U. S. ELECTION ASSISTANCE COMMISSION
Voting System Testing and Certification Program
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

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.

- □ **Data Suppression** – any data provided to outside sources is suppressed to only contain the data necessary for that entity to perform its legally authorized functions. For example, if an entity wants to obtain a copy of the data files to determine where specific voters live for GOTV campaigns, it does not need data field containing ID numbers and therefore, the additional information should not be provided.
- □ **Encryption** – encryption should be used throughout, including but not limited to encrypting the database, server, backups, any files used for distribution, all data transmission and communication.
- □ **Firewalls** – implementation of the proper use of network firewalls for the environment in use. Unauthorized access (or attempts to access) to the data should be detected, prevented, reported and escalated.
- □ **Remote Access Control** – only allow remote access through secure networks, such as Virtual Private Networks (VPN).
- □ **System Interconnection** – do not connect the voter registration database to any other information system that is not required for its use. When the voter registration system is required to be interconnected with another information system make sure the necessary security controls are in place for each system individually, as well as the communication channel between the systems.
- □ **Documentation** – when data is obtained from an authorized entity, make sure to maintain documentation on who was provided the information, for what purpose, and what information was contained within the data set. If data is inappropriately distributed, it will be easier to determine the source distribution.

Conclusion: The security of voter registration data along with providing the assurance to the public that the data has been protected is of the upmost importance to every election official. Any database containing personal information should be protected with strategic layers of physical and technological security. Election officials may use this list as a baseline to assess the current security protocol surrounding the voter registration database as well as a reference to guide the public on what has already been implemented to protect their voter registration data and the integrity of their vote.

Resources: For additional technical resources, reference the following documents.

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- NIST Special Publication 800-30
- NIST Special Publication 800-39
- International Organization for Standardization (ISO) 31000:2009
- ISO/IEC 27005:2011