SENATE FINANCE COMMITTEE SUBSTITUTE FOR
SENATE HEALTH AND PUBLIC AFFAIRS COMMITTEE SUBSTITUTE FOR
SENATE BILL 129

56TH LEGISLATURE - STATE OF NEW MEXICO - SECOND SESSION, 2024

AN ACT

RELATING TO CYBERSECURITY; AMENDING THE CYBERSECURITY ACT; ADDING A DEFINITION FOR "PUBLIC BODY"; PROVIDING FOR RULEMAKING; ESTABLISHING REPORTING REQUIREMENTS FOR PUBLIC ENTITIES RECEIVING STATE APPROPRIATIONS IN CERTAIN SITUATIONS; REQUIRING CERTIFICATION OF COMPLIANCE WITH CERTAIN INFORMATION SECURITY STANDARDS; CHANGING THE MEMBERSHIP OF THE CYBERSECURITY ADVISORY COMMITTEE.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

SECTION 1. Section 9-27A-1 NMSA 1978 (being Laws 2023, Chapter 115, Section 1) is amended to read:

"9-27A-1. SHORT TITLE.--[~~This act~~] Chapter 9, Article 27A NMSA 1978 may be cited as the "Cybersecurity Act"."

SECTION 2. Section 9-27A-2 NMSA 1978 (being Laws 2023, Chapter 115, Section 2) is amended to read:

"9-27A-2. DEFINITIONS.--As used in the Cybersecurity Act:

A. "agency" means executive cabinet agencies and their administratively attached agencies, offices, boards and commissions;

B. "cybersecurity" means acts, practices or systems that eliminate or reduce the risk of loss of critical assets, loss of sensitive information or reputational harm as a result of a cyber attack or breach within an organization's network;

C. "information security" means acts, practices or systems that eliminate or reduce the risk that legally protected information or information that could be used to facilitate criminal activity is accessed or compromised through physical or electronic means;

D. "information technology" means computer hardware, storage media, networking equipment, physical devices, infrastructure, processes and code, firmware, software and ancillary products and services, including:

(1) systems design and analysis;

(2) development or modification of hardware or solutions used to create, process, store, secure or exchange electronic data;

(3) information storage and retrieval systems;

(4) voice, radio, video and data communications systems;

(5) network, hosting and cloud-based systems;

underscored material = new
[~~bracketed material~~] = delete

(6) simulation and testing;

(7) interactions between a user and an information system; and

(8) user and system credentials; [~~and~~]

E. "public body" means a branch, agency, department, institution, board, bureau, commission, district or committee of the state or a county, municipality, public school or institution of higher education; and

[~~E.~~] F. "security officer" means the state chief information security officer."

SECTION 3. Section 9-27A-3 NMSA 1978 (being Laws 2023, Chapter 115, Section 3) is amended to read:

"9-27A-3. CYBERSECURITY OFFICE CREATED--SECURITY OFFICER--DUTIES AND POWERS.--

A. The "cybersecurity office" is created and is administratively attached to the department of information technology. The office shall be managed by the security officer.

B. Except as required by federal law, the cybersecurity office shall oversee, in a fiscally responsible manner, cybersecurity- and information security-related functions for agencies and may:

(1) adopt and implement rules establishing minimum security standards and policies to protect [~~agency~~] state information technology systems and infrastructure and

provide appropriate governance and application of the standards and policies across state information technology resources [~~used by agencies~~] to promote the availability, security and integrity of the information processed, transacted or stored by agencies in the state's information technology infrastructure and systems. The rules shall include a requirement that a public body that receives general fund appropriations for information technology resources shall report to the cybersecurity office all cybersecurity and information technology security expenditures in a form and manner established by the cybersecurity office;

(2) [~~develop~~] adopt and implement rules establishing minimum cybersecurity controls for managing and protecting information technology assets and infrastructure for all entities that are connected to an agency-operated or -owned telecommunications network;

(3) consistent with information security standards, monitor agency information technology networks and conduct information technology and security assessments to detect security vulnerability incidents and support mitigation efforts as necessary and within capabilities;

(4) as reasonably necessary to perform its monitoring and detection duties, obtain agency system [~~event~~] logs to support monitoring and detection pursuant to Paragraph (3) of this subsection;

(5) in coordination with state and federal cybersecurity emergency management agencies as appropriate, create a model incident-response plan for public bodies to adopt with the cybersecurity office as the incident-response coordinator for incidents that:

(a) impact multiple public bodies;

(b) impact more than ten thousand residents of the state;

(c) involve a nation-state actor; or

(d) involve the marketing or transfer of confidential data derived from a breach of cybersecurity;

(6) serve as a cybersecurity resource for local governments;

(7) develop a service catalog of cybersecurity services to be offered to agencies and to political subdivisions of the state;

(8) collaborate with agencies in developing standards, functions and services in order to ensure the agency regulatory environments are understood and considered as part of a cybersecurity incident response;

(9) establish core services to support minimum security standards and policies;

(10) <u>adopt and implement rules to</u> establish minimum data classification policies and standards and design controls to support compliance with classifications and report

on exceptions;

(11) adopt and implement rules to develop and issue cybersecurity awareness policies and training standards and develop and offer cybersecurity training services; [~~and~~]

(12) adopt and implement rules to establish a centralized cybersecurity and data breach reporting process for agencies and political subdivisions of the state;

(13) approve agency cybersecurity and information security requests for proposals and invitations for bids that are subject to the Procurement Code, prior to final approval;

(14) approve agency cybersecurity and information security contracts and amendments to those contracts, including sole source contracts and price agreements, prior to final approval. Prior to making a cybersecurity or information security emergency procurement, an agency shall consult with the cybersecurity office and, upon making the procurement, shall immediately transmit notice of the procurement to the cybersecurity office; and

(15) review and make recommendations to the legislature on all agency, public school, higher education institution, county and municipality legislative appropriation requests related to cybersecurity and information security projects that incorporate protection of personal, sensitive or confidential information as defined by the cybersecurity office

by rule prior to submission of such appropriation requests to the legislature.

