Calendar No. 500

116TH CONGRESS
2d Session

SENATE

REPORT
116–242

CYBERSECURITY VULNERABILITY IDENTIFICATION AND NOTIFICATION ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3045

TO AMEND THE HOMELAND SECURITY ACT OF 2012 TO PROTECT UNITED STATES CRITICAL INFRASTRUCTURE BY ENSURING THAT THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY HAS THE LEGAL TOOLS IT NEEDS TO NOTIFY PRIVATE AND PUBLIC SECTOR ENTITIES PUT AT RISK BY CYBERSECURITY VULNERABILITIES IN THE NETWORKS AND SYSTEMS THAT CONTROL CRITICAL ASSETS OF THE UNITED STATES

JULY 29, 2020.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
99–010 WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
JOSEPH C. FOLIO III, *Chief Counsel*
MICHAEL FLYNN, *Senior Counsel*
DAVID M. WEINBERG, *Minority Staff Director*
ZACHARY I. SCHRAM, *Minority Chief Counsel*
JEFFREY D. ROTHBLUM, *Minority Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 500

116TH CONGRESS *2d Session* | SENATE | REPORT 116–242

CYBERSECURITY VULNERABILITY IDENTIFICATION AND NOTIFICATION ACT

JULY 29, 2020.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 3045]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3045), to amend the Homeland Security Act of 2002 to protect United States critical infrastructure by ensuring that the Cybersecurity and Infrastructure Security Agency has the legal tools it needs to notify private and public sector entities put a risk by cybersecurity vulnerabilities in the networks and systems that control critical assets of the United States, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The purpose of S. 3045, the Cybersecurity Vulnerability Notification Act of 2020, is to authorize the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to issue administrative subpoenas for the purpose of warning U.S. critical infrastructure owners and operators about CISA-

identified potential cybersecurity vulnerabilities. Specifically, the bill authorizes CISA to detect, identify, and receive information about security vulnerabilities related to critical infrastructure for a cybersecurity purpose. The Director of CISA is then authorized to issue an administrative subpoena for the production of information necessary to identify and notify the entity with the specific cybersecurity vulnerability.

Additionally, the bill requires that the Director of CISA coordinate the issuance of a subpoena with the Department of Justice (DOJ), notify any entity identified by the subpoena within seven days, and that the subpoena be authenticated with a digital signature. The bill also requires the Director of CISA to develop procedures to protect nonpublic information from dissemination, absent certain national security or law enforcement interests in resolving a cybersecurity incident related to the vulnerability that gave rise to the subpoena. The bill includes privacy and transparency protections such as provisions for the retention and destruction of information by CISA, the publication of information about the subpoena process, and an annual report to Congress.

II. Background and the Need for Legislation

In December 2019, the National Infrastructure Advisory Council issued a report titled, *Transforming the U.S. Cyber Threat Partnership*, in which it concluded that, "[e]scalating cyber risks to America's critical infrastructure present an existential threat to continuity of the government, economic stability, social order, and national security." [1] This is perhaps most evident by the increase and severity of cyberattacks on our nation's industrial control systems (ICS).[2] Facilitating this increase in threat activity is the use of open source tools that make it easy for nefarious actors to identify and exploit vulnerabilities in these critical infrastructure assets.[3]

Mitigating these cyber vulnerabilities requires that our nation's critical infrastructure owners and operators have access to timely and actionable vulnerability information, some of which may be known to the Federal Government. However, in its March 2020 report, the Cyberspace Solarium Commission found that the Federal Government is often limited in its ability "to systematically identify those who are vulnerable or compromised, notify them, and assist them in mitigating or reducing vulnerability," and recommended that Congress grant certain agencies, including CISA, with administrative subpoena authority to enhance their threat detection and response capabilities.[4]

As the nation's lead civilian cybersecurity agency, CISA is charged with facilitating the sharing of information on cybersecurity vulnerabilities across the nation's critical infrastructure sys-

---

[1] The President's National Infrastructure Advisory Council, *Transforming the U.S. Cyber Threat Partnership*, CISA (Dec. 12, 2019), *available at* https://www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf.

