

that is consistent with section 1504(c)(1)(B) of this title and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 1504(a)(1) of this title and guidelines are submitted to Congress under section 1504(b)(1) of this title; or

(B) the date that is 60 days after December 18, 2015.

(c) Construction

Nothing in this subchapter shall be construed—

(1) to create—

(A) a duty to share a cyber threat indicator or defensive measure; or

(B) a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(Pub. L. 114–113, div. N, title I, § 106, Dec. 18, 2015, 129 Stat. 2950.)

§ 1506. Oversight of government activities

(a) Report on implementation

(1) In general

Not later than 1 year after December 18, 2015, the heads of the appropriate Federal entities shall jointly submit to Congress a detailed report concerning the implementation of this subchapter.

(2) Contents

The report required by paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities, policies, procedures, and guidelines under this subchapter and shall include the following:

(A) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 1504(c) of this title, including any impediments to such real-time sharing.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) The number of cyber threat indicators or defensive measures received through the capability and process developed under section 1504(c) of this title.

(D) A list of Federal entities that have received cyber threat indicators or defensive measures under this subchapter.

(b) Biennial report on compliance

(1) In general

Not later than 2 years after December 18, 2015 and not less frequently than once every 2 years thereafter, the inspectors general of the appropriate Federal entities, in consultation with the Inspector General of the Intelligence

Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the actions of the executive branch of the Federal Government to carry out this subchapter during the most recent 2-year period.

(2) Contents

Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this subchapter, including a review of the following:

(i) The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this subchapter, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 1504(c) of this title.

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government¹ entity with the Federal government¹ in contravention of this subchapter, or was shared within the Federal Government in contravention of the guidelines required by this subchapter, including a description of any significant violation of this subchapter.

(iii) The number of times, according to the Attorney General, that information shared under this subchapter was used by a Federal entity to prosecute an offense listed in section 1504(d)(5)(A) of this title.

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive meas-

¹ So in original. Probably should be capitalized.

ures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 1504(b)(3)(E) of this title.

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this subchapter on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.

(3) Recommendations

Each report submitted under this subsection may include such recommendations as the inspectors general may have for improvements or modifications to the authorities and processes under this subchapter.

(c) Independent report on removal of personal information

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this subchapter. Such report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this subchapter in addressing concerns relating to privacy and civil liberties.

(d) Form of reports

Each report required under this section shall be submitted in an unclassified form, but may include a classified annex.

(e) Public availability of reports

The unclassified portions of the reports required under this section shall be made available to the public.

(Pub. L. 114–113, div. N, title I, § 107, Dec. 18, 2015, 129 Stat. 2951.)

§ 1507. Construction and preemption

(a) Otherwise lawful disclosures

Nothing in this subchapter shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government under this subchapter; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this subchapter.

(b) Whistle blower protections

Nothing in this subchapter shall be construed to prohibit or limit the disclosure of informa-

tion protected under section 2302(b)(8) of title 5 (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5 (governing disclosures to Congress), section 1034 of title 10 (governing disclosure to Congress by members of the military), section 3234 of title 50 (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) Protection of sources and methods

Nothing in this subchapter shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) Relationship to other laws

Nothing in this subchapter shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

(e) Prohibited conduct

Nothing in this subchapter shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) Information sharing relationships

Nothing in this subchapter shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any non-Federal entity and a Federal entity or another non-Federal entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 1504(c) of this title.

(g) Preservation of contractual obligations and rights

Nothing in this subchapter shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.