NATIONAL CONFERENCE OF STATE LEGISLATURES
7700 EAST FIRST PLACE DENVER, COLORADO 80230
303-364-7700 FAX: 303-364-7800

**State Cybersecurity Statutes Referencing the National Institute of Standards**
In at least 14 states: Calif., Colo., Conn., Fla., Ga., Ky., Md., Minn., Nev., New Jersey, Ohio, Okla., Tex., Wash.
*As of April 7, 2022*

**California**

Cal Gov Code § 12168.7
Government Code > Title 2. Government of the State of California > Division 3. Executive Department > Part 2. Constitutional Officers > Chapter 3. Secretary of State > Article 2. Duties > Uniform standards for storing and recording documents in electronic media; Trusted system for recording documents; Cloud computing storage service [Effective until January 1, 2026]
(1) "Cloud computing" has the same definition as the term is defined by the **National Institute of Standards and Technology** Special Publication 800-145, or a successor publication, and includes the service and deployment models referenced therein.

Cal Pen Code § 11077.2
Penal Code > Part 4. Prevention of Crimes and Apprehension of Criminals > Title 1. Investigation and Control of Crimes and Criminals > Chapter 1. Investigation, Identification, and Information Responsibilities of the Department of Justice > Article 2.5. Criminal Record Dissemination > Establishment of communication network to allow electronic transmission of requests from certain private service providers for criminal offender record information
(d) Users of the communication network shall only use hardware and software in relation to or for connection to the communication network that is currently approved and certified by the department, the **National Institute of Standards and Technology**, and the Federal Bureau of Investigation.

Cal Pub Resources Code § 25402
Public Resources Code > Division 15. Energy Conservation and Development > Chapter 5. Energy Resources Conservation > Reduction of wasteful consumption of energy; Water efficiency and conservation standards
(2) In adopting the flexible demand appliance standards, the commission shall consider the **National Institute of Standards and Technology's** reliability and cybersecurity protocols, or other cybersecurity protocols that are equally or more protective, and shall adopt, at a minimum, the North American Electric Reliability Corporation's Critical Infrastructure Protection standards.

Cal Pub Util Code § 740.16
Public Utilities Code > Division 1. Regulation of Public Utilities > Part 1. Public Utilities Act > Chapter 4. Regulation of Public Utilities > Article 2. Rates > Legislative findings and declarations; Electric vehicle grid integration
(5) The commission shall consider incorporating the **National Institute of Standards and Technology's** reliability and cybersecurity protocols, or other equally protective or more protective cybersecurity protocols, into the electric vehicle grid integration strategies.

Cal Pub Util Code § 8362

Public Utilities Code > Division 4.1. Provisions Applicable to Privately Owned and Publicly Owned Public Utilities > Chapter 4. Smart Grid Systems > Determining requirements for smart grid; Standards and protocols; Products by non-electrical corporations; Required improvements

The commission shall institute a rulemaking or expand the scope of an existing rulemaking to adopt standards and protocols to ensure functionality and interoperability developed by public and private entities, including, but not limited to, the **National Institute of Standards and Technology**, Gridwise Architecture Council, the International Electrical and Electronics Engineers, and the National Electric Reliability Organization recognized by the Federal Energy Regulatory Commission.

**Colorado**

C.R.S. § 2-3-103

Title 2. Legislative > Title 2. Legislative Services > Article 3. Legislative Services > Part 1. Legislative Audit Committee - State Auditor > Duties of state auditor - definition

(b) Any testing or assessment of security practices and procedures concerning information technology in accordance with paragraph (a) of this subsection (1.5) shall be conducted or caused to be conducted by the state auditor: (I) After consultation and in coordination with, but not requiring the approval of, the chief information officer appointed pursuant to section 24-37.5-103, C.R.S., or any person performing comparable duties for either a state agency that is not under the jurisdiction of the office of information technology created in section 24-37.5-103, C.R.S., or a political subdivision of the state; (II) In accordance with industry standards prescribed by the **national institute of standards and technology** or any successor agency;

C.R.S. § 24-33.5-1905

Title 24. Government - State > Title 24 Principal Departments > Article 33.5. Public Safety > Part 19. Colorado Cybersecurity > Research and development

(1) The university of Colorado at Colorado Springs may partner with a nonprofit organization that supports national, state, and regional cybersecurity initiatives to work to establish a secure environment for research and development, initial operational testing and evaluation, and expedited contracting for production for industrial cyber products and techniques. (2) In furtherance of subsection (1) of this section, the university of Colorado at Colorado Springs and any nonprofit organization with which the university has a partnership may consider the following: ….