[2] *Global Oil and Gas Cyber Threat Perspective*, Dragos (Aug. 2019), *available at* https://www.dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf?hsCtaTracking=c1b77456-192a-401c-b33b-e972fbd923b5%7C197e055e-bf16-4c14-84ee-e3264e2f5716.

[3] Derek Johnson, *Why CISA Wants Subpoena Authority to Probe Cyber Risks*, FCW Resource Center (Oct. 16, 2019), *available at* https://fcw.com/articles/2019/10/16/cisa-bill-cyber-subpoena.aspx.

[4] U.S. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report* 102 (Mar. 11, 2020), *available at* https://www.solarium.gov/report.

tems and devices. More specifically, in its role as the lead agency for national cybersecurity asset response activities, CISA serves as the primary "interface" for the "real time . . . sharing of information related to cybersecurity risks, incidents, analysis, and warnings" with Federal and non-Federal entities.[5] While CISA often possesses actionable information that could improve the nation's critical systems and assets, the agency is unable to contact at-risk entities due in part to longstanding legal constraints. CISA is generally unable to identify the individual or organization that owns the Internet Protocol (IP) address associated with a potentially vulnerable critical infrastructure device or system. Under the Electronic Communications Privacy Act (ECPA), an Internet Service Provider (ISP)—the company that enables a customer to access the internet via the assigned IP address-is prohibited from disclosing customer information to the Federal Government absent legal process or consent.[6]

CISA has provided examples of multiple instances in which the agency was "delayed, restricted, or altogether foreclosed in responding to known and actionable cyber risks," because of its inability to identify the at-risk entities.[7] Further, CISA informed Congress that information its analysts obtained from Shodan, a publicly available search engine that scans for devices connected to the Internet, identified at least 82,000 ICS devices that were directly accessible via (or from) the Internet at the time the scan was conducted.[8] During a March 2020 Committee hearing titled, *What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity*, CISA Director Christopher Krebs explained how readily accessible tools such as Shodan are used by nefarious actors to identify and exploit vulnerabilities stating that "these automated probes and scans that look for vulnerabilities, and when they see these vulnerabilities they then try a number of techniques to get into the system."[9]

ECPA allows for ISPs to provide customer information to the Federal Government through legal processes, and currently law enforcement agencies can obtain subscriber information with a subpoena if there is a pending investigation.[10] However, there are limits on what information can be shared from pending investigations with other agencies, and the vulnerabilities detected by CISA are not often linked to, and may be of no interest to, pending law enforcement investigations, thereby leaving CISA with little to no ability to fulfil its statutory obligation to identify and respond to cyber threat activity.[11]

S. 3045 provides CISA with the authority to issue administrative subpoenas to ensure that it has the ability to warn critical infrastructure owners and operators about cybersecurity vulnerabilities CISA identifies in critical infrastructure devices and systems.

---

[5] 6 U.S.C. § 659(c)(1),(2); *see also* 6 U.S.C. § 659(c)(5)(B), (7), (9).
[6] 18 U.S.C. § 2703; *see also* 18 U.S.C. § 2703(c)(2).
[7] Cybersecurity and Infrastructure Security Agency classified briefing to the S. Comm. On Homeland Sec. & Gov't Affairs, 116th Cong. (Sept. 17, 2019).
[8] *Id.*
[9] *What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity: Hearing before the Comm. on Homeland Security & Governmental Affairs*, 116th Cong. (2020) (Statement of CISA Director Krebs), *available at* https://www.hsgac.senate.gov/what-states-locals-and-the-business-community-should-know-and-do-a-roadmap-for-effective-cybersecurity.
[10] *Id.*
[11] *Id.*

The Committee recognizes the importance of the privacy and civil liberties protections provided by the ECPA, as well as the concerns inherent when Federal agencies have the authority to compel the disclosure of personally identifiable information. Consistent with those concerns this legislation is limited in scope, includes strict non-dissemination provisions, and robust reporting requirements. As stated by Director Krebs during the March 2020 hearing, such subpoena authority if granted would be used for "purely defensive vulnerability mitigation on critical infrastructure systems, not your average user, not your home device."[12] The narrow scope of the subpoena authority is intended to ensure that the authority cannot be misused by CISA or to advance the interests of other Federal agencies.

