

CYBERSECURITY WORKING GROUP STRATEGY ON A PAGE FOR 2015 – 2016

Vision Statement - A secure and resilient cybersecurity environment which facilitates and protects the business of the state of Illinois, reduces risk and protects privacy, while promoting innovation, economic growth and transparency.

State of Cybersecurity in 2015

Top Characteristics of the Initial State

- Lack of measurable outcomes as applicable to cyber security which display value to stakeholders.
- Inconsistent executive support regarding the prioritization of cyber security. Lack of specific authority and processes to direct resources to address critical security controls at state agencies. Competing priorities between security and business resources. Lack of wide understanding of the criticality of enterprise information security.
- Lack of a comprehensive security awareness program.
- Cybersecurity efforts and teams are decentralized and lack common standards and direction.
- Lack of uniformity on how security standards are applied. Lack of implementation of critical security controls and lack of consistent inventory practices for cyber-assets across state agencies.
- Inconsistent practices and expertise across entities in identifying that an attack or incident is taking place or has taken place.
- Cyber-risk information is not consistently shared across the state as an enterprise.
- Lack of a statewide cyber response plan as part of the Illinois Emergency Response Plan
- Absence of consistent risk management practices across state agencies. Security risks are either not known or not addressed.
- Lack of standardized cybersecurity policies across the state.
- Lack of sufficient cybersecurity expertise.

Key Initiatives

- Cybersecurity awareness training for all state employees
- Campaign to involve the Governor's Cabinet in cybersecurity oversight
- Cybersecurity Strategic Plan which identifies funding and staffing needs.
- Cybersecurity Governance and Authority structure for the state of Illinois
- Strategy for the adoption of a common cybersecurity framework
- Proactive threat detection training and technology sharing and innovation
- Cybersecurity information sharing initiative (builds on STIC, MS-ISAC, FBI)
- Cyber Disruption Strategy integrated into the State Emergency Operations Plan
- Risk Management framework guidelines, policies and training for all state agencies
- Model cybersecurity policies deployment across all state agencies
- Illinois Cybersecurity Workforce Development Plan

Top Underlying Beliefs and Assumptions

- Efforts to improve cybersecurity must properly reflect the borderless, interconnected, and global nature of today's cyber environment.
- Efforts to improve cybersecurity must be based on risk management.
- Efforts to improve cybersecurity must focus on awareness.
- Cybersecurity efforts must be able to adapt rapidly to emerging threats, technologies, and business models.
- Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments.
- Efforts to improve cybersecurity must more directly focus on bad actors and their threats.
- Sufficient funding and resources will be provided to further the overall strategy.
- All agencies will participate toward the success of the cybersecurity strategy.

State of Cybersecurity in 2016

Top Characteristics of the End State

- Illinois' cybersecurity strategies and programs are continually aligned with the business strategies of Illinois agencies, boards and commissions as well as the enterprise as whole.
- Cybersecurity programs and initiatives are developed based on a sound and consistent Risk Management Process across all state agencies.
- A culture of cyber-risk awareness at all levels of state government has been created and is continually enhanced.
- Illinois utilizes a common framework for cybersecurity across all state agencies.
- Illinois has developed and maintains a proactive approach to threat and attack detection and rapidly and effectively responds to mitigate the threats and reduce the impact to the state.
- Cybersecurity planning is prevalent during all phases of the solution development
- Emerging information security threats and vulnerabilities are appropriately shared across Illinois agencies, boards and commissions in a reliable and timely manner.
- Illinois' response to a significant cyber disruption is fully defined, exercised and effective. Cyber response is governed by the Cybersecurity Response Annex in the Illinois Emergency Operations Plan.
- Effective and consistent cybersecurity policies are in place across all state agencies.
- Illinois' cybersecurity workforce is well-trained and continually developed.

Statement of Risk - The lack of a comprehensive and consistent approach to cybersecurity strategy across the state poses an immediate threat to the State of Illinois and places the confidentiality, integrity and availability of critical information in jeopardy and poses risks to privacy assurances our citizens expect and deserve.