Rep. Berry, Hills. 44
February 3, 2025
2025-0217h
11/02

Amendment to HB 626

Amend the bill by replacing section 1 with the following:

1 Secretary of State; Chief Election Officer; Duty to Investigate System Vulnerabilities. Amend RSA 652:23 to read as follows:

652:23 Chief Election Officer.

I. The secretary of state shall be the chief election officer for the state. The secretary of state shall provide information regarding voter registration procedures and absentee ballot procedures for all voters, including absent uniformed services voters, absent voters temporarily residing outside the United States, and federal ballot only voters domiciled outside the United States. Instructional and informational materials published by the secretary of state for clerks to provide such voters shall include information on how to communicate electronically with election officials.

II. Within 180 days of the effective date of this paragraph, the secretary of state shall implement and operate a public vulnerability disclosure program which substantially meets or exceeds the recommendations contained within the publication "Guide to Vulnerability Reporting for America's Election Administrators" published by the Cybersecurity and Infrastructure Security Agency of the United States Department of Homeland Security, to make it easier for security researchers and the general public to report security vulnerabilities appropriately. The scope of the program shall include at least all of the secretary's information technology systems which bear on the integrity of the voter registration and election processes, including the centralized voter registration database and the user interfaces used by voters, town clerks, ballot clerks, and supervisors of the checklist relative to elections and voter registration. The secretary shall work with the cybersecurity advisory committee established in RSA 21-R:16, and such committee shall be responsible for the oversight of the public vulnerability disclosure program.

III. Upon identification of a security vulnerability, the secretary of state shall have a reasonable period to implement corrective measures before the vulnerability is publicly disclosed. The secretary shall coordinate with the cybersecurity advisory committee, established in RSA 21-R:16, to assess the nature and severity of the vulnerability and determine an appropriate remediation timeline. Until the vulnerability is adequately mitigated, disclosure shall be limited to those individuals or entities necessary to facilitate remediation and prevent exploitation. If the vulnerability remains unresolved beyond the

agreed remediation period, the cybersecurity advisory committee shall determine whether disclosure is necessary in the interest of election security.