

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

SENATE BILL

55TH LEGISLATURE - STATE OF NEW MEXICO - SECOND SESSION, 2022

INTRODUCED BY

Michael Padilla

AN ACT

RELATING TO CYBERSECURITY; ENACTING THE CYBERSECURITY ACT;
ESTABLISHING THE CYBERSECURITY OFFICE; CREATING THE
CYBERSECURITY ADVISORY COMMITTEE; ESTABLISHING THE
INTRAGOVERNMENTAL CYBERSECURITY COORDINATING COMMITTEE;
CREATING THE STATE CHIEF OF INFORMATION SECURITY AND CHIEF
INFORMATION SECURITY OFFICERS FOR THE ADMINISTRATIVE OFFICE OF
THE COURTS AND THE LEGISLATIVE COUNCIL SERVICE; PROVIDING
POWERS AND DUTIES; REQUIRING RULEMAKING AND REPORTS; MAKING
APPROPRIATIONS; DECLARING AN EMERGENCY.

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

SECTION 1. [NEW MATERIAL] SHORT TITLE.--Sections 1
through 7 of this act may be cited as the "Cybersecurity Act".

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

.221320.1

underscoring material = new
[bracketed material] = delete

1 A. "chief information security officer" means the
2 person responsible for developing and implementing a
3 cybersecurity program, including standards designed to protect
4 agency communications, systems and assets from both internal
5 and external threats;

6 B. "cybersecurity" means the protection of digital
7 information networks, devices and data from unauthorized access
8 or criminal use to ensure the confidentiality, integrity and
9 availability of the digital information;

10 C. "elective state officer" means a state official
11 who is elected to an executive office established in the
12 constitution of New Mexico as a separate entity from the
13 agencies that are under the purview of the governor and
14 includes the agency that the official administers;

15 D. "local government" means the government of a
16 municipality, county or political subdivision of the state;

17 E. "public educational institution" means a public
18 school, a school district, a public post-secondary educational
19 institution or a state agency that provides administrative,
20 funding or technical support to public schools, school
21 districts and public post-secondary educational institutions;

22 F. "standards" means standards, procedures and
23 requirements adopted by a chief information security officer to
24 ensure the cybersecurity of information technology and
25 databases owned or maintained by a governmental agency or to

underscoring material = new
[bracketed material] = delete

1 respond to a cybersecurity threat or actual breach of
2 cybersecurity experienced by a governmental agency; and

3 G. "statewide cybersecurity plan" means a five-year
4 plan, including recommended statutory changes and
5 implementation requirements for the development and
6 implementation of standards, for:

7 (1) responding to cyberattacks and database
8 intrusions and recommended cybersecurity training programs and
9 certifications for state employees;

10 (2) requiring collaboration among state
11 agencies, local government agencies, public educational
12 institutions and tribal agencies on cybersecurity and
13 responses;

14 (3) formally including local government
15 agencies, or public educational institutions, in the statewide
16 cybersecurity plan; and

17 (4) entering into state-tribal or interstate
18 agreements regarding cybersecurity.

19 SECTION 3. [NEW MATERIAL] CYBERSECURITY OFFICE CREATED--
20 STATE CHIEF OF INFORMATION SECURITY--STANDARDS.--

21 A. The "cybersecurity office" is created within the
22 department of information technology.

23 B. The cybersecurity office shall be managed by the
24 "state chief of information security", who shall be appointed
25 by the secretary of information technology. The state chief of

.221320.1

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

1 information security may hire staff as needed to meet the
2 responsibilities of the cybersecurity office.

3 C. The cybersecurity office shall:

4 (1) establish preliminary standards on or
5 before September 1, 2022 for all executive state agencies, and
6 on or before September 1, 2023, update and adopt the standards
7 by rule;

8 (2) develop a statewide cybersecurity plan
9 pursuant to Section 4 of the Cybersecurity Act; and

10 (3) coordinate with the chief information
11 security officers for the legislative council service, the
12 administrative office of the courts and the elective state
13 officers regarding standards for response actions to
14 cybersecurity breaches.

15 SECTION 4. ~~[NEW MATERIAL]~~ STATEWIDE CYBERSECURITY PLAN--
16 ASSISTANCE FOR LOCAL GOVERNMENTS.--

17 A. On or before September 1, 2022, the
18 cybersecurity office shall develop and present to the governor
19 and the appropriate legislative interim committee a preliminary
20 five-year statewide cybersecurity plan. The preliminary plan
21 shall include an assessment of cybersecurity services for
22 governmental agencies and public educational institutions
23 across the state compared to the standards established by
24 various federal requirements for research grants or education
25 or cybersecurity assistance programs.

