# 6 USCS § 1503

Current through Public Law 118-62, approved May 13, 2024.

*United States Code Service > TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534) > CHAPTER 6. CYBERSECURITY (§§ 1500 — 1534) > CYBERSECURITY INFORMATION SHARING (§§ 1500 — 1510)*

## § 1503. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats

**(a) Authorization for monitoring.**

**(1)** In general. Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

**(A)** an information system of such private entity;

**(B)** an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

**(C)** an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

**(D)** information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

**(2)** Construction. Nothing in this subsection shall be construed—

**(A)** to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title [6 USCS §§ 1501 et seq.]; or

**(B)** to limit otherwise lawful activity.

**(b) Authorization for operation of defensive measures.**

**(1)** In general. Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

**(A)** an information system of such private entity in order to protect the rights or property of the private entity;

**(B)** an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

**(C)** an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

**(2)** Construction. Nothing in this subsection shall be construed—

**(A)** to authorize the use of a defensive measure other than as provided in this subsection; or

**(B)** to limit otherwise lawful activity.

**(c) Authorization for sharing or receiving cyber threat indicators or defensive measures.**

**(1)** In general. Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.

**(2)** Lawful restriction. A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity.

**(3)** Construction. Nothing in this subsection shall be construed—

**(A)** to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

**(B)** to limit otherwise lawful activity.

**(d) Protection and use of information.**

**(1)** Security of information. A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

**(2)** Removal of certain personal information. A non-Federal entity sharing a cyber threat indicator pursuant to this title [6 USCS §§ 1501 et seq.] shall, prior to such sharing—

**(A)** review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

**(B)** implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

**(3)** Use of cyber threat indicators and defensive measures by non-Federal entities.

**(A)** In general. Consistent with this title [6 USCS §§ 1501 et seq.], a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

**(i)** be used by a non-Federal entity to monitor or operate a defensive measure that is applied to—

**(I)** an information system of the non-Federal entity; or

**(II)** an information system of another non-Federal entity or a Federal entity upon the written consent of that other non-Federal entity or that Federal entity; and

**(ii)** be otherwise used, retained, and further shared by a non-Federal entity subject to—

**(I)** an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure; or

**(II)** an otherwise applicable provision of law.

**(B)** Construction. Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

**(4)** Use of cyber threat indicators by State, tribal, or local government.

**(A)** Law enforcement use. A State, tribal, or local government that receives a cyber threat indicator or defensive measure under this title [6 USCS §§ 1501 et seq.] may use such cyber threat indicator or defensive measure for the purposes described in section 105(d)(5)(A) [6 USCS § 1504(d)(5)(A)].

**(B)** Exemption from disclosure. A cyber threat indicator or defensive measure shared by or with a State, tribal, or local government, including a component of a State, tribal, or local government that is a private entity, under this section shall be—

**(i)** deemed voluntarily shared information; and

**(ii)** exempt from disclosure under any provision of State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

**(C)** State, tribal, and local regulatory authority.

**(i)** In general. Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this title [6 USCS §§ 1501 et seq.] shall not be used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any non-Federal entity or any activity taken by a non-Federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

**(ii)** Regulatory authority specifically relating to prevention or mitigation of cybersecurity threats. A cyber threat indicator or defensive measure shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

**(e) Antitrust exemption.**

**(1)** In general. Except as provided in section 108(e) [6 USCS § 1507(e)], it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title [6 USCS §§ 1501 et seq.].

**(2)** Applicability. Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

**(A)** facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

**(B)** communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

**(f) No right or benefit.** The sharing of a cyber threat indicator or defensive measure with a non-Federal entity under this title [6 USCS §§ 1501 et seq.] shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

## History

**HISTORY:**

Dec. 18, 2015, P. L. 114-113, Div N, Title I, § 104, 129 Stat. 2940.