ARC 3914C

SECRETARY OF STATE[721]

Notice of Intended Action

Proposing rule making related to elections technology security and providing an opportunity for public comment

The Secretary of State hereby proposes to adopt new Chapter 29, "Elections Technology Security," Iowa Administrative Code.

Legal Authority for Rule Making

This rule making is proposed under the authority provided in Iowa Code section 47.7.

State or Federal Law Implemented

This rule making implements, in whole or in part, Iowa Code section 47.7.

Purpose and Summary

Proposed Chapter 29 requires that all Secretary of State and County Auditor staff who access Iowa's statewide voter registration database (I-Voters) take an approved training course related to cybersecurity practices.

This new chapter is necessary because of heightened awareness of cybersecurity issues and the need for those with lawful access to I-Voters to be alert to common cybersecurity threats and mitigation techniques. The Secretary of State, as the State Registrar of Voters, has determined this training is necessary for a variety of reasons, including the federal Department of Homeland Security's designation of elections as "critical infrastructure."

Fiscal Impact

This rule making has no fiscal impact to the State of Iowa.

Jobs Impact

After analysis and review of this rule making, no impact on jobs has been found.

Waivers

Any person who believes that the application of the discretionary provisions of this rule making would result in hardship or injustice to that person may petition the Secretary of State for a waiver of the discretionary provisions, if any, pursuant to 721—Chapter 10.

Public Comment

Any interested person may submit written comments concerning this proposed rule making. Written comments in response to this rule making must be received by the Secretary of State no later than 4:30 p.m. on August 21, 2018. Comments should be directed to:

Eric Gookin
Office of the Secretary of State
Lucas State Office Building
321 East 12th Street
Des Moines, Iowa 50319
Email: eric.gookin@sos.iowa.gov

Public Hearing

No public hearing is scheduled at this time. As provided in Iowa Code section 17A.4(1)"b," an oral presentation regarding this rule making may be demanded by 25 interested persons, a governmental subdivision, the Administrative Rules Review Committee, an agency, or an association having 25 or more members.

Review by Administrative Rules Review Committee

The Administrative Rules Review Committee, a bipartisan legislative committee which oversees rule making by executive branch agencies, may, on its own motion or on written request by any individual or group, review this rule making at its regular monthly meeting or at a special meeting. The Committee's meetings are open to the public, and interested persons may be heard as provided in Iowa Code section 17A.8(6).

The following rule-making action is proposed:

Adopt the following **new** 721—Chapter 29:

CHAPTER 29
ELECTIONS TECHNOLOGY SECURITY

721—29.1(47) Definitions. The following definitions are adopted.

"Breach" means a compromise of security processes that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected information.

"Commissioner" means the county commissioner of elections as defined in Iowa Code chapter 47.

"Cybersecurity" means the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

"Elections technology" means the statewide voter registration database, voting system, electronic poll books, and other technologies used to register, maintain, or process voters or conduct any election. For purposes of this rule, these terms shall have the definitions as described in the administrative rules of the secretary of state.

"Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

"Incident" means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

"I-Voters" means the statewide voter registration database.

"Office of the chief information officer" or *"OCIO"* means the state chief information officer.

"Registrar" means the county commissioner of registration as defined in Iowa Code section 48A.3.

"State commissioner" means the state commissioner of elections as described in Iowa Code chapter 47.

"State registrar" means the state registrar of voters as defined in Iowa Code chapter 48A.

"User" means anyone from the state registrar or county registrar or approved third-party vendor who accesses I-Voters.

721—29.2(47) Cybersecurity training.

29.2(1) All users who access the I-Voters database must complete annual training programs on principles of cybersecurity. Upon completion of the training, a user shall transmit proof of completion to the state registrar. The state registrar shall maintain a list of approved training programs on the secretary of state's website. The state registrar shall consult with the OCIO or the federal Election Assistance Commission before adding trainings to the list of approved programs. If requested by the office of the chief information officer, the federal Election Assistance Commission, or a county registrar, the state registrar may review and add recommended cybersecurity training programs to the approved list.

29.2(2) The state registrar may disable any user account if the user does not complete the training within 30 days of access granted, or on the anniversary date set by the state registrar.

29.2(3) The state registrar may temporarily waive this requirement for any user if the state registrar believes it is necessary to the execution of the election.

721—29.3(47) Cybersecurity incident or breach.

29.3(1) A commissioner who identifies or suspects an actual or possible cybersecurity incident or breach shall immediately report the incident to the state commissioner. Upon receiving the report, the state commissioner shall alert the appropriate state or federal law enforcement agencies, the federal Department of Homeland Security, the OCIO, and the vendor responsible for maintaining the affected technology. The state commissioner may disseminate the information to other agencies as the state commissioner deems necessary.

29.3(2) Information reported to the state commissioner under this rule shall be exempt from public records requests pursuant to Iowa Code section 22.7(50).

29.3(3) Nothing in this rule prohibits a commissioner from alerting local law enforcement prior to contacting the state commissioner in the event of an incident or breach.

These rules are intended to implement Iowa Code section 47.7(2).