


---

---

---


---

---

---

---

---



## Agenda

- ▣ Introduction
- ▣ Role of the CISO
- ▣ Cyber Security Overview
  - Current State
  - Targeted State and Initial Strategy
- ▣ What Are We Asking of You?
- ▣ Open Discussion

---

---

---


---

---

---

---

---



## Introduction

- ▣ 35 Years Public Service
- ▣ Police Officer
  - Patrol, Investigations, Undercover
- ▣ Intelligence
  - Criminal Intelligence Analyst, Intel Asst. Chief
- ▣ Administration and Leadership
  - Firearms Services Chief, Assistant Deputy Director
- ▣ Information Technology
  - Deputy CIO ISP (8 years)
  - CIO IEMA (5 years)
- ▣ CISO Effective August 2015

---

---

---

---

---

---

---

---



## Role of the CISO

- Provides leadership and oversight in the strategic planning, execution, and assessment of all statewide information and cyber security strategies, policies, procedures and guiding practices to be implemented by all State agencies.
- Establishes and maintains a comprehensive statewide information security program to insure that all State information assets are adequately protected against current/future internal/external threats.
- Responsible for identifying, directing, coordinating, evaluating, and reporting on information security risks while enabling the State to develop an anticipatory response to minimize information security risk.
- Coordinates the necessary alignment of internal staff, State agencies, Multi-Agency Information Sharing and Analysis Center (MS-ISAC), Federal agencies, and related third parties. The position is also responsible for project prioritization, and serving as a subject matter expert on legislative areas in matters of cyber security.

---

---

---

---

---

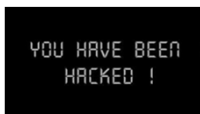
---

---

---



## Cybersecurity is a State Business Operations Issue (with significant financial risk)




---

---

---

---

---

---

---

---



## Goals

### Information Security

- Protect information from unauthorized disclosure
- Ensure information is trustworthy
- Guarantee reliable access to mission critical information



### Cyber-Resiliency

- Ability to anticipate, withstand and recover from adverse cyber-events.
- Evolve and improve in pace with the ever-changing cyber landscape.




---

---

---

---

---

---

---

---




---

---

---

---

---

---

---

---




---

---

---

---

---

---

---

---




---

---

---

---

---

---

---

---

THE WHITE HOUSE | PRESIDENT BARACK OBAMA | Contact Us | Get Email Updates

HOME | BRIEFING ROOM | ISSUES | THE ADMINISTRATION | PARTICIPATE | 1600 PENN |

HOME - BRIEFING ROOM - PRESIDENTIAL ACTIONS - EXECUTIVE ORDERS

### Briefing Room

Your Weekly Address  
Speeches & Remarks  
Press Briefings  
Statements & Releases  
White House Schedule  
Presidential Actions  
**Executive Orders**  
Presidential Memoranda  
Proclamations  
Legislation  
Nominations & Appointments  
Disclosures

**The White House**  
Office of the Press Secretary  
For Immediate Release  
February 12, 2013

## Executive Order-- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, I am hereby ordered as follows:

**Section 1 Policy.** Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

SHARE THIS: EMAIL, FACEBOOK, TWITTER

---

---

---

---

---

---

---

---

---

---

### Breaches in State Government

South Carolina Department of Revenue

- Exposed Tax Records of 70 Million People
- Costs to the state - \$70 Million

Utah - Medicaid Program


- Theft of 750,000 Medicaid Records
- Costs to the state - \$9 Million

California - Reported that there have been multiple data breaches at state agencies

- Costs to the state - \$8.8 Million

IBM 2015 Study of breaches in the U.S.

- \$6.5 million is the average total cost of a data breach
- \$217 is average cost per lost or stolen record




---

---

---

---

---

---

---

---

---

---

### Cybersecurity and Economic Growth

Private Sector Perspective


- Effective information and cybersecurity instills confidence by stockholders and potential investors and customers

What does this mean for state government?

- Another step toward making Illinois the place to live, work and play

Cybersecurity Workforce Development

- It is estimated that there will be a gap of approximately 2 million cybersecurity jobs vs qualified candidates




