NATIONAL CONFERENCE OF STATE LEGISLATURES

7700 EAST FIRST PLACE DENVER, COLORADO 80230
303-364-7700 FAX: 303-364-7800

State Statutes Requiring Reporting of Cybersecurity Incidents

July 14, 2021

Below are excerpts from statutes in six states—Florida, Indiana, New Jersey, North Carolina, Washington and West Virginia—that require government entities to report cybersecurity incidents (typically to the state department of technology or other cybersecurity agency). New Jersey's law requires "water purveyors" to create a cybersecurity incident reporting process, and in North Carolina, private sector entities are *encouraged* to report cybersecurity incidents to the Department of Information Technology.

STATE AND CITATION/LINK	STATUTORY EXCERPT
Florida Fla. Stat. § 282.318	9. Establishing an information technology security incident reporting process that includes procedures and tiered reporting timeframes for notifying the department and the Department of Law Enforcement of information technology security incidents. The tiered reporting timeframes shall be based upon the level of severity of the information technology security incidents being reported.
Indiana Ind. Code § 4-13.1-2-9 Ind. Code § 4-13.1-2-10	A state agency (as defined in IC 4-1-10-2), other than state educational institutions, and a political subdivision (as defined in IC 36-1-2-13) shall: (1) report any cybersecurity incident using their best professional judgment to the office without unreasonable delay and not later than two (2) business days after discovery of the cybersecurity incident in a format prescribed by the chief information officer; and (2) provide the office with the name and contact information of any individual who will act as the primary reporter of a cybersecurity incident described in subdivision (1) before September 1, 2021, and before September 1 of every year thereafter. Nothing in this section shall be construed to require reporting that conflicts with federal privacy laws or is prohibited due to an ongoing law enforcement investigation. A state educational institution (as defined in IC 21-7-13-32) shall: (1) submit a summary analysis report of cyber security incidents to the office on a quarterly basis in a format prescribed by the chief information officer; and (2) provide the office with the name and contact information of any individual who will act as the primary reporter of a summary report of cybersecurity incidents described in subdivision (1) before September 1, 2021, and before September 1 of every year thereafter. Nothing in this section shall be construed to require reporting by the state educational institution that conflicts with federal privacy laws or is prohibited due to an ongoing law enforcement investigation.

New Jersey N.J. Stat. § 58:31-4	a. Within 120 days after the effective date of this act, each water purveyor shall develop a cybersecurity program, in accordance with requirements established by the board, that defines and implements organization accountabilities and responsibilities for cyber risk management activities, and establishes policies, plans, processes, and procedures for identifying and mitigating cyber risk to its public water system. As part of the program, a water purveyor shall conduct risk assessments and implement appropriate controls to mitigate identified risks to the public water system, maintain situational awareness of cyber threats and vulnerabilities to the public water system, and create and exercise incident response and recovery plans. A copy of the program developed pursuant to this subsection shall be provided to the New Jersey Cybersecurity and Communications Integration Cell, established pursuant to Executive Order No. 178 (2015) in the New Jersey Office of Homeland Security and Preparedness. b. Within 60 days after developing the program required pursuant to subsection a. of this section, each water purveyor shall join the New Jersey Cybersecurity and Communications Integration Cell, established pursuant to Executive Order No. 178 (2015), and create a cybersecurity incident reporting process. c. A water purveyor that does not have an internet-connected control system shall be exempt from the requirements of this section.
North Carolina N.C. Gen. Stat. § 143B-1379	(a) The head of each principal department and Council of State agency shall cooperate with the State CIO in the discharge of the State CIO's duties by providing the following information to the Department: (1) The full details of the State agency's information technology and operational requirements and of all the agency's significant cybersecurity incidents within 24 hours of confirmation. (c) County and municipal government agencies shall report cybersecurity incidents to the Department. Information shared as part of this process will be protected from public disclosure under G.S. 132-6.1(c). Private sector entities are encouraged to report cybersecurity incidents to the Department.
Washington Rev. Code Wash. § 43.105.___ (2021 S.B. 5432, Chap. 291 § 3)	(1) In the event of a major cybersecurity incident, as defined in policy established by the office of cybersecurity in accordance with section 1 of this act, state agencies must report that incident to the office of cybersecurity within 24 hours of discovery of the incident. (2) State agencies must provide the office of cybersecurity with contact information for any external parties who may have material information related to the cybersecurity incident. (3) Once a cybersecurity incident is reported to the office of cybersecurity, the office of cybersecurity must investigate the incident to determine the degree of severity and facilitate any necessary incident response measures that need to be taken to protect the enterprise. (4) The chief information security officer or the chief information security officer's designee shall serve as the state's point of contact for all major cybersecurity incidents. (5) The office of cybersecurity must create policy to implement this section.

West Virginia W. Va. Code § 5A-6C-1 to -4	"Incident" or "cybersecurity incident" means a violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices. (a) Qualified cybersecurity incidents shall be reported to the Cybersecurity Office before any citizen notification, but no later than 10 days following a determination that the entity experienced a qualifying cybersecurity incident. (b) A qualified cybersecurity incident meets at least one of the following criteria: (1) State or federal law requires the reporting of the incident to regulatory or law-enforcement agencies or affected citizens; (2) The ability of the entity that experienced the incident to conduct business is substantially affected; or (3) The incident would be classified as emergency, severe, or high by the U.S. Cybersecurity and Infrastructure Security Agency. (c) The report of the cybersecurity incident to the Cybersecurity Office shall contain at a minimum: (1) The approximate date of the incident; (2) The date the incident was discovered; (3) The nature of any data that may have been illegally obtained or accessed; and (4) A list of the state and federal regulatory agencies, self-regulatory bodies, and foreign regulatory agencies to whom the notice has been or will be provided. (d) The procedure for reporting cybersecurity incidents shall be established by the Cybersecurity Office and disseminated to the entities listed §5A-6C-2 of this code. (a) On or before December 31 of each year, and when requested by the Legislature, the Cybersecurity Office shall provide a report to the Joint Committee on Government and Finance containing the number and nature of incidents reported to it during the preceding calendar year.

NCSL contact for additional information: Pam Greenberg, NCSL Denver Office, pam.greenberg@ncsl.org.