

1 SENATE BILL 254

2 **57TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2025**

3 INTRODUCED BY

4 Michael Padilla and Debra M. Sariñana

5
6
7
8
9
10 AN ACT

11 RELATING TO CYBERSECURITY; AMENDING THE CYBERSECURITY ACT;
12 CHANGING THE NAME AND DUTIES OF THE CYBERSECURITY OFFICE;
13 CHANGING THE MEMBERSHIP OF THE CYBERSECURITY ADVISORY
14 COMMITTEE.

15
16 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

17 SECTION 1. Section 9-27A-3 NMSA 1978 (being Laws 2023,
18 Chapter 115, Section 3) is amended to read:

19 "9-27A-3. [~~CYBERSECURITY~~] OFFICE OF CYBERSECURITY
20 CREATED--SECURITY OFFICER--DUTIES AND POWERS.--

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

25 B. Except as required by federal law, the

.229897.2

underscored material = new
[bracketed material] = delete

underscored material = new
[bracketed material] = delete

1 [cybersecurity] office of cybersecurity shall oversee, in a
2 fiscally responsible manner, cybersecurity- and information
3 security-related functions for agencies and may:

4 (1) adopt and implement rules establishing
5 minimum security standards and policies to protect agency
6 information technology systems and infrastructure and provide
7 appropriate governance and application of the standards and
8 policies across information technology resources used by
9 agencies to promote the availability, security and integrity of
10 the information processed, transacted or stored by agencies in
11 the state's information technology infrastructure and systems;

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

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

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

25 (5) in coordination with state and federal

.229897.2

1 cybersecurity emergency management agencies as appropriate,
2 create a model incident-response plan for public bodies to
3 adopt with the [~~cybersecurity~~] office of cybersecurity as the
4 incident-response coordinator for incidents that:

- 5 (a) impact multiple public bodies;
- 6 (b) impact more than ten thousand
7 residents of the state;
- 8 (c) involve a nation-state actor; or
- 9 (d) involve the marketing or transfer of
10 confidential data derived from a breach of cybersecurity;
- 11 (6) serve as a cybersecurity resource for
12 local governments;
- 13 (7) develop a service catalog of cybersecurity
14 services to be offered to agencies and to political
15 subdivisions of the state;
- 16 (8) collaborate with agencies in developing
17 standards, functions and services in order to ensure the agency
18 regulatory environments are understood and considered as part
19 of a cybersecurity incident response;
- 20 (9) establish core services to support minimum
21 security standards and policies;
- 22 (10) establish minimum data classification
23 policies and standards and design controls to support
24 compliance with classifications and report on exceptions;
- 25 (11) develop and issue cybersecurity awareness

.229897.2

underscored material = new
[bracketed material] = delete

1 policies and training standards and develop and offer
2 cybersecurity training services; and

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

6 SECTION 2. Section 9-27A-5 NMSA 1978 (being Laws 2023,
7 Chapter 115, Section 5) is amended to read:

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

10 A. The "cybersecurity advisory committee" is
11 created within the [~~cybersecurity~~] office of cybersecurity and
12 shall:

13 (1) assist the office in the development of:

- 14 (a) a statewide cybersecurity plan;
- 15 (b) guidelines for best cybersecurity
16 practices for agencies; and

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

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

22 B. The security officer or the security officer's
23 designee shall chair [~~and be an advisory nonvoting member of~~]
24 the cybersecurity advisory committee; provided that the
25 security officer shall be recused from deliberations and votes

.229897.2

underscored material = new
[bracketed material] = delete

1 concerning supervision, discipline or compensation of the
2 security officer and the secretary of information technology
3 shall chair those deliberations. The remaining members consist
4 of:

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

7 (2) [~~the principal information technology~~
8 ~~staff person for the administrative office of the courts or the~~
9 ~~director's designee~~] one member appointed by the chief justice
10 of the supreme court who is experienced with cybersecurity
11 issues;

12 (3) [~~the director of the legislative council~~
13 ~~service or the director's designee~~] a member of the legislature
14 appointed by the New Mexico legislative council who is familiar
15 with cybersecurity issues;

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

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

24 (6) [~~three~~] two members appointed by the chair
25 of the board of directors of the New Mexico municipal league

.229897.2

underscoring material = new
[bracketed material] = delete

1 who represent municipal governmental agencies and who are
2 experienced with cybersecurity issues; provided that only one
3 member may represent a home rule municipality; and

4 (7) ~~[three]~~ four members appointed by the
5 governor who ~~[may represent separate agencies other than the~~
6 ~~department of information technology and]~~ are experienced with
7 cybersecurity issues; provided that at least one appointee
8 shall be:

9 (a) an educator or employed by an
10 education institution;

11 (b) a health care provider or employed
12 by a health care provider;

13 (c) employed by the homeland security
14 and emergency management department; and

15 (d) a private sector cybersecurity
16 expert or employed by a business offering cybersecurity
17 services.

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

24 D. A meeting of and material presented to or
25 generated by the cybersecurity advisory committee are subject

.229897.2

1 to the Open Meetings Act and the Inspection of Public Records
2 Act subject to an exception for a meeting or material
3 concerning information that could, if made public, expose a
4 vulnerability in:

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

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

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

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

23 G. The cybersecurity advisory committee shall
24 present a report to the legislative finance committee and the
25 appropriate legislative interim committee concerned with

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

1 information technology at those committees' November 2023
2 meetings and to the governor by November 30, 2023 regarding the
3 status of cybersecurity preparedness within agencies and
4 elsewhere in the state. On or before October 30, 2024 and on
5 or before October 30 of each subsequent year, the
6 ~~[cybersecurity]~~ office of cybersecurity shall present updated
7 reports to the legislative committees and the governor. The
8 reports to legislative committees shall be in executive
9 session, and any materials connected with the report
10 presentations are exempt from the Inspection of Public Records
11 Act.

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