NASS
National Association of Secretaries of State

October 2020

Frequently Asked Questions (FAQ): Public Voter Registration Information and Security of State Voter Registration Databases

1. **Who can access voter registration data?**
   The majority of states make some voter data available to political parties, campaigns and other third parties, like researchers, for non-commercial use. A portion of voter registration information, for example name and address, is designated as public information under state laws. States have dealt with disclosure and conditions for use in a variety of ways, balancing transparency requirements with privacy protections for Personally Identifiable Information (PII) such as social security numbers, drivers' license numbers and state ID numbers. Please note, access or attempted access to information exempt from public disclosure is subject to criminal prosecution or civil liability. For another resource, the National Conference of State Legislatures also has information on Access to and Use of Voter Registration Lists.

2. **What data is kept in a voter registration list?**
   The information collected on a voter application form varies by state, with state law determining what qualifies as personal information. All states, however, collect name, address and certain PII such as full or partial social security numbers, drivers' license numbers and state ID numbers. Some states also collect political party affiliation, phone number, email address, voting history (if a person voted, not how they voted) and voting method (absentee, in-person, etc.).

3. **How can voter registration data be obtained from the state?**
   In most states, voter registration data is made available for purchase from the Secretary of State or local election offices. The cost of purchasing the data varies across states, often depending on the amount and type of data requested—like county, congressional district, etc.

   To be clear, no state shares a voter's social security number, drivers' license number or state ID number.

4. **What are states doing to protect voter registration information?**

   Election officials are working diligently to further secure state voter registration databases by implementing security measures, such as multi-factor authentication and data backup processes. It is important to note, election officials cannot control the dissemination or protection of voter registration information that has been provided to third parties. However as noted in the answer to Question #3, no state includes voter PII in lists sold or provided to third parties.

5. **Has voter registration data been manipulated by bad actors?**

   There have been no documented instances of actual voter registration data manipulation by bad actors.

6. **Can bad actors change election results by breaching voter registration systems?**
   No. Voter registration systems are segmented from vote casting and vote tabulation systems. While voter registration systems are important to election processes, a breach of a voter registration system would not result in access to vote tallies or affect official election results. Additionally, election officials are working daily to protect voter registration systems from attempted breaches and to build resilience into election processes. Voter registration lists are backed-up, often daily and are closely monitored by election officials in the run-up to an election in order to detect anomalies.

   It is true technical problems with voter registration systems, could result in longer lines at polling places or cause some voters to cast a provisional ballot, but voter registration systems are resilient. There are also methods for verifying your registration status post-election, so provisional ballots can be properly processed and counted.

7. **What are states doing to protect the November 3, 2020 election from cyber threats?**
   In 2018 and 2019, Congress provided a total of $780 million to the states to help enhance the security of election infrastructure. Utilizing these funds and existing partnerships with federal agencies, states are working to protect election systems through a multi-layered approach that includes cybersecurity assessments, penetration testing, intrusion detection sensors, and implementation of recommended cybersecurity practices such as multi-factor authentication. States have also increased cybersecurity training, built robust cybersecurity teams within their offices, and utilized information sharing protocols designed to improve communication between election officials and the federal government.

8. **What should voters do if they are concerned about their voter registration information?**
   Your trusted sources for any election-related information such as registering to vote, requesting an absentee ballot, voting are your state and local election officials. To learn more about your state's specific tools, deadlines and requirements for registering and ultimately voting or to verify your voter registration information, visit canivote.org—a helpful nonpartisan website created by state election officials to provide eligible Americans with accurate election information. This site takes you directly to your Chief State Election Official's website. In addition, contact your state and local election officials immediately if you believe you are a victim of a scam related to your voter registration information or if you receive false information about the upcoming elections.

###