SENATE BILL 280

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

INTRODUCED BY

Michael Padilla and Debra M. Sariñana

AN ACT

RELATING TO CYBERSECURITY; ENACTING THE CYBERSECURITY ACT; CREATING THE CYBERSECURITY OFFICE; PROVIDING DUTIES AND POWERS; CREATING THE POSITION OF STATE INFORMATION SECURITY OFFICER; PROVIDING DUTIES; ESTABLISHING QUALIFICATIONS; CREATING THE CYBERSECURITY ADVISORY COMMITTEE; PROVIDING EXEMPTIONS TO THE OPEN MEETINGS ACT AND INSPECTION OF PUBLIC RECORDS ACT; AMENDING A SECTION OF THE DEPARTMENT OF INFORMATION TECHNOLOGY ACT TO INCLUDE REVIEW AND APPROVAL OF RATES AND FEES FOR SERVICES BY THE CYBERSECURITY OFFICE IN THE DUTIES OF THE INFORMATION TECHNOLOGY RATE COMMITTEE; REQUIRING REPORTS.

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

SECTION 1. [NEW MATERIAL] SHORT TITLE.--Sections 1 through 5 of this act may be cited as the "Cybersecurity Act".

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

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

Cybersecurity Act:

A. "agency", unless otherwise specified, means an agency within the executive branch of state government;

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;

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

(6) simulation and testing; and

(7) related interactions between users and information systems; 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. The cybersecurity office is responsible for all cybersecurity and information security related functions for agencies and shall:

(1) establish security standards and policies to protect agency information technology systems and infrastructure, provide appropriate governance and application of the standards and policies across information technology resources used by agencies and ensure the availability, confidentiality and integrity of the information processed, transacted or stored by agencies in the state's information technology infrastructure and systems;

(2) develop cybersecurity protocols for managing and protecting information technology assets and infrastructure for all entities that are connected to an

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

agency-operated or -owned telecommunications network or that receive funding from agencies used to operate or own information technology;

(3) detect, mitigate and monitor security incidents consistent with information security standards and policies;

(4) access information technology systems connected to agency-operated or -owned telecommunications networks as reasonably necessary for detection and monitoring pursuant to Paragraph (3) of this subsection;

(5) in coordination with state and federal cybersecurity emergency management agencies, 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

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

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) define core services that will be required to be managed by agency information technology security programs;

(10) establish data classification policies and standards and design controls to comply with classifications and report on exceptions;

(11) define cybersecurity awareness policies and training standards and develop and provide cybersecurity training services; and

(12) define cybersecurity and data breach notification standards for agencies and publish the standards as recommendations for non-executive 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 appointed by the secretary of information technology, shall be a classified employee as established pursuant to the Personnel Act by the state personnel office by rule and shall have the following minimum qualifications:

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

A. a postgraduate degree in engineering, management, science or technology;

B. at least two non-vendor-issued information technology related certifications; and

C. at least fifteen years of employment or consulting experience in information-technology-related enterprises, including:

(1) at least five years of employment with or consulting for a government agency or a publicly traded corporation; and

(2) at least five years of experience as a manager of an engineering, a science or a technology enterprise or an agency.

SECTION 5. [NEW MATERIAL] CYBERSECURITY ADVISORY COMMITTEE CREATED--MEMBERSHIP--DUTIES.--

A. The "cybersecurity advisory committee" is created within the cybersecurity office to assist the office in the development of:

(1) a statewide cybersecurity plan;

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

(3) recommendations on how to respond to a specific cybersecurity threat or attack.

B. The security officer or the security officer's designee shall chair and be a voting member of the

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

cybersecurity advisory committee and the remaining members shall 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 that staff person's designee;

(3) the principal information technology staff person for the legislative council service or that staff person'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 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; and

(7) two members appointed by the governor who

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

represent separate agencies other than the department of information technology and who are experienced with cybersecurity issues.

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

D. The security officer may invite representatives of unrepresented county, municipal or tribal agencies or public educational institutions to participate as advisory members of the cybersecurity advisory committee as the security officer determines their participation would be useful to the deliberations of the committee.

E. The meetings of the cybersecurity advisory committee are exempt from the Open Meetings Act.

F. Materials presented to or generated by the cybersecurity advisory committee pursuant to its duties described in Subsection A of this section and minutes or recordings of its meetings are exempt from the Inspection of Public Records Act.

G. 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

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

governments shall be strictly voluntary.

H. 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.

I. 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 governor. The report presentations 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.

J. 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.

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

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. Section 9-27-7 NMSA 1978 (being Laws 2007, Chapter 290, Section 7, as amended) is amended to read:

"9-27-7. INFORMATION TECHNOLOGY RATE COMMITTEE--MEMBERSHIP--DUTIES.--

A. The "information technology rate committee" is created. The committee consists of seven members as follows:

(1) five members appointed by the governor from [~~executive~~] agencies that use information technology services and pay rates to an internal service fund;

(2) the secretary of finance and administration, who shall serve as chair of the committee; and

(3) the secretary of information technology.

B. The information technology rate committee shall:

(1) review the rate and fee schedule proposed by the secretary;

(2) review the rate and fee schedule proposed by the cybersecurity office for its services provided pursuant to the Cybersecurity Act;

[~~(2)~~] (3) ensure that the rate and fee [~~schedule complies~~] schedules comply with the federal office of management and budget circular A-87 or its successor directive;

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

[~~(3)~~] (4) consider for approval [~~an~~] equitable rate and fee [~~schedule~~] schedules based on cost recovery for [~~state~~] agencies that use information technology services and pay rates to an internal service fund, with priority service to public safety agencies;

[~~(4)~~] (5) present the committee's proposed rate and fee [~~schedule~~] schedules by June 1 of each year to the office of the governor, the department of finance and administration and the legislative finance committee; and

[~~(5)~~] (6) by July 15 of each year, implement [~~a rate and fee schedule~~] rate and fee schedules based on the committee's recommendations; provided, however, that a reduction in rates or fees by the department shall not require the committee's approval if the reduction is based on cost recovery and if the committee is notified timely."

SECTION 7. TEMPORARY PROVISION--TRANSFER OF FUNCTIONS, PERSONNEL, MONEY, APPROPRIATIONS, PROPERTY, CONTRACTUAL OBLIGATIONS AND STATUTORY REFERENCES.--

A. On the effective date of this act, 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. On the effective date of this act, all

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

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

C. On the effective date of this act, 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.

SECTION 8. EFFECTIVE DATE.--The effective date of the provisions of this act is July 1, 2023.

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