---

---

---

---

---

---

---

---

---

---

## So what are we doing?




---

---

---

---

---

---

---

---



### 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 CIO's Cyber Security Working Group

**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	Key Initiatives	State of Cybersecurity in 2018
<p><b>Top Characteristics of the Initial State</b></p> <ul style="list-style-type: none"> <li>Lack of measurable outcomes applicable to cyber security which display value to stakeholders.</li> <li>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 interests. Lack of clear understanding of the criticality of enterprise information security.</li> <li>Lack of a comprehensive security awareness program.</li> <li>State of Illinois security 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 monitoring practices for cyber assets across state agencies.</li> <li>Inconsistent practices and expertise across entities in identifying that an attack or incident is taking place or has taken place.</li> <li>Cyber risk information is not consistently shared across the state as an enterprise.</li> <li>Lack of a statewide cyber response plan as part of the Illinois Emergency Response Plan.</li> <li>Absence of consistent risk management practices across state agencies. Security risks are either not known or not addressed.</li> <li>Lack of standardized cybersecurity policies across the state.</li> <li>Lack of sufficient cybersecurity expertise in many agencies.</li> </ul>	<p><b>Key Initiatives</b></p> <ul style="list-style-type: none"> <li>Campaign to involve the Governor's Cabinet in cybersecurity oversight</li> <li>Cybersecurity Governance and Authority structure for the state of Illinois</li> <li>Cybersecurity training for all state employees</li> <li>Adoption of the NIST Cybersecurity Framework across all state agencies</li> <li>Proactive threat detection training and technology sharing and innovation</li> <li>Cybersecurity information sharing initiative (builds on STIC, MS-ISAC, FBI)</li> <li>Cyber Disruption Strategy integrated into the State Emergency Operations Plan</li> <li>Risk Management guidelines, policies and training for all state agencies</li> <li>Model cybersecurity policies deployment across all state agencies</li> <li>Illinois Cybersecurity Workforce Development Plan</li> </ul> <p><b>Quick Wins</b></p> <ul style="list-style-type: none"> <li>Assess state agencies with addressing critical risks and vulnerabilities, including securing personal identifying information, strengthening passwords and addressing vulnerable websites.</li> <li>Identification of the top current cyber risks for the State of Illinois.</li> <li>Security scans for all state agencies to help identify specific cyber risks</li> <li>Release of the "Top Things To Do Now" to all state agencies to enhance the cybersecurity posture of the state.</li> <li>The release of cybersecurity awareness training for state employees.</li> <li>Training for state CIOs, CSOs and other personnel in the NIST Cybersecurity Framework</li> </ul>	<p><b>Top Characteristics of the End State</b></p> <ul style="list-style-type: none"> <li>Illinois' cybersecurity strategies and programs are continually aligned with the business strategies of Illinois' agencies, boards and commissions as well as the enterprise as a whole.</li> <li>A culture of cyber risk awareness at all levels of state government has been created and is continually reinforced.</li> <li>Illinois utilizes a common framework for cybersecurity across all state agencies.</li> <li>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.</li> <li>Emerging information security threats and vulnerabilities are appropriately shared across Illinois' agencies, boards and commissions in a timely and timely manner.</li> <li>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.</li> <li>Cybersecurity programs and initiatives are developed based on a sound and consistent Risk Management Process across all state agencies.</li> <li>Effective and consistent cybersecurity policies and procedures are in place across all state agencies.</li> <li>Illinois' cybersecurity workforce is well trained and continually developed.</li> </ul>

---

---

---

---

---

---

---

---



**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce



International  
Organization for  
Standardization



Control Objectives  
for Information and  
related Technology

## A Common Cybersecurity Framework for Illinois

Functions

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

---

---

---




---

---




---

---

---

## Illinois Emergency Operations Plan Cyber-Disruption Response Strategy

---

---

---




---

---





---

---

---

## Cyber-Risk Awareness Campaign

---

---

---

---

---

---

---

---



## Governor's Proclamation



### Support of National Cyber Security Awareness Month

WHEREAS, the State of Illinois recognizes that it has a vital role in identifying, protecting, and responding to cyber threats that are a significant aspect of our daily lives and critical to our security and privacy; and

WHEREAS, critical infrastructure sectors are increasingly reliant on information systems to support financial services, energy, transportation, communications, education, health care, and emergency response systems; and

WHEREAS, the Stop Think Connect™ Campaign (www.stopthinkconnect.org) has been designated as the National Cyber Security Awareness Campaign, implemented through a coalition of private companies, nonprofits and governmental organizations, as well as a national initiative working together to increase the understanding of cyber threats and improve the nation's ability to identify and respond to them; and

WHEREAS, the National Institute of Standards and Technology Cybersecurity Framework and the U.S. Department of Homeland Security's Critical Infrastructure Cyber Security (CIS) Voluntary Program have been developed as the measures to help organizations large and small, both public and private, implement the Cybersecurity Framework and improve their cyber practices through a practical approach to addressing existing threats and challenges; and

WHEREAS, President Barack Obama signed Executive Order 13526, Promoting Private Sector Cybersecurity Information Sharing, to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government through the development of Information Sharing and Analysis Organizations; and

WHEREAS, maintaining the security of cyberspace is a shared responsibility in which each of us has a critical role to play, and awareness of computer security matters will improve the security of the State of Illinois' information infrastructure and economy; and

WHEREAS, the President of the United States of America, the U.S. Department of Homeland Security (www.dhs.gov), the State of Illinois Information Sharing and Analysis Center (ISAC) (www.isac.org), the National Association of State Cyber Security Officers (www.nascs.org), and the National Cyber Security Alliance (www.nicsa.org) have declared October as National Cyber Security Awareness Month, and all citizens are encouraged to join their efforts, along with State of Illinois Governor Bruce Rauner, in supporting the Stop Think Connect™ Campaign (www.stopthinkconnect.org) to learn about cyber security and put that knowledge into practice to keep homes, schools, workplaces, and businesses safe.

