Frequently Asked Questions
Regarding Data Exposure of Online Voter Registration System

1. What was the problem that allowed unauthorized access to the Division's data?

   The Division contracted with an outside vendor to build its online voter registration system as part of the implementation of the new VREMS which was deployed in late 2015. It was recently discovered that an outside actor exploited a flaw to access voter information. This did not allow those who accessed the system to manipulate the data in the system—the incident resulted in the disclosure of select personal information. As explained below, that information included things like a voter's name and address, but it did *not* allow the outside actor to identify who an individual voted for or how they voted. The flaw was immediately remedied when it was discovered.

2. What online systems were accessed?

   The Division's online voter registration system.

3. What data was available for unauthorized access?

   By exploiting the flaw in the online voter registration system, someone could gain access to records that contained a voter's:
   - Name
   - Date of birth
   - Last 4 digits of Social Security Number
   - Driver's license/State-issued identification number
   - Residence and mailing addresses
   - Registered political affiliation
   - Email address

   Under AS 15.07.195, the date of birth, last four digits of the social security number, and driver's license/state-issued identification number are confidential. The Alaska Personal Information Protection Act additionally protects the driver's license/state-issued identification number in connection with a person's name.

   The affected system contains only voter information relevant to registration. It does not contain any Division information regarding other topics like vote tallies, voter history, polling places, voting software or machines, etc.

4. Who actually accessed this data?

   The State's preliminary investigation has shown that an outside actor exploited the flaw to access some voter data. The State's investigation is still ongoing.

5. When did they access it?

   Between September 19 and October 17.

6. What did they do when they accessed it?

   The State's preliminary investigation showed that the outside actors copied the voter information that they accessed. There is no evidence that the actors changed, deleted or added to the information in any way—indeed, the flaw they exploited did not allow them to manipulate the data in the system. The evidence thus far indicates the actors used the information for voter intimidation and propaganda, which was likely their primary goal. The State's investigation is still ongoing.

7. When and how did the State find out?

   The unauthorized access was confirmed by the Division on October 26 and the Lt. Governor was briefed on October 27.

8. What has the Division been doing since then?

   First, the Division worked with the vendor to quickly remedy the flaw. Next, the Division commissioned an immediate investigation by an outside computer forensics contractor with expertise in online security. The contractor's preliminary report identified the source of the problem, the extent and severity of the unauthorized access, and initial recommendations for preventing such problems in the future and investigating the incident further. The Division also worked with its outside vendor, to identify all individuals whose data was accessed so that they can be notified and take action to prevent any misuse of their personal information.

   The incident involved access; it did not involve manipulation of the voter registration information. There is also no evidence that the outside actor intended to do anything other than intimidate and sow distrust through propaganda. The State continues to investigate the incident. Because of the sensitivity of this information and the need to protect the security of the elections systems, the Division cannot provide more details at this time.

9. How can I trust that the election results are accurate and secure?

   There is no connection between the online voter registration system and the voting and vote-counting processes. Alaska's elections system and processes has received high marks for security, and those same safeguards give the Division confidence in the election results. Those safeguards include, the use of a centralized voting system, having paper back-ups for all votes, independent verification and cross-checking of paper ballots and preliminary electronic results, audit of machine-counts of votes by hand-counts in a random sample of precincts, and observers invited to watch both voting and vote-counting procedures.

10. What is the state doing to assist any voters who may have been affected by this?

    In partnership with the vendor, 1 year of credit and ID monitoring services are being offered.

    Voters may call 1-833-269-0003 to find out if they were affected. This line will be open from 8:00am to 5:00pm Monday through Friday until further notice.