



**Board of  
Elections**

# Protecting New York's Election System

**Mike Haber**

**Chief Information Officer (CIO)**

**Ben Spear**

**Chief Information Security Officer  
(CISO)**

**NYSAC**

**October 19, 2022**



## **Mark LaVigne, PhD**

Deputy Director

**NYS Association of Counties**

# Roles & Responsibilities of the State Board

- Bipartisan agency vested with the responsibility for administration and enforcement of all laws relating to elections in New York State.
- Responsible for:
  - Overseeing county election administration compliance with state and federal election law
  - Facilitate recording and disclosure of campaign financing
- ~115 employees across 9 units. Units include Executive, Administrative, Counsel, Public Information, Enforcement, Public Campaign Finance, Compliance, Information Technology and Election Operations

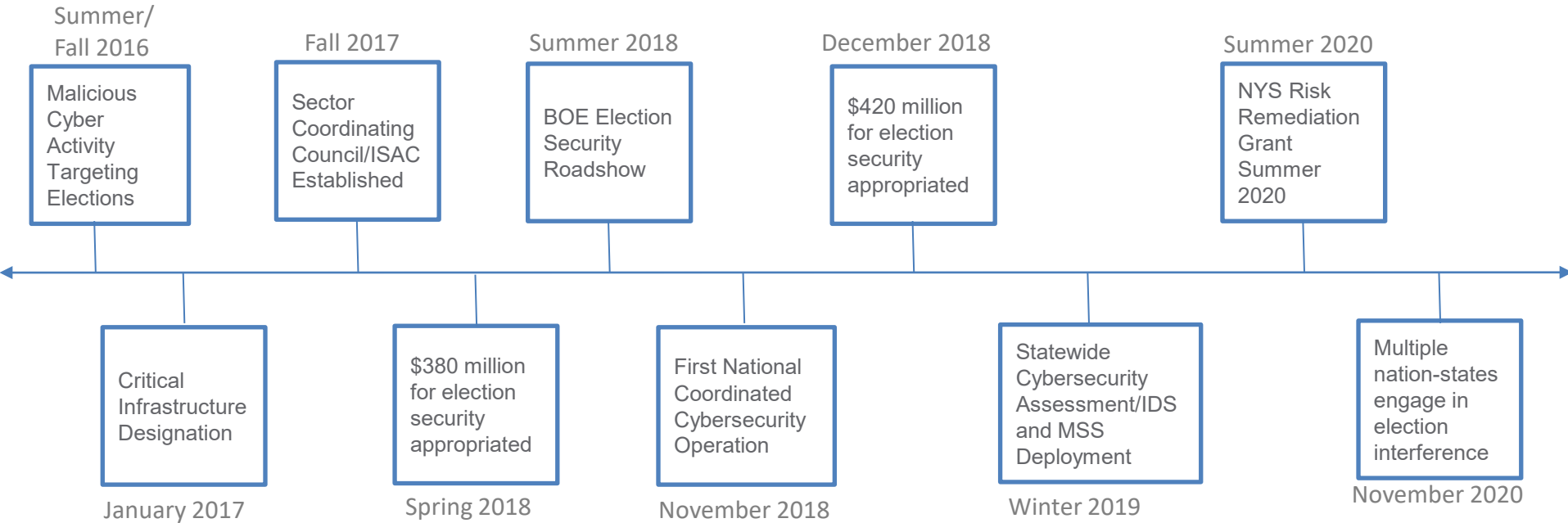
# How Does the State Board Fit In?

- County Boards are their own entities. They are not satellite offices of the State Board.
  
- We see our relationship with County Boards as collaborative.
  - *Board visits*
  