S. 3045 limits CISA's ability to disclose any non-public information it obtains as a result of the administrative subpoena with its Federal and non-Federal partners. Similar authorities have been the subject of misuse by other Federal agencies, and as such the authorities granted in this bill are meant to ensure that CISA's compulsory authority is used strictly to enhance the cybersecurity of the nation's critical infrastructure.[13] To ensure that this authority is not used as the basis for law enforcement or regulatory action, S. 3045 requires any entity identified in the subpoena to be notified within seven days. The bill also includes an annual report to Congress specifically requiring detailed information about the security vulnerability that gave rise to the issuance of the subpoena and the effectiveness of the subpoena authority in mitigation the cybersecurity risk.

S. 3045 also makes explicit the voluntary nature of an at-risk entity's engagement with CISA by affirming that responding to the notice from CISA or accepting any services, capabilities, or resources to mitigate the cybersecurity vulnerability are done so voluntarily. Consistent with the principles established in the Cybersecurity Information Sharing Act of 2015, response by an at-risk entity to a notice from CISA about a potential vulnerability remains voluntary. As such, the cybersecurity risk associated with the systems and devices identified by CISA, remains the responsibility of the critical infrastructure owners and operators. The at-risk entity that is identified as a result of the administrative subpoena will receive a notice regarding the cybersecurity vulnerability from CISA, but is not required to take any action thereafter.

Some private sector stakeholders have suggested that rather than seeking the administrative subpoena authority and directly notifying at-risk entities, CISA could disclose the specific vulnerability to the ISP.[14] The ISP could then warn its subscriber (i.e. the at-risk entity) of the identified vulnerability.[15] The challenge with this proposal is that ISPs are among private sector leaders in the provision of cybersecurity services and solutions, and often sell those capabilities to their customers. As a result, when an ISP con-

---

[12] *Id.*

[13] David Kravets, *We Don't Need No Stinking Warrant: The Disturbing, Unchecked Rise of Administrative Subpoena's*, Wired Magazine (Aug. 12, 2008), *available at* https://www.wired.com/2012/08/administrative-subpoenas/.

[14] Greg Nojeim, *Proposed Administrative Subpoena for Cybersecurity Vulnerabilities*, cdt.org blog (Nov. 26, 2019), *available at* https://cdt.org/insights/proposed-administrative-subpoenas-for-cybersecurity-vulnerabilities/?preview=true&_thumbnail_id=85495.

[15] *Id.*

tacts a customer notifying it of a vulnerability, as Director Krebs testified, "it looks like an upsell."[16] As such, at risk-entities may not readily heed warnings coming from the ISP.

S. 3045 does not amend ECPA or expand the scope of the information ISPs may provide the Federal Government under that statute. Rather, this bill grants CISA limited authority to issue an administrative subpoena to obtain specific personal identifiable information about at-risk entities that is restricted under ECPA in fulfilment of CISA's statutory mission. S. 3045 strengthens CISA's cyber threat detection and assets response capabilities by ensuring the nation's critical infrastructure owners and operators have the information needed to mitigate the potentially catastrophe effects of cyber intrusions.

III. Legislative History

Chairman Ron Johnson (R–WI) introduced S. 3045 on December 12, 2019, with Senator Margaret Wood Hassan (D–NH). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 3045 at a business meeting on March 11, 2020. During the business meeting, a substitute amendment was offered by Chairman Johnson and Senator Hassan adding limitations on bulk data collection, liability protections, and emphasizing voluntary engagement by at risk entities, among other things. The amendment was adopted by voice vote *en bloc*. Senators present for the voice vote were Johnson, Portman, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Harris, Sinema and Rosen.

Senator Rand Paul offered an amendment, as modified, adding protections for, and placing limits on, the use of nonpublic information. The amendment was adopted by voice vote *en bloc*. Senators present for the voice vote were Johnson, Portman, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Harris, Sinema and Rosen.