(j) Encouraging coordination with the United States department of commerce and the national institute of standards and technologies to develop the capability to act as a Colorado instate center of excellence on cybersecurity advice and **national institute of standards and technologies** standards;

**Connecticut**

Conn. Gen. Stat. § 42-901

Title 42 Business, Selling, Trading and Collection Practices > Chapter 743ii Motor Fuel Industry Market Concentration > Cybersecurity programs adopted by businesses

(c) A covered entity's cybersecurity program, as described in subsection (b) of this section, conforms to an industry recognized cybersecurity framework if:

(1) (A) The cybersecurity program conforms to the current version of or any combination of the current versions of:

(i) The “Framework for Improving Critical Infrastructure Cybersecurity” published by the **National Institute of Standards and Technology**;

(ii) The **National Institute of Standards and Technology's** special publication 800-171;

(iii) The **National Institute of Standards and Technology's** special publications 800-53 and 800-53a;

**Florida**

Fla. Stat. § 282.0041

Title XIX. Public Business. > Chapter 282. Communications and Data Processing. > Part I. Enterprise Information Technology Services Management. > Definitions

(5) "Cloud computing" has the same meaning as provided in Special Publication 800-145 issued by the **National Institute of Standards and Technology**.

Fla. Stat. § 282.0051

Title XIX. Public Business. > Chapter 282. Communications and Data Processing. > Part I. Enterprise Information Technology Services Management. > Department of Management Services; Florida Digital Service; powers, duties, and functions.

(q)1. Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The information technology policy must include: ….

f. At a minimum, a requirement that any contract for information technology commodities or services meet the **National Institute of Standards and Technology Cybersecurity Framework**.

Fla. Stat. § 282.318(3)

Title XIX. Public Business. > Chapter 282. Communications and Data Processing. > Part I. Enterprise Information Technology Services Management. Cybersecurity. > Cybersecurity

(3) The department, acting through the Florida Digital Service, is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures. Such standards and processes must be consistent with generally accepted technology best practices, including **the National Institute for Standards and Technology Cybersecurity Framework**, for cybersecurity

Fla. Stat. § 282.319(10)

Title XIX. Public Business. > Chapter 282. Communications and Data Processing. > Part I. Enterprise Information Technology Services Management. > Florida Cybersecurity Advisory Council

(10) The council shall work with the **National Institute of Standards and Technology** and other federal agencies, private sector businesses, and private cybersecurity experts

Fla. Stat. § 282.0051(q)(1)(f)

Title XIX. Public Business> Chapter 282. Communications and Data Processing. > Department of Management Services; Florida Digital Service; powers, duties, and functions

f. At a minimum, a requirement that any contract for information technology commodities or services meet the **National Institute of Standards and Technology** Cybersecurity Framework.

**Georgia**

O.C.G.A. § 45-13-20

Title 45 Public Officers and Employees > Chapter 13 Secretary of State > Article 2 Powers and Duties Generally > Duties of Secretary of State generally.

(14.1) To promulgate a regulation that establishes security protocols for voter registration information maintained and developed by the Secretary of State pursuant to Code Section 21-2-211 and 52 U.S.C. Section 21083. The regulation shall be generally consistent with current industry security standards, and in promulgating the regulation, the Secretary of State shall consider those security standards issued by the **National Institute of Standards and Technology**, the Center for Internet Security, and the federal Election Assistance Commission.

**Kentucky**

Ky. Rev. Stat. § 61.931(3)(a)

Title VIII Offices and Officers > Chapter 61 General Provisions as to Offices and Officers — Social Security for Public Employees — Employees Retirement System > Chapter 61 Personal Information Security and Breach Investigations; Definitions for 61.931(3)(a) to 61.934

(3) "Encryption" means the conversion of data using technology that: (a) Meets or exceeds the level adopted by the **National Institute of Standards Technology** as part of the Federal Information Processing Standards: and

**Maryland**

Md. State Government Code § 9-2901(j)

State Government > Title 9. Miscellaneous Executive Agencies. > Subtitle 29. Maryland Cybersecurity Council.

