municipal-government computer systems tend to be old and basic cyber-hygiene is often neglected."
> **- Tyler Moore, Washington Post**



Office of the
Chief Information Officer

CIO@Iowa.gov
515-281-5503