.221320.1

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

1 B. On or before July 1, 2023, the cybersecurity
2 office shall adopt a revised and updated five-year statewide
3 cybersecurity plan by rule and shall present the adopted plan
4 to the governor and the appropriate legislative interim
5 committee.

6 C. On or before July 1, 2024 and on or before July
7 1 of each year thereafter, the cybersecurity office shall
8 update and revise the statewide cybersecurity plan and present
9 the updated and revised plan to the governor and the
10 appropriate legislative interim committee.

11 D. In the development of the statewide
12 cybersecurity plan, the cybersecurity office shall request
13 advice and provide opportunities for meaningful input from each
14 local and tribal government within New Mexico, and all state
15 agencies and public educational institutions shall cooperate
16 with and provide relevant cybersecurity-related information
17 collected or developed by the agencies as requested by the
18 cybersecurity office.

19 E. The cybersecurity office shall provide planning
20 and technical assistance to local governments, public
21 educational institutions and state agencies in the design,
22 development or implementation of plans for the development of
23 cybersecurity. When providing planning and technical
24 assistance, the cybersecurity office shall encourage the use of
25 regional planning and may provide planning and technical

.221320.1

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

1 assistance to tribal government agencies and schools when those
2 entities are participants in a joint powers agreement with a
3 local government, public educational institution or state
4 agency or a memorandum of understanding for the design,
5 development or implementation of a regional cybersecurity plan.

6 SECTION 5. [NEW MATERIAL] CYBERSECURITY ADVISORY
7 COMMITTEE.--

8 A. The "cybersecurity advisory committee" is
9 created to assist the cybersecurity office in the development
10 of the statewide cybersecurity plan.

11 B. The cybersecurity advisory committee consists
12 of:

13 (1) the state chief of information security;
14 (2) the chief information security officer for
15 the administrative office of the courts;

16 (3) the chief information security officer for
17 the legislative council service;

18 (4) three members appointed by the secretary
19 of Indian affairs, including one representative of the Navajo
20 Nation, one representative of Apache tribal governments and one
21 representative of Indian pueblo tribal governments, who have
22 experience with cybersecurity issues;

23 (5) three members appointed by the state chief
24 of information security representing county governmental
25 agencies, who have experience with cybersecurity issues;

.221320.1

1 provided that at least one member shall represent a county
2 other than a class A or an H class county;

3 (6) three members appointed by the state chief
4 of information security representing municipal governmental
5 agencies, who have experience with cybersecurity issues;
6 provided that only one member may represent a home rule
7 municipality; and

8 (7) three members appointed by the governor,
9 who represent different state agencies.

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

13 D. The state chief of information security may
14 invite representatives of unrepresented state, county, local or
15 tribal agencies or public educational institutions to
16 participate as ex-officio members of the cybersecurity advisory
17 committee if the state chief of information security determines
18 that their participation would be useful to the development of
19 the state cybersecurity plan.

20 E. The state chief of information security shall
21 convene the initial meeting of the cybersecurity advisory
22 committee within sixty days of the enactment of the
23 Cybersecurity Act. After its initial meeting, the committee
24 shall meet at least once a month until a statewide
25 cybersecurity plan is adopted pursuant to Subsection B of

.221320.1

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

1 Section 4 of the Cybersecurity Act. After a statewide
2 cybersecurity plan is adopted, the advisory committee shall
3 meet as deemed necessary by the state chief of information
4 security, but at least once prior to August 1 of each year.

5 SECTION 6. [NEW MATERIAL] COORDINATION OF STATE AND LOCAL
6 GOVERNMENT CYBERSECURITY EFFORTS.--

7 A. The cybersecurity office shall identify federal
8 and nongovernmental cybersecurity funding assistance
9 opportunities for local governments, public educational
10 institutions, state agencies and tribal governments and shall
11 publish a list of those opportunities in a manner that can be
12 searched on a county-by-county basis.

13 B. The cybersecurity office shall be the applicant
14 for federal cybersecurity funding assistance for all executive
15 state agencies; provided that with approval of the supreme
16 court, the administrative office of the courts may
17 independently apply for federal cybersecurity assistance; and
18 provided further that with approval of the New Mexico
19 legislative council, the legislative council service may
20 independently apply for federal cybersecurity assistance.

21 C. The cybersecurity office shall coordinate with
22 state agencies and public educational institutions and,
23 pursuant to applicable state-tribal or interstate agreements,
24 may coordinate with tribal agencies or with agencies from other
25 states for the purchase of cybersecurity software, hardware and

.221320.1

underscored material = new
[bracketed material] = delete

1 services with the goal of implementing bulk pricing agreements.