C. The security officer may issue orders:

(1) regarding agency compliance with rules, policies, standards or controls issued by cybersecurity office guidelines or recommendations of the cybersecurity advisory committee; and

(2) necessary to protect the state's digital assets from imminent threat.

D. Public bodies that receive general fund appropriations used for information technology resources and that are not subject to the jurisdiction of the security officer shall adopt and implement cybersecurity, information security and privacy policies, standards and procedures based upon no less than moderate-impact security control baselines, frameworks and standards issued by the national institute of standards and technology. A public body shall certify that it complied with the applicable standard during the preceding fiscal year. The certification shall be made in the form and manner specified by the security officer by a person who possesses the compliance qualifications specified by the security officer by rule. The security officer may report any compliance concerns to authorized oversight entities and cooperate with any compliance assessment.

E. A public body that is not under the jurisdiction of the security officer may voluntarily comply with the rules, standards, orders and other requirements of the Cybersecurity Act and participate in the cybersecurity and information security programs offered by the cybersecurity office."

SECTION 4. Section 9-27A-5 NMSA 1978 (being Laws 2023, Chapter 115, Section 5) is amended to read:

"9-27A-5. CYBERSECURITY ADVISORY COMMITTEE CREATED--MEMBERSHIP--DUTIES.--

A. The "cybersecurity advisory committee" is created within the cybersecurity office and shall:

(1) assist the office in the development of:

(a) a statewide cybersecurity plan;

(b) guidelines for best cybersecurity practices for agencies; and

(c) recommendations on how to respond to a specific cybersecurity threat or attack; and

(2) have authority over the hiring, supervision, discipline and compensation of the security officer.

B. The security officer or the security officer's designee shall chair and be [~~an advisory nonvoting~~] a voting member of the cybersecurity advisory committee; provided that the security officer shall be recused from deliberations and voting on matters concerning supervision, discipline or compensation of the security officer, and [~~the secretary of~~

~~information technology shall chair~~] the committee shall select an alternate person who is not an employee of the cybersecurity office to chair those deliberations and votes. The remaining members of the committee consist of:

(1) the secretary of [~~information technology~~] homeland security and emergency management or the secretary's designee;

(2) the principal information technology staff person for the administrative office of the courts or the [~~director's~~] staff person's designee;

(3) the director of the legislative council service or the director's designee;

(4) one member appointed by the secretary of Indian affairs, who is experienced with cybersecurity issues;

(5) three members appointed by the chair of the board of directors of the New Mexico association of counties who represent county governmental agencies and who are experienced with cybersecurity issues; provided that at least one member shall represent a county other than a class A or H class county;

(6) three members appointed by the chair of the board of directors of the New Mexico municipal league who represent municipal governmental agencies and who are experienced with cybersecurity issues; provided that only one member may represent a home rule municipality; [~~and~~]

(7) [~~three members appointed by the governor who may represent separate agencies other than the department of information technology and are experienced with cybersecurity issues~~] one member appointed by the governor who has experience with cybersecurity issues for public education institutions; and

(8) one member appointed by the governor who has experience with cybersecurity issues for public health institutions.

C. The cybersecurity advisory committee may invite representatives of unrepresented county, municipal or tribal agencies or other public entities to participate as advisory members of the committee as it determines that their participation would be useful to the deliberations of the committee.

D. A meeting of and material presented to or generated by the cybersecurity advisory committee are subject to the Open Meetings Act and the Inspection of Public Records Act subject to an exception for a meeting or material concerning information that could, if made public, expose a vulnerability in:

(1) an information system owned or operated by a public entity; or

(2) a cybersecurity solution implemented by a public entity.

underscored material = new
[~~bracketed material~~] = delete

[~~E. Pursuant to the Cybersecurity Act or other statutory authority, the security officer may issue orders regarding the compliance of agencies with guidelines or recommendations of the cybersecurity advisory committee; however, compliance with those guidelines or recommendations by non-executive agencies or county, municipal or tribal governments shall be strictly voluntary.~~

~~F.~~] E. The cybersecurity advisory committee shall hold its first meeting on or before August 16, 2023 and shall meet every two months at minimum after that; provided that the security officer shall have the discretion to call for more frequent meetings as circumstances warrant. At the discretion of the security officer, the committee may issue advisory reports regarding cybersecurity issues.

[~~G.~~] F. The cybersecurity advisory committee shall present a report to the legislative finance committee and the appropriate legislative interim committee concerned with information technology at those committees' November 2023 meetings and to the governor by November 30, 2023 regarding the status of cybersecurity preparedness within agencies and elsewhere in the state. On or before October 30, 2024 and on or before October 30 of each subsequent year, the cybersecurity office shall present updated reports to the legislative committees and the governor. The reports to legislative committees shall be in executive session, and any materials

underscored material = new
[~~bracketed material~~] = delete

connected with the report presentations are exempt from the Inspection of Public Records Act.

[~~H.~~] G. The members of the cybersecurity advisory committee shall receive no pay for their services as members of the committee, but shall be allowed per diem and mileage pursuant to the provisions of the Per Diem and Mileage Act. All per diem and contingent expenses incurred by the cybersecurity office shall be paid upon warrants of the secretary of finance and administration, supported by vouchers of the security officer."