N.J. Stat. § 52:17B-193.3

Current through New Jersey 220th Second Annual Session, L. 2023, c. 280 and J.R. 18

LexisNexis® New Jersey Annotated Statutes > Title 52. State Government, Departments and Officers (Subts. 1 — 5) > Subtitle 3. Executive and Administrative Departments (Chs. 14 — 27J) > Chapter 17B. Department of Law and Public Safety (§§ 52:17B-1 — 52:17B-247)

§ 52:17B-193.3. Report, cybersecurity incidents, New Jersey Office of Homeland Security and Preparedness

a. Every public agency and government contractor shall report cybersecurity incidents to the New Jersey Office of Homeland Security and Preparedness. The report shall be made within 72 hours of when the public agency or government contractor reasonably believes that a cybersecurity incident has occurred.

b. The New Jersey Office of Homeland Security and Preparedness shall receive and maintain cybersecurity incident notifications from public agencies, government contractors, and private entities in accordance with this act [C.52:17B-193.2 et seq.].

c. No later than 90 days after the effective date of this act, the Director of the New Jersey Office of Homeland Security and Preparedness shall establish cyber incident reporting capabilities to facilitate submission of timely, secure, and confidential cybersecurity incident notifications from public agencies, government contractors, and private entities to the office.

d. No later than 90 days after the effective date of this act, the New Jersey Office of Homeland Security and Preparedness shall prominently post instructions for submitting cybersecurity incident notifications on its website. The instructions shall include, at a minimum, the types of cybersecurity incidents to be reported and any other information to be included in the notifications made through the established cyber incident reporting system.

e. The cyber incident reporting system shall permit the New Jersey Office of Homeland Security and Preparedness to:

(1) securely accept a cybersecurity incident notification from any individual or private entity, regardless of whether the entity is a public agency or government contractor;

(2) track and identify trends in cybersecurity incidents reported through the cyber incident reporting system; and

(3) produce reports on the types of incidents, indicators, defensive measures, and entities reported through the cyber incident reporting system.

f. Any cybersecurity incident notification submitted to the New Jersey Office of Homeland Security and Preparedness pursuant to P.L.2023, c.19 (C.52:17B-193.2 et seq.) shall be deemed confidential, non-public, and not subject to the provisions of P.L.1963, c.73 (C.47:1A-1 et seq.),

commonly known as the open public records act, as amended and supplemented, may not be discoverable in any civil or criminal action, and may not be subject to subpoena, unless the subpoena is issued by the New Jersey State Legislature and is deemed necessary for the purposes of legislative oversight.

g. Notwithstanding the provisions of subsection f. of this section, the New Jersey Office of Homeland Security and Preparedness may anonymize and share cyber threat indicators and relevant defensive measures to help prevent additional or future attacks and share cybersecurity incident notifications with relevant law enforcement authorities.

h. Information submitted to the New Jersey Office of Homeland Security and Preparedness through the cyber incident reporting system shall be subject to privacy and protection procedures developed and implemented by the office, which shall be based on the comparable privacy protection procedures developed for information received and shared pursuant to the federal Cyber Security Information Sharing Act of 2015 (6 U.S.C. § 1501 et seq.).

History

L. 2023, c. 19, § 2, effective March 13, 2023.

End of Document