(j) The Council shall work with the **National Institute of Standards and Technology** and other federal agencies, private sector businesses, and private cybersecurity experts to: ….

(4) assist private sector cybersecurity businesses in adopting, adapting, and implementing the **National Institute of Standards and Technology** cybersecurity framework of standards and practices;

Md. State Government Code § 10-13A-01

State Government > Title 10. Governmental Procedures. > Subtitle 13A. Protection of Personally Identifiable Information by Public Institutions of Higher Education > Definitions

(c) "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using a technology that:

(1) is certified to meet or exceed the level that has been adopted by the Federal Information Processing Standards issued by the **National Institute of Standards and Technology;**

Md. State Government Code § 10-1301

State Government > Title 10. Governmental Procedures. > Subtitle 13. Protection of Information by Government Agencies > Definitions

(a) In this subtitle the following words have the meanings indicated.

(b) "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using a technology that:

(1) is certified to meet or exceed the level that has been adopted by the Federal Information Processing Standards issued by the **National Institute of Standards and Technology**; and

(b) "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using a technology that:

(1) is certified to meet or exceed the level that has been adopted by the Federal Information Processing Standards issued by the **National Institute of Standards and Technology**; and

Md. Tax-General Code § 10-733.1(a)(3)

Tax - General > Title 10. Income Tax. > Subtitle 7. Income Tax Credits. > Purchase of cybersecurity technology and cybersecurity service.

(a)(1)In this section the following words have the meanings indicated.

(2)"Cybersecurity business" means an entity organized for profit that is engaged primarily in the development of innovative and proprietary cybersecurity technology or the provision of cybersecurity service.

(3) "Cybersecurity service" means an activity that is associated with a category or subcategory identified under the Framework Core established by the **National Institute of Standards and Technology's Cybersecurity Framework.**

**Minnesota**

Minn. Stat. § 16E.03

Administration and Finance > Chapter 16E. Office of Enterprise Technology > State Information and Communications Systems.

(g) "Cloud computing" has the meaning described by the **National Institute of Standards and Technology** of the United States Department of Commerce in special publication 800-145, September 2011.

**Nevada**

Nev. Rev. Stat. § 439B.___ [Added by 2021 Nev. SB 40, § 17]

New Sections Added by 2021 Legislation > Added to Title 40. Public Health and Safety.

Sec. 17. If the all-payer claims database is established pursuant to section 9 of this act:

1. The Department shall adopt regulations that prescribe: ….

(b) Require the contractor to: (1) Obtain certification by the HITRUST Alliance or its successor organization and maintain such certification for the term of the contract; (2) Comply with the requirements of subsection 2 of section 11 of this act to the same extent as the Department; and

(3) Comply with any applicable standards prescribed by the **National Institute of Standards and Technology** of the United States Department of Commerce.

Nev. Rev. Stat. § 603A.210(2).

Trade Regulations and Practices. > Chapter 603A. Security and Privacy of Personal Information > Chapter 603A. Security of Information Maintained by Data Collectors and Other Businesses > Chapter 603A. Regulation of Business Practices > Security measures

2. If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the **National Institute of Standards and Technology** of the United States Department of Commerce.

Nev. Rev. Stat. § 603A.215

Title 52. Trade Regulations and Practices. > Chapter 603A. Security and Privacy of Personal Information > Chapter 603A. Security of Information Maintained by Data Collectors and Other Businesses > Chapter 603A. Regulation of Business Practices > Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability

(b) “Encryption” means the protection of data in electronic or optical form, in storage or in transit, using:

(1) An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the **National Institute of Standards and Technology**, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data;

Nev. Rev. Stat. § 701(3)(a). (Statutes of Nevada, Page 2206 (Chapter 368, AB 383)

Energy; Public Utilities and Similar Entities.

3. In establishing standards for appliances pursuant to subsection 1, the Director shall:

(a) Consider the reliability and cybersecurity protocols of the National Institute of Standards and Technology of the United States Department of Commerce, or other cybersecurity protocols that are equally or more protective and adopt, at minimum, the North American Electric Reliability Corporation Critical Infrastructure Protection Standards, as those standards exist on the effective date of this act.