  - *Monthly Conference Calls*
  
  - *Frequent Emailed Guidance*
  
  - *Biannual Association Conferences*

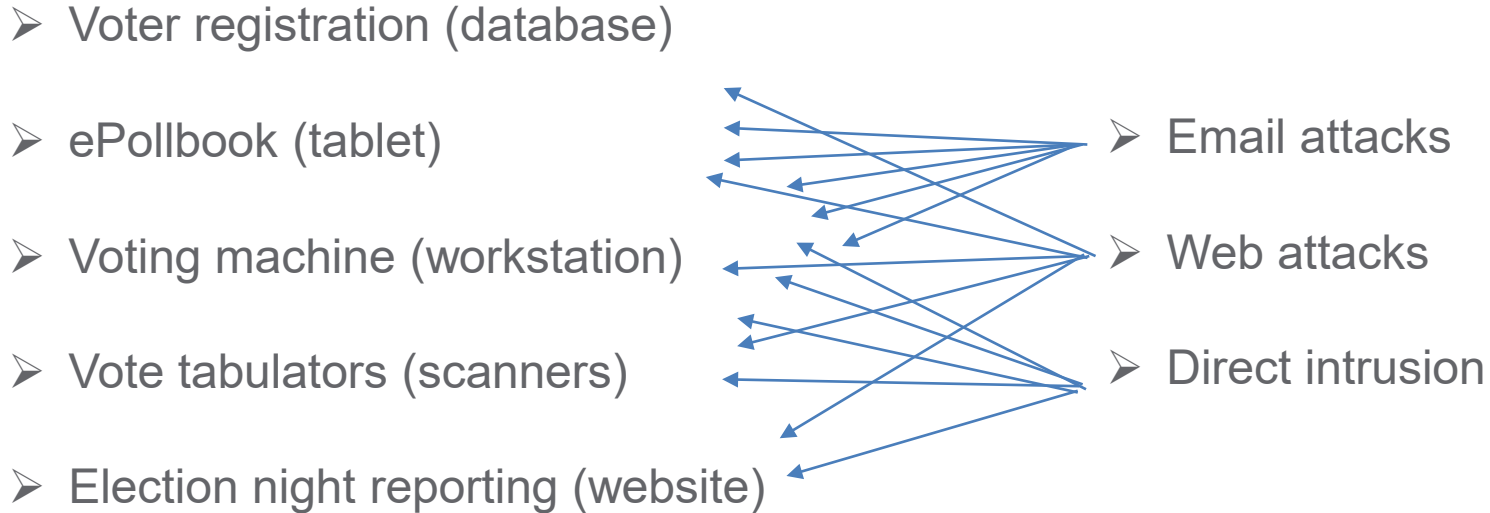
# How Does the State Board Fit In?

- We also try to foster collaborative relationship between the State Board, County Boards and their County IT Departments.
  - *NYSLGITDA Conference*
  - *EI-ISAC/MS-ISAC Membership*
  - *Grant Programs*
  - *NYSBOE-funded IDS & MSS*
  - *Annual cybersecurity training of County Board staff*

# Why are we here?



# What are we securing?



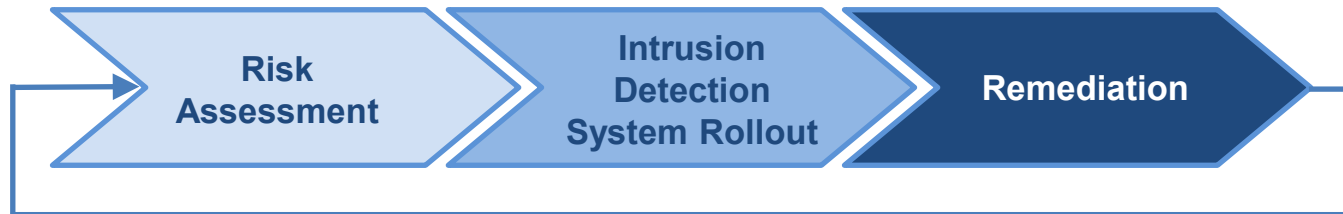
# NYSBOE's A.R.M.O.R. Plan

**A**ssess the Risk;

**R**emediate the Vulnerabilities;

**M**onitor Ongoing **O**perations;

**R**espond to Incidents.



Continuous Monitoring & Feedback



# Cyber Programs Overview

- Cyber Incident Response Procedure
- Statewide Security Assessment
- Cybersecurity Regulation
- Risk Remediation Grants
- Security Consulting Services
- Intrusion Detection and Managed Security Services
- Election Day Operations

# Partners in Success

- County Boards of Elections
- New York State Local Government Information Technology Directors Association (NYSLGITDA) and other County IT Departments
- University at Albany's Center for Technology and Government (SUNY CTG)
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- New York State Association of Counties (NYSAC)
- U.S. Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- Governor's Cybersecurity Advisory Board
- NYS Division of Homeland Security and Emergency Services (DHSES)
- NYS Department of Public Service (DPS)
- NYS Office of Information Technology Services (ITS)
- New York State Technology Enterprise Corp. (NYSTEC)
- The Belfer Center for Science and International Affairs at Harvard University

# New York State Elections Cyber Incident Reporting Procedure

## What to Report?

The State and County Board of Elections must report all cyber incidents affecting or potentially affecting elections systems to the New York State Division of Homeland Security and Emergency Services (DHSES) and to the New York State Board of Elections (NYSBOE).

Cyber incidents that require notification:

- There is a cyber incident or threat that impacts, or has the potential to impact, personally identifiable information (PII).
- There is a cyber incident or threat that impacts, or has the potential to impact, election systems, infrastructure or election administration.
- A cyber incident that receives significant media attention.

Examples include: Unusual system behavior, unauthorized access attempts, web page compromise, credential compromise, unauthorized use of systems, denial of service, unauthorized or malicious software (malware).



**First call:** NYS Division of Homeland Security and Emergency Services Cyber Incident Response Team (CIRT):  
**1 (844) OCT-CIRT** or **1 (844) 628-2478**.  
Staffed 24x7.

**Second call:** NYSBOE Secure Elections Center at:  
**1 (833) CYBERNY** or **1 (833) 292-3769**.

DHSES and the NYSBOE Secure Elections Center will coordinate State resources for election-related cyber incidents in New York State.



