

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:

.228048.1

underscoring material = new
[bracketed material] = delete

1 "9-27A-2. DEFINITIONS.--As used in the Cybersecurity Act:

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

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

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

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

18 (1) systems design and analysis;

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

22 (3) information storage and retrieval systems;

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

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

.228048.1

1 (6) simulation and testing;

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

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

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

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

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

13 "9-27A-3. CYBERSECURITY OFFICE CREATED--SECURITY
14 OFFICER--DUTIES AND POWERS.--

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

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

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

.228048.1

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

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

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

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

.228048.1

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

- 6 (a) impact multiple public bodies;
- 7 (b) impact more than ten thousand
8 residents of the state;
- 9 (c) involve a nation-state actor; or
- 10 (d) involve the marketing or transfer of
11 confidential data derived from a breach of cybersecurity;

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

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

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

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

23 (10) adopt and implement rules to establish
24 minimum data classification policies and standards and design
25 controls to support compliance with classifications and report

.228048.1

underscored material = new
[bracketed material] = delete

1 on exceptions;

2 (11) adopt and implement rules to develop and
3 issue cybersecurity awareness policies and training standards
4 and develop and offer cybersecurity training services; ~~and~~

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

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

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

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

.228048.1

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

3 C. The security officer may issue orders:

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

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

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

25 E. A public body that is not under the jurisdiction

.228048.1

1 of the security officer may voluntarily comply with the rules,
2 standards, orders and other requirements of the Cybersecurity
3 Act and participate in the cybersecurity and information
4 security programs offered by the cybersecurity office."

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

7 "9-27A-5. CYBERSECURITY ADVISORY COMMITTEE CREATED--
8 MEMBERSHIP--DUTIES.--

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

- 11 (1) assist the office in the development of:
12 (a) a statewide cybersecurity plan;
13 (b) guidelines for best cybersecurity
14 practices for agencies; and
15 (c) recommendations on how to respond to
16 a specific cybersecurity threat or attack; and

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

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

.228048.1

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

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

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

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

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

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

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

.228048.1

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

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

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

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

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

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

.228048.1

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

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

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

.228048.1

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

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