**New Jersey**

N.J. Stat. § 58:31-4.1(a)(1). Title 58. Waters and Water Supply > Chapter 31. Water Quality Accountability Act > Update of cybersecurity program; revision; proof of compliance; audit

3. a. In addition to the requirements of section 4 of P.L.2017, c.133 (C.58:31-4), and the requirements established by the board pursuant thereto, no later than 180 days after the effective date of P.L.2021, c.262 (C.58:31-4.1 et al.), each water purveyor shall update its cybersecurity program developed pursuant to section 4 of P.L.2017, c.133 (C.58:31-4) to apply to all of the public community water system's industrial control systems, and to reasonably conform to the most recent version of one or more of the following industry-recognized cybersecurity frameworks:

(1) the Framework for Improving Critical Infrastructure Cybersecurity developed by the **National Institute of Standards and Technology;**

**Ohio**

ORC § 1354.03

Title 13: Commercial Transactions — Other Commercial Transactions > Chapter 1354: Safe Harbor for Cybersecurity Programs > Reasonably Conforms to industry standard

(A)(1) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to divisions (A)(2) and (D) of this section:

(a) The "framework for improving critical infrastructure cybersecurity" developed by the "**national institute of standards and technology**" (NIST);

**Oklahoma**

62 Okl. St. § 34.32

Title 62. Public Finance > Chapter 1. State Fiscal Affairs > Chapter 1. Oklahoma State Finance Act > Security risk assessment—reports—exceptions

C. A state agency with an information technology system that is not consolidated under the Information Technology Consolidation and Coordination Act or that is otherwise retained by the agency shall additionally be required to have an information security audit conducted by a firm approved by the Information Services Division that is based upon the most current version of the **NIST Cyber-Security Framework**, and shall submit a final report of the information security risk assessment and information security audit findings to the Information Services Division each year on a schedule set by the Information Services Division.

**Texas**

Tex. Gov't Code § 418.192

Government Code > Title 4 Executive Branch > Subtitle B Law Enforcement and Public Protection > Chapter 418 Emergency Management > Subchapter H Miscellaneous Provisions > Communications by Public Service Providers During Disasters and Emergencies.

(d) The dynamic information database must comply with:

(1) the Telecommunications Service Priority program established by the Federal Communications Commission; and

(2) the Federal Information Processing Standard 140-2 governing compliant cryptographic modules for encryption and security issued by the **National Institute of Standards and Technology.**

Tex. Govt. Code § 2054.5181(a)(3)

Government Code > Title 10 General Government > Subtitle B Information and Planning > Chapter 2054 Information Resources [Expires September 1, 2025] > Subchapter N-1 Cybersecurity [Expires September 1, 2025] > Cyberstar Program; Certificate of Approval. [Expires September 1, 2025]

(a) The state cybersecurity coordinator, in collaboration with the cybersecurity council and public and private entities in this state, shall develop best practices for cybersecurity that include: …
(3) consistency with the **National Institute of Standards and Technology** standards for cybersecurity;

Tex. Gov't Code § 2157.007
Government Code > Title 10 General Government > Subtitle D State Purchasing and General Services [Expires September 1, 2027] > Chapter 2157 Purchasing: Purchase of Automated Information Systems [Expires September 1, 2027] > Subchapter A General Provisions [Expires September 1, 2027] > Cloud Computing Service
(1) "Cloud computing service" has the meaning assigned by Special Publication 800-145 issued by the United States Department of Commerce **National Institute of Standards and Technology**, as the definition existed on January 1, 2015.

**Washington**
Rev. Code Wash. § 19.255.005
Title 19 Business Regulations — Miscellaneous > Chapter 19.255 Personal Information — Notice of Security Breaches > Definitions
The definitions in this section apply throughout this chapter unless the context clearly requires otherwise. ….
(3) "Secured" means encrypted in a manner that meets or exceeds the **national institute of standards and technology standard** or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

Rev. Code Wash. § 42.56.590
Title 42 Public Officers and Agencies > Chapter 42.56 Public Records Act > Personal information — Notice of security breaches.
(11) For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the **national institute of standards and technology standard** or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.