**If You See Something Say Something**  
Be Observant and Report Suspicious Cyber Activity



# Statewide Cybersecurity Assessment

## Governance Assessment Areas of Focus

- Information security policies and procedures review
- Data classification policy review
- Hardware and software inventories review
- Roles review (security admins / transmission of data)
- Security awareness training program review
- Disaster Recovery / Business Continuity Plans review
- Hosting provider Service Level Agreements review
- Incident Response Plan review
- Physical security controls review

## Technical Security Assessment Areas of Focus

- Generate and/or validate hardware and software inventory lists using network discovery scans
- Generate and/or validate system architecture diagram(s)
- Perform automated vulnerability scans and produce associated report(s)
- Run automated configuration security assessments and generate policy compliance report(s)
- Conduct web application security scans and produce associated report(s) [per website]

*Based on NY State Elections Law, NYSBOE Security Policy, and CIS Handbook-recommended best practices and controls*

# Cyber Security Regulation – Reporting

- Dates:
  - Annually by August 1
  
- Reporting Tool
  - Microsoft Excel spreadsheet
  - Yes/No for each requirement
    - If No, provide expected date and brief plan
  - Work with County IT to complete (NYSTEC also available)
  - Provide bipartisan contacts for Elections System Security Officers (ESSOs)
  - Provide updated Incident Response Contact List and COO

# Cyber Security Regulation – County IT Work Group

- Allegany (Keith Hooker)
  - Fulton (Perry Lovell)
  - Madison (Paul Lutwak)
  - Nassau (Christopher Baumler)
  - New York City (Steve Ferguson, John Naudus)
  - Oswego (Greg Powlin)
  - Saratoga (Eileen Bennett)
  - Steuben (Cody Ryan)
  - Suffolk (Vijay Kumar)
  - Sullivan (Lorne Green)
  - Tioga (Doug Camin)
  - Tompkins (Loren Cottrell)
  - Washington (Teri McNall and Karen Pratt)
  - Westchester (Lennox Harris)
- Additional informational sessions with full NYSLGITDA membership and other county IT leaders

# Cyber Security Regulation – The technical stuff

- Data Classification
- Asset Inventory
- Patch Management
- Vulnerability Scanning
- Backups of Election Data
- Restoration of Data
- Network Segmentation
- Remote Access
- Logging
- Incident Response
- Continuity of Operations
- Credential Management and Access
- Multi-factor Authentication
- Email and Web Protections
- Third Party Risk Management
- Continuous Monitoring and Reporting
- Removable Media
- Security Awareness Training
- EI-ISAC Membership

# Cyber Security Regulation - Tools

- Incident Response Template
- Data Classification Template
  - Identify information assets
  - Classify assets by confidentiality, integrity, and availability
  - Determine controls based on classification
  - Training planned
- Continuity of Operations Plans (COOP)
  - Template forthcoming
  - Instructions for each task
  - Grab and Go worksheets

CONFIDENTIALITY QUESTIONS			
	No	Yes	
1. Is the information publicly available?			
2. Does the information include or contain PPSI (Personal, Private, or Sensitive Information)?	No	Yes	
	None	Limited	Serious Severe
3. What impact does unauthorized disclosure of information have on health and personal safety?			
4. What is the financial or agency liability impact of unauthorized disclosure of information?			

Key Position	Successor	Delegated Authority(s)	Activation/Termination of Delegated Authority(s)	Documentation of Authority(s)

Essential Function	# of Staff	Power	Furniture Equipment	Comms	Floor Space	Telecommute?



# Risk Remediation – Fixing current issues

- Plans created for all counties
  - Based on Statewide Cybersecurity Assessments
  - Split into Short and Long-term planning
  - All counties making significant progress!
  
- Reimbursement Grant
  - Available for any line item on the Risk Remediation Plan
  - Available until December 31, 2023

# Security Consulting Services

- 32 hours available to each county (currently 40% used)
- Available through 2027
- Can be used by CBOE or CIT (or together)
- Service Options
  - Drafting policies and plans required under the cyber regulation
  - Guidance on security practices
  - Menu of Pre-Packaged Services:
    - Review of Microsoft 365 Configuration
    - Voter Registration Responsibility Chart
    - Incident Response Planning
    - Application Whitelisting Assistance

# Direct Cybersecurity Support

- Intrusion Detection and Managed Security Services
  - Network monitoring device
  - Centralization and monitoring of logs
  
- Annual Cybersecurity Awareness Training
  
- Tabletop Exercises
  
- Election Day Operations (Early Voting and Election Day)
  - Monitored by a combination of state, federal, and private sector partners
  - Cyber and physical incident response
  - Mis-, dis-, and malinformation
  - Utility tracking

# What you can do?

- Understand your role as the ultimate decision maker/responsible party
- Identify where additional county support would be beneficial
- Facilitate relationships between BOE and relevant county divisions (IT, OEM, Police, Sheriff)
- Amplify BOE public communications on election processes
- Fund IT security efforts across the county
- Conduct exercises of incident response plans

# Questions?

Contact Us  
[secure@elections.ny.gov](mailto:secure@elections.ny.gov)