The bill, as amended, was ordered reported favorably by voice vote *en bloc*. The Senators present for the vote were Johnson, Portman, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Harris, Sinema and Rosen.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section provides that the bill may be cited as the "Cybersecurity Vulnerability Identification and Notification Act of 2020."

Section 2. Subpoena authority

Subsection (a) of the bill amends Section 2209 of the Homeland Security Act of 2002 (HSA) by defining "security vulnerability" and establishes subpoena authority following the detection and identification of security vulnerabilities. This subsection also defines

[16] *What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity: Hearing before the Comm. on Homeland Security & Governmental Affairs*, 116th Cong. (2020) (Statement of CISA Director Krebs), *available at* https://www.hsgac.senate.gov/what-states-locals-and-the-business-community-should-know-and-do-a-roadmap-for-effective-cybersecurity.

"covered device or system" as any device or system frequently used in relation to critical infrastructure and stipulates that consumer and personal devices are not included.

Subsection (a) of the bill adds a new subsection (o) at the end of Section 2209 of the HSA that authorizes the Director of CISA to issue a subpoena in the event the Director identifies a specific security vulnerability and has reason to believe that it is related to critical infrastructure, and the subsection describes the limitations on that authority. The subpoena authority extends only to the production of information necessary to identify and notify the at risk entity. Disclosing providers are subject to the liability protections specified in 18 U.S.C. 2703(e).

The CISA Director must coordinate with DOJ and the FBI prior to a subpoena being issued. The subpoena is subject to procedures set forth by the CISA Director and Attorney General. The CISA Director can request enforcement of a subpoena by the Attorney General against any person or entity in the appropriate jurisdiction. The CISA Director must notify any person or entity identified by the subpoena response within seven days following compliance with a subpoena. A cryptographic signature must be applied to any subpoena issued to ensure its validity.

The CISA Director shall establish internal procedures and associated training regarding subpoenas issued under new subsection (o). This includes the protection of and restriction on dissemination of nonpublic information obtained through the use of the subpoena. These restrictions include limits on the use of obtained information and timelines for the the retention and destruction of non-public information obtained. Within one year of the date of enactment, the Privacy Officer of the Agency shall review the procedures developed and notify the Committee on Homeland Security and Governmental Affairs of the Senate and House of Representatives of the results of the review.

The CISA Director must publish information on the website of the agency regarding the subpoena process within 120 days of establishing the internal procedures. The CISA Director must also submit annual reports to the Committee on Homeland Security and Governmental Affairs of the Senate and House of Representatives that include a discussion of subpoenas as a whole and the steps and description of each subpoena issued, and the statute requires a version of the annual report to be made public.

The bill establishes the prohibition on the use of information for unauthorized purposes detailing that any information obtained pursuant to a subpoena will not be provided to any other Federal agency for any purpose other than cybersecurity. Nonpublic information obtained through the use of the subpoena cannot be shared except with Federal entities in the event of a national security or law enforcement interest in resolving a cybersecurity incident related to the vulnerability that gave rise to the subpoena.

Subsection (b)(1) includes a rule of construction stipulating that the authorities granted in this bill do not grant the Secretary of Homeland Security or any other Federal agency the authority to establish new regulations or standards relating to private sector cybersecurity.

Subsection (b)(2) states that private sector entities are not required to request assistance from DHS or if such assistance is re-

quested by a private sector entity, the entity is not required to implement any recommendations made by DHS.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform bill (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, March 30, 2020.

Hon. Ron Johnson,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 3045, the Cybersecurity Vulnerability Identification and Notification Act of 2020.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

Phillip L. Swagel,
Director.

Enclosure.

S. 3045, Cybersecurity Vulnerability Identification and Notification Act of 2020

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 11, 2020

By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	*	*	*
Revenues	*	*	*
Increase or Decrease (-) in the Deficit	*	*	*
Spending Subject to Appropriation (Outlays)	*	*	not estimated

Statutory pay-as-you-go procedures apply?	Yes	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2031?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between -$500,000 and $500,000.

