#BeReady16: Working with election officials to secure the process
U.S. Election Assistance Commission

- Created after 2000 election by Help America Vote Act (HAVA)
- Four main missions:
  • Distribute Money
  • Collect Election Data
  • Best Practices on Election Administration
  • Testing & Certification of Voting Systems
Managing Election Technology

Checklist for Securing Voter Registration Data

The Help America Vote Act (HAVA) requires that each State, acting through the chief State election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State...

State requirements for registration differ greatly, but every State maintains personally identifiable information associated with the voter’s name to determine eligibility and precinct information. Due to the sensitive nature of this personal information, there is a natural concern on what security protocol has been used to secure the data.

This list is intended to provide election officials information on best practices to protect their voter registration data. State and local election officials have already implemented many of these items. Election officials may use it to provide assurance to members of the public who may question the security measures that have been implemented in their State.

- **Access Control** – only authorized personnel should have access to the voter registration database. Each person with authorization to the database should only have access to the data and information necessary for them to perform their job duties.
- **Auditability** – the database should have sufficient logging capabilities, including who has made modifications, the nature of the modifications, the authority to make those modifications, and to determine if there has been any unauthorized or inappropriate activity.
- **Detection** – use an intrusion detection system and monitor the incoming and outgoing traffic for signs of irregularities, such as multiple log-in attempts, above average traffic, large amounts of data being transmitted, etc. If detected have a response and mitigation plan in place.
- **Data Backups** – the database should be backed up routinely. If any unexpected modifications to the data were to occur, the database could be restored to the last known state prior to the unexpected modifications. The ability to perform backups and restores should be tested and validated.

Voter registration data includes names, dates of birth, physical and email addresses and phone numbers, as well as political affiliation in some states. | Getty

Researcher: Voter registration data of 191 million exposed online

By DAVID PERERA | 12/28/15 02:49 PM EST | Updated 12/28/15 04:59 PM EST
Contingency Plans

In preparation for the 2016 elections, EAC is collecting and sharing continuity of operations plans (COOPs) and resources from election officials at the state and local levels. Submit COOP plans to BeReady16@eac.gov and sign up to be a contingency planning expert in the Election Official Exchange.

EAC Resources

U.S. Election Assistance Commission
01/2016 – Roundtable - Preparing for Election 2016 in Battleground Jurisdictions
(view the webcast discussion that includes best practices for emergency-related risk mitigation)
01/2016 – Contingency Planning 2016 (Video)
10/2015 – Commissioner Masterson on Contingency Planning for "No Time Out" (Blog)
10/2014 – 6 Tips for Contingency and Disaster Planning (Tips)
05/2010 – Contingency Planning (Video)
04/2010 – Contingency Planning and Change Management (EMG Chapter 11)
10/2007 – Contingency and Disaster Planning (Quick Start)

NASS Resources

National Association of Secretaries of State
NASS Election Contingency Planning Resources

California

Contra Costa County (Election Division)
10/2009 – Flu Season and Emergency Contingency Plans

Colorado

Colorado Office of the Secretary of State
09/2015 – 2015 Disaster Mitigation Planning Outline
09/2015 – 2015 Election Disaster Mitigation Planning
What to know about voting systems

- This conversation about security of voting systems is not a new one to election officials
- Voting systems selected at state and/or local level
- Voting systems tested at federal, state and local level
- Voting systems certified by EAC are not connected to the internet
- Many layers and aspects to securing the voting systems
- The voting system is just one system of a larger election ecosystem
- Election technology should be viewed as infrastructure for your state
What questions to ask?

- What are largest risks to process? What steps have you taken to address these?
- What security procedures are in place? When were they updated?
- What steps do you take to mitigate new or emerging risks?
- What resources/people are you using to address risks? What do you wish were available to you?
- What opportunities do voters have to engage in the process and improve their confidence?
What to tell voters

If you have concerns or questions talk to your state and local election officials.

Get involved... Be a poll worker!

Take advantage of other opportunities to be involved (pre-election testing, public displays of the voting systems, public count, post-election audits)
Questions?

More information:
EAC.gov
BeReady16@eac.gov
1-866-747-1471
mmasterson@eac.gov
cmccormick@eac.gov
@mastersonmv

Connect with us:
U.S. Election Assistance Commission  @EACgov  Facebook.com/EACgov1