Summary of the State's Preliminary Investigation

The Division of Elections, with the assistance of the State Security Office, and an outside computer forensics contractor, conducted an audit of Internet traffic logs relating to the division's public-facing election servers.

The preliminary investigation was specifically focused on several attempts to obtain unauthorized access, with varying levels of sophistication, to the high-profile Online Voter Registration (OLVR) servers.

The outside actors exploited a flaw that allowed them to exfiltrate voter information. The automated nature of the attack allowed the outside actors to gain access to significant amount of personally identifiable information (PII) quickly. The information exposed was the registered voter's name, date of birth, driver's license, or state identification number, last four digits of the social security number, residence and mailing addresses, and party affiliation.

The outside actors tried to attack the system in other ways, but security controls worked and rebuffed them. The outside actors attempted several aggressive attacks from controlled assets within and outside of the United States. These attacks were ultimately unsuccessful, largely because the attacks were not sophisticated, and they did not successfully mask their intent.

The division analyzed how the outside actors gained access, and then checked the impacted host servers for signs of infection. There were none. An extensive investigation was also performed on the impacted servers, including a review of event logs and an audit of system memory, for indicators that data had been altered or deleted. There were no signs of this, either.

The State's preliminary investigation thus confirmed the initial findings – that Alaskan voter records were extracted from a publicly exposed web page by an unauthorized party using publicly available tools, but no data was altered. It was also assessed as unlikely that the attackers achieved any foothold on the systems that were analyzed.