Now, therefore, I, Bruce Rauner, Governor of the State of Illinois, do hereby proclaim that the State of Illinois is officially supporting National Cyber Security Awareness Month and the National Public Awareness Campaign, Stop Think Connect.



## "Protect Yourself" Campaign on Ready Illinois



## Workforce Development Planning

### Workforce Development

#### Planning for Future Workforce Needs

The Illinois Department of Commerce and Economic Development (IDCED) is committed to ensuring that the state's workforce is prepared for the future. This report provides a comprehensive overview of the current workforce situation and offers recommendations for addressing future workforce needs.

The report is organized into four main sections: Introduction, Current Workforce Situation, Future Workforce Needs, and Recommendations. Each section provides a detailed analysis of the data and offers specific recommendations for action.

The report is intended for a wide range of stakeholders, including policymakers, business leaders, and the general public. It is hoped that the report will provide valuable insights and guidance for addressing the state's future workforce needs.

The report is a collaborative effort of the IDCED, the Illinois Department of Labor, and the Illinois Department of Education. It is hoped that the report will provide valuable insights and guidance for addressing the state's future workforce needs.



## Advanced Cyber Protection and Detection Technologies

- ❑ P.I.I. Encryption
- ❑ Expansion of monitoring capabilities and detection.
- ❑ Detection of weak passwords
- ❑ Initial implementations of Two-Factor Authentication




---

---

---

---

---

---

---



## Questions You Should Ask

- ❑ To what extent have the essential services and functions of YOUR agency been identified and programs implemented to provide for their resilience in the event of a disruption or cyber incident?
- ❑ What are the risks to critical operations and what strategies are in place to mitigate that risk?
- ❑ Is sufficient attention being given to the ability to defend against intrusions?
- ❑ What is our plan in the case of a breach or other cyber-event?

---

---

---

---

---

---

---



## Hold Me Accountable For Proving That Illinois Can;

- ✓ Anticipate Threatening Events
- ✓ Quickly Detect Intrusions
- ✓ Protect Critical and Confidential Information
- ✓ Continue Essential Activities Despite Adverse Conditions
- ✓ Restore Mission-Critical Functions Within Agreed Upon Time Periods
- ✓ Evolve and Learn so that the Impact of Potential and Actual Events is Minimized

---

---

---

---

---

---

---





### How Do We Get There?

- Identify Your Most Critical Functions and Services
- Identify the Information, Communications and Industrial Control Systems Which are Mission-Critical to Those Functions and Services
- Identify the Information Which Must Be Protected
- Determine Resiliency Requirements to Ensure Effective Public Safety Services Are Not Compromised
- Establish Controls, Plans and Practices to Meet Those Requirements

---

---

---

---

---

---

---

### What Are We Asking of You?

- ☐ Establish Cyber Security as a Standing Agenda Item for this board, reviewed on an ongoing basis.
- ☐ This body can help serve as part of the "Board of Directors" for Cyber Security Governance.

---

---

---

---

---

---

---

### What Are We Asking of You?

Agency Directors

- ☐ Insist that you are fully briefed on;
  - The current and emerging cyber security situation; and,
  - Metrics that are MEANINGFUL to helping ensure the cyber-resiliency of **your** critical Public Safety business and functions.




---

---

---

---

---

---

---



## We Need Your Help

Agency Directors and Senior Leadership

- ☐ Recognize that Cyber Security is an OPERATIONAL Issue, and that the Critical Functions and Services of your oversight are AT RISK.
- ☐ Appoint Two Individuals From Your Agency To Assist
  - Individual who has the knowledge and authority to identify your most critical business functions and services
  - Individual who can identify the systems that are mission-critical to those business functions and services
- ☐ Ask Your CIO to Brief You Regarding the Personal Information in Your Systems Which Requires Attention/Protection
- ☐ Personally participate in online cyber security awareness training
- ☐ Ensure your CIO has completed the Cyber-Security Awareness Training Survey

---

---

---

---

---

---

---

---



## Questions and Discussion

---

---

---

---

---

---

---

---