2 SECTION 7. [NEW MATERIAL] VACANCIES--INTRAGOVERNMENTAL
3 CYBERSECURITY COORDINATION COMMITTEE.--

4 A. The "intragovernmental cybersecurity
5 coordination committee" is established. The committee consists
6 of the state chief of information security, the chief
7 information security officer for the administrative office of
8 the courts, the chief information security officer for the
9 legislative council service and the elective state officers or
10 the elective state officers' designees; provided that:

11 (1) if the position of state chief of
12 information security is vacant, the secretary of information
13 technology or the secretary's designee shall serve as the
14 acting state chief of information security;

15 (2) if the position of chief information
16 security officer for the administrative office of the courts is
17 vacant, the director of the administrative office of the courts
18 or the director's designee shall serve as the acting chief
19 information security officer; and

20 (3) if the position of chief information
21 security officer for the legislative council service is vacant,
22 the director of the legislative council service or the
23 director's designee shall serve as the acting chief information
24 security officer.

25 B. Within thirty days of the enactment of the

.221320.1

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

1 Cybersecurity Act and at least quarterly thereafter, the
2 intragovernmental cybersecurity coordination committee shall
3 meet to ensure that the standards for each branch of government
4 are compatible.

5 SECTION 8. A new section of Chapter 2, Article 3 NMSA
6 1978 is enacted to read:

7 "[NEW MATERIAL] CHIEF INFORMATION SECURITY OFFICER--
8 DUTIES.--

9 A. The position of "chief information security
10 officer" is created within the legislative council service, and
11 the director of the legislative council service shall appoint
12 the chief information security officer.

13 B. The chief information security officer shall:

14 (1) develop and implement standards as defined
15 in the Cybersecurity Act for the legislature and its
16 committees, staff and services;

17 (2) coordinate the development and
18 implementation of standards with the state chief of information
19 security and the chief information security officer for the
20 administrative office of the courts pursuant to Section 7 of
21 the Cybersecurity Act; and

22 (3) on or before September 1, 2022 and by
23 September 1 of each subsequent year, provide a report to the
24 New Mexico legislative council and the appropriate legislative
25 interim committee regarding the development of standards and

.221320.1

underscored material = new
[bracketed material] = delete

1 the status of cybersecurity as defined in the Cybersecurity Act
2 for the legislature, legislative committees and the legislative
3 council service.

4 C. The report provided pursuant to Subsection B of
5 this section shall be confidential and only presented in an
6 executive session of the New Mexico legislative council or the
7 appropriate legislative interim committee."

8 SECTION 9. A new section of Chapter 34, Article 9 NMSA
9 1978 is enacted to read:

10 "[NEW MATERIAL] CHIEF INFORMATION SECURITY OFFICER--
11 DUTIES.--

12 A. The position of "chief information security
13 officer" is created within the administrative office of the
14 courts, and the director of the administrative office of the
15 courts shall appoint the chief information security officer.

16 B. The chief information security officer shall:

17 (1) develop and implement standards as defined
18 in the Cybersecurity Act for the administrative office of the
19 courts and the courts;

20 (2) coordinate the development and
21 implementation of standards with the state chief of information
22 security and the chief information security officer for the
23 legislative council service pursuant to Section 7 of the
24 Cybersecurity Act; and

25 (3) on or before September 1, 2022 and by

.221320.1

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

1 September 1 of each subsequent year, provide a report to the
2 supreme court regarding the development of standards and the
3 status of cybersecurity as defined in the Cybersecurity Act for
4 the state's court system.

5 C. The report provided pursuant to Subsection B of
6 this section shall be confidential and only presented in a
7 closed session of the supreme court."

8 SECTION 10. APPROPRIATIONS.--

9 A. One million dollars (\$1,000,000) is appropriated
10 from the general fund to the department of information
11 technology for expenditure in fiscal years 2022 and 2023 to
12 establish and operate the cybersecurity office. The
13 appropriation may be used to hire up to five full-time-
14 equivalent staff. Any unexpended or unencumbered balance
15 remaining at the end of fiscal year 2023 shall revert to the
16 general fund.

17 B. One hundred fifty thousand dollars (\$150,000) is
18 appropriated from the general fund to the legislative council
19 service for expenditure in fiscal years 2022 and 2023 to
20 establish the position of chief information security officer
21 for the legislative council service. Any unexpended or
22 unencumbered balance remaining at the end of fiscal year 2023
23 shall revert to the general fund.

24 C. One hundred fifty thousand dollars (\$150,000) is
25 appropriated from the general fund to the administrative office

.221320.1

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

1 of the courts for expenditure in fiscal years 2022 and 2023 to
2 establish the position of chief information security officer
3 for the administrative office of the courts. Any unexpended or
4 unencumbered balance remaining at the end of fiscal year 2023
5 shall revert to the general fund.

6 SECTION 11. EMERGENCY.--It is necessary for the public
7 peace, health and safety that this act take effect immediately.

8 - 13 -

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25