SENATE RULES COMMITTEE SUBSTITUTE FOR
SENATE BILL 280

56TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2023

AN ACT

RELATING TO CYBERSECURITY; ENACTING THE CYBERSECURITY ACT; CREATING THE CYBERSECURITY OFFICE; PROVIDING DUTIES AND POWERS; CREATING THE POSITION OF STATE CHIEF INFORMATION SECURITY OFFICER; PROVIDING DUTIES; CREATING THE CYBERSECURITY ADVISORY COMMITTEE; PROVIDING EXEMPTIONS TO THE OPEN MEETINGS ACT AND INSPECTION OF PUBLIC RECORDS ACT; REQUIRING REPORTS.

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

SECTION 1. [NEW MATERIAL] SHORT TITLE.--This act may be cited as the "Cybersecurity Act".

SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the Cybersecurity Act:

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

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

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) acquisition, storage and conversion of hardware or solutions used to create, process, store, secure or exchange electronic data;

(3) information storage and retrieval;

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

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

(6) simulation and testing;

(7) related interactions between users and information systems; and

(8) user and system credentials; and

E. "security officer" means the state chief information security officer.

SECTION 3. [NEW MATERIAL] 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 information technology systems and infrastructure and provide appropriate governance and application of the standards and policies across 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;

(2) develop 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;

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

(3) consistent with information security standards, monitor agency information technology networks to detect security 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) establish minimum data classification policies and standards and design controls to support compliance with classifications and report on exceptions;

(11) develop and issue cybersecurity awareness policies and training standards and develop and offer cybersecurity training services; and

(12) establish a centralized cybersecurity and data breach reporting process for agencies and political subdivisions of the state.

SECTION 4. [NEW MATERIAL] STATE CHIEF INFORMATION SECURITY OFFICER--QUALIFICATIONS.--The position of "state chief information security officer" is created. The security officer shall be a classified information security position in accordance with rules promulgated pursuant to the Personnel Act and hired by the cybersecurity advisory committee.

SECTION 5. [NEW MATERIAL] 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:

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

(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 member of the cybersecurity advisory committee; provided that the security officer shall be recused from deliberations concerning supervision, discipline or compensation of the security officer and the secretary of information technology shall chair those deliberations. The remaining members consist of:

(1) the secretary of information technology or the secretary's designee;

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

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

(4) three members appointed by the secretary of Indian affairs, composed of one representative of the Navajo Nation, one representative of Apache tribal governments and one

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

representative of Indian pueblo tribal governments, who are experienced with cybersecurity issues;

(5) three members appointed by the security officer 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 security officer who represent municipal governmental agencies and who are experienced with cybersecurity issues; provided that only one member may represent a home rule municipality;

(7) a designee of the secretary of homeland security and emergency management who has experience with cybersecurity issues;

(8) a designee of the secretary of public education who has experience with cybersecurity issues; and

(9) a designee of the secretary of public safety who has experience with cybersecurity issues.

C. The cybersecurity advisory committee may form subcommittees to address specific or regional cybersecurity issues as it deems necessary.

D. 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

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

participation would be useful to the deliberations of the committee.

E. 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.

F. 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.

G. 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

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

reports regarding cybersecurity issues.

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

I. 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."

SECTION 6. TEMPORARY PROVISION--TRANSFER OF FUNCTIONS, PERSONNEL, MONEY, APPROPRIATIONS, PROPERTY, CONTRACTUAL OBLIGATIONS AND STATUTORY REFERENCES.--On the effective date of

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

this act:

A. all functions, personnel, money, appropriations, records, furniture, equipment, supplies and other property pertaining to cybersecurity or information security of the department of information technology are transferred to the cybersecurity office;

B. all contractual obligations of the department of information technology for cybersecurity or information security services are binding on the cybersecurity office;

C. all references in law to the chief information security officer of the department of information technology shall be deemed to be references to the state chief information security officer; and

D. the chief information security officer for the department of information technology shall become the initial state chief information security officer.

SECTION 7. EFFECTIVE DATE.--The effective date of the provisions of this act is July 1, 2023.

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