# New Jersey HAVA Funds & Election Security

Tahesha Way New Jersey Secretary of State



## NJCCIC Election Security Mission

MISSION: To lead and coordinate New Jersey's cyber and physical security efforts while building resiliency to threats throughout the election offices in the State.

Tasked with coordinating election security efforts in conjunction with the New Jersey Office of the Secretary of State, the New Jersey Department of State/Division of Elections, which includes:

 The development, management, and execution of an election security program that ensures the confidentiality, integrity, and availability of the information resources, systems, and services of the State of New Jersey's twenty-one counties



## **Election Monitoring**



### **Election Monitoring**

- Operation of a centralized early voting and election day SOC (Security Operations Center) based out of the Regional Operations Intelligence Center (ROIC)
- Real-time incident response meeting room (Virtual)
  - Accessible to all counties and partners
  - TLP:GREEN Updates provided on a timed basis
- Monitoring of all networked devices used in polling sites within all 21 counties.
- Incident response to all activity, primary and secondary
- Coordination with FBI daily activities.



## **Election Cybersecurity**



## Selection Cybersecurity

#### **Cybersecurity Approach to Elections**

- Cybersecurity training and awareness for election officials and staff
- Security on statewide voter registration systems (SVRS)
  - Assessment of the system as well as all changes
  - Review and implementation of security policy
  - Review of access logs
- Focus on the potential cyber threat to election equipment
- Set policies and monitor statewide polling site routers in coordination with the security of electronic poll books
- Coordination with county IT election related specifics



## **Election Physical Security**



### **Election Physical Security**

#### Physical awareness of election infrastructure

- In coordination with our partners at NJOHSP Infrastructure Security and CISA, physical security assessments are completed for all election offices
- Detailed reports and recommendations are provided back to the county election offices
- Some recommendations include:
  - Surveillance of specific areas
  - Door access (keys, cards or badges, RFID, access logs)
  - Physical security of entrances



## **Election Preparedness**



## **Election Office Preparedness**

#### **Preparing for the Unexpected**

- Continuity of Operations Plans (COOP)
  - Assist in developing county and municipal COOPs
  - Utilizing a workshop-type format, training is used to prepare counties and municipalities throughout New Jersey for emergencies by developing and practicing response strategies to ensure public safety and continuity of services
- Early-Voting Security Plans
  - Collaboration with counties to detail each of their early voting locations, including facility assessments and network analysis from our data provider
  - De-escalation training for counties



## **Election Security Partnerships**



## Election Security Partnerships

#### **New Jersey Election Security Strategic Partnerships**

- MS/EI-ISAC
- New Jersey State Police
- New Jersey Attorney Generals Office
- FBI
- CISA (Cybersecurity Infrastructure Security Agency)
- Local/County Emergency Management Coordinator
- Local/County Law Enforcement
- USPS/USPIS (US Postal Inspection Service)



## Election Day Emergency Response Guide



### ELECTION DAY EMERGENCY RESPONSE GUIDE



Developed by the New Jersey Secretary of State Security's Election Security Initiative (August, 2019)

#### IMPORTANT CONTACT INFORMATION

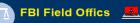
#### **STATE CONTACTS**



New Jersey Offic of Home I and Security and Preparedness (OHSP) 1-866-4-SAFE-NJ or tips@njohsp.gov







- Newark (973) 792-3000
- Philadelphia (215) 418-4000



**National Cybersecurity and Communications** Integration Center (NCCIC) (888) 282-0870

### WHENINDOUBT, CALL THE DIVISION OF ELECTIONS (DOE)



#### Cybersecurity Incident RED FLAGS

- Unsolicited request from a voting machine vendor providing a flah drive with instructions to install a critical software update
- Email containing long hyperlinks and/ or attachments with no additional information
- Email message from an unrecognized sender trying to persuade you to click on a link or open an attachment
- Unexplained or unauthorized activities occur on election system software
- Software operates slower than usual or frequently freezes or crashes



#### Severe Weather RESPONSE STEPS

- 1. Secure ballots and voting equipment.
- 2. Stay updated on natural hazards by following the New Jersey Offic of Emergency Management on social media.
- 3. Hurricane stay indoors and keep away from windows or other breakable objects.
- 4 Blizzard remain indoors and seal cracks in doors or windows.
- Call 9-1-1 if a life-threatening emergency occurs.
- Stay in contact with DOE.



- 1. When, or if it is safe to do so:
  - · Evacuate the building.
  - Call 9-1-1.
  - Secure ballots and voting equipment.
  - Notify DOE.
- 2. For bomb threat or suspicious object:
  - Keep everyone away from the object.
  - Call 9-1-1.
- Notify OHSP and DOE.
- For active shooter: ensure staff s trained - RUN, HIDE, FIGHT.

Report any suspicious activity to local law enforcement and to OHSP.







- Proceed to evacuation route.
- 2. Proceed to designated assembly location.
- 3. Call 9-1-1.
- Take a head count. Take note of. and report any missing people to emergency response personnel.
- 5. If safe, secure ballots and voting equipment.
- 6. Notify DOE.



### Cybersecurity Incident

- Report incident to local law enforcementethe NJCCIC, DOE, FBh Field Offic, and the NCCI C
- 2. Take compromised device(s) offliedisconnect from the interhet and from Wi-Fi. Do not power off evi ce(s).
- 3. Remember any information entered into a fraudulent website.
- 4. Change passwords by logging in from a diffeent, non-compromised device.
- Record unauthorized/unusual activity.















