

**N.J. Stat. § 52:17B-193.2**

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-193.2. Definitions**

---

As used in this act, P.L.2023, c.19 (C.52:17B-193.2 et seq.):

“Cybersecurity incident” means a malicious or suspicious event occurring on or conducted through a computer network that jeopardizes the integrity, confidentiality, or availability of an information system or the information the system processes, stores, or transmits.

“Cyber threat indicator” means information that is necessary to describe or identify:

- (1) malicious reconnaissance, including, but not limited to, anomalous patterns of communication that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or vulnerability;
- (2) a method of defeating a security control or exploitation of a security vulnerability;
- (3) a security vulnerability, including, but not limited to, anomalous activity that appears to indicate the existence of a security vulnerability;
- (4) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- (5) malicious cyber command and control;
- (6) the actual or potential harm caused by an incident, including but not limited to, a description of the data exfiltrated as a result of a particular cyber threat; and
- (7) any other attribute of a cyber threat, if disclosure of such attribute is not otherwise prohibited by law.

“Defensive measure” means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cyber threat or security vulnerability, but does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the

entity operating the measure, or another entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

“Government contractor” means an individual or entity that performs work for or on behalf of a public agency on a contract basis with access to or hosting of the public agency’s network, systems, applications, or information.

“Information resource” means information and related resources, such as personnel, equipment, funds, and information technology.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Information technology” means any equipment or interconnected system or subsystem of equipment that is used in automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information used by a public agency or a government contractor under contract with a public agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology includes, but is not limited to, computers, ancillary equipment, software, firmware, and similar procedures, services, including support services, and related resources.

“Private entity” means any individual, corporation, company, partnership, firm, association, or other entity, but does not include a public agency as defined in this act, or a foreign government, or any component thereof.

“Public agency” means any public agency of the State or any political subdivision thereof.

## History

---

L. 2023, c. 19, § 1, effective March 13, 2023.