721—29.4(47) Election security by the commissioners.

29.4(1) At the start of each calendar year, the commissioner shall provide to the state commissioner the following information:

a. The full personnel roster, phone numbers, and email addresses of the commissioner's office that identify who from the office will participate in election administration in any form throughout the year. This does not include precinct election workers.

(1) The roster will identify the personnel that the commissioner considers critical to the successful execution of elections.

(2) The roster will further identify a technical point-of-contact (POC) for the state commissioner. If the commissioner wishes to serve as the POC, the commissioner will also designate an additional POC. The POC needs to be a government employee but does not necessarily need to be a person within the commissioner's office.

b. A list of other county employees who may be involved in the event of an incident in the county.

29.4(2) Every commissioner shall be a member of the Elections Infrastructure Information Sharing and Analysis Center. The state commissioner shall provide information on how to become a member upon request by a commissioner.

29.4(3) In every odd-numbered year, every commissioner shall request the following services from CISA. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than CISA for substantively similar services. A failure of CISA to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

a. Cyber resilience review.

b. Risk and vulnerability assessment.

c. External dependencies management assessment.

d. Remote penetration testing.

e. Protective security assessment.

29.4(4) Every commissioner shall utilize the following services from OCIO. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than OCIO for substantively similar services. A failure of OCIO to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

a. Intrusion detection system.

b. Endpoint malware detection.

c. Cybersecurity training, including phishing assessments.

d. Vulnerability management.

29.4(5) Every commissioner shall request a weekly vulnerability scanning by CISA.

29.4(6) A commissioner shall remediate all critical or high-risk vulnerabilities identified by any assessment.

29.4(7) The state commissioner may require every commissioner and commissioner's staff to participate in phishing assessments.

29.4(8) Commissioners may choose to participate in any other assessments or testing from vendors approved by the state commissioner. Commissioners shall notify the state commissioner when any assessments are scheduled.

29.4(9) The state commissioner may require a commissioner and commissioner's staff to participate in any assessment or training that the state commissioner arranges.

29.4(10) A commissioner shall use only county-issued email for the conduct of elections. This applies to all full-time and part-time staff of the commissioner as well as the commissioner. No other email addresses are permitted for full-time and part-time employees of the county who assist in any part of the administration or security of elections for the conduct of elections. However, this does not apply to precinct election officials who are not normally employed by the county on a regular basis in another capacity. This prohibition includes forwarding election business emails to a personal email address. This does not include

out-of-band emails created and authorized as a part of a continuity of government plan or an incident response plan.

29.4(11) Any county information technology infrastructure that is used to access or conduct any part of elections in the state is subject to the following requirements:

a. Passwords to access the county network must be compliant with the standards enumerated by either the National Institute of Standards and Technology, the OCIO, or guidance issued by the state commissioner.

b. Session-lock timeout standards must be compliant with the standards enumerated by either the National Institute of Standards and Technology or guidance issued by the state commissioner.

c. A current inventory of IT assets assigned to the commissioner's office shall be kept.

d. Daily, weekly and monthly data backups within the commissioner's office will be maintained and physically or logically separated from production data.

29.4(12) The website of a commissioner shall have a top-level domain of ".gov" and shall utilize secure socket layer or transport layer security certificates for all publicly facing websites. A commissioner's agreement with OCIO to use a subdomain of ".iowa.gov" is sufficient to satisfy this requirement. A commissioner's site that redirects traffic from a different top-level domain to a ".gov" domain is sufficient to satisfy this requirement.

29.4(13) If the state commissioner is satisfied that a county has an adequate alternative to any requirement in this rule, the state commissioner may waive that requirement. It is the sole discretion of the state commissioner whether a county qualifies for a waiver.

29.4(14) Except where otherwise exempted, failure by a commissioner to follow these rules constitutes a technical violation pursuant to Iowa Code section 39A.6.

[**ARC 5036C**, IAB 5/6/20, effective 6/10/20]