Under current law, the Cybersecurity and Infrastructure Security Agency (CISA) shares information about cyber threats with owners and operators of critical infrastructure (such as power gen-

eration and transmission facilities). In rare instances, the agency cannot do so because it is unable to identify the owners of computers or devices that are vulnerable to malicious activity. S. 3045 would authorize CISA to issue administrative subpoenas in those instances to compel Internet service providers (ISPs) to disclose the identity of owners of such critical infrastructure. The bill also would require CISA to provide annual reports to the Congress on its use of that authority.

ISPs that do not comply with subpoenas could be subject to civil and criminal penalties; therefore, the government might collect additional fines under the legislation. Civil fines are recorded in the budget as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent without further appropriation. CBO expects that few ISPs would be fined for defying subpoenas. Thus, both revenues and direct spending would increase by insignificant amounts over the 2020–2030 period. On net, enacting the bill would reduce the deficit by an insignificant amount, CBO estimates.

On the basis of information from CISA, satisfying the bill's reporting requirements would cost less than $500,000 over the 2020–2025 period; such spending would be subject to the availability of appropriated funds.

On February 24, 2020, CBO transmitted a cost estimate for H.R. 5680, the Cybersecurity Vulnerability Identification and Notification Act of 2020, as ordered reported by the House Committee on Homeland Security on January 29, 2020. The two pieces of legislation are similar and CBO's estimate of their budgetary effects is the same.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 6—DOMESTIC SECURITY

* * * * * * *

CHAPTER 1—HOMELAND SECURITY

* * * * * * *

Subchapter XVIII—Cybersecurity and Infrastructure Security Agency

* * * * * * *

SEC. 659. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—

(1) * * *

* * * * * * *

(5) the term "information system" has the meaning given that term in section 3502(8) of title 44; [and]

(6) the term "security vulnerability" has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 7 U.S.C. 1501(17)); and

[(6)] *(7)* * * *.

(b) * * *

(c) * * *

(1) * * *

* * * * * * *

(10) participating, as appropriate, in national exercises run by the Department; [and]

(11) in coordination with the Emergency Communications Division of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications[.] and

(12) detecting, identifying, and receiving information about security vulnerabilities relating to critical infrastructure in the information systems and devices of Federal and non-Federal entities for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 20 U.S.C. 1501).

* * * * * * *

(o) SUBPOENA AUTHORITY.—

(1) DEFINITION.—In this subsection, the term "covered device or system"—

(A) means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and

(B) does not include personal devices and systems, such as consumer mobile devices, home 9 computers, residential wireless routers, or residential internet enabled consumer devices.

(2) AUTHORITY.—

(A) IN GENERAL.—If the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe that the security vulnerability relates to critical infrastructure and affects a covered device or system owned or operated by a Federal or non-Federal entity, and the Director is unable to identify the entity at risk, the Director may issue a subpoena for the production of information necessary to identify and notify the entity at risk, in order to carry out a function authorized under subsection (c)(12).

(B) LIMIT OF INFORMATION.—A subpoena issued under the authority under subparagraph 2 (A) may seek information—

(i) only in the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18, United States Code; and

(ii) for not more than 20 covered devices or systems.

(C) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—The provisions of section 2703(e) of title 18, United States Code, shall apply to any subpoena issued under the authority under subparagraph (A).

(3) COORDINATION.—

(A) IN GENERAL.—If the Director decides to exercise the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to inter-agency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after the date of enactment of this subsection.

(B) CONTENTS.—The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

(i) issued in order to carry out a function described in subsection (c)(12); and

(ii) subject to the limitations under this subsection.

(4) NONCOMPLIANCE.—If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued under this subsection, the Director may request that the Attorney General seek enforcement of the subpoena in any judicial district in which such person, partnership, corporation, association, or entity resides, is found, or transacts business.

(5) NOTICE.—Not later than 7 days after the date on which the Director receives information obtained through a subpoena issued under this subsection, the Director shall notify any entity identified by information obtained under the subpoena regarding the subpoena and the identified vulnerability.

(6) AUTHENTICATION.—

(A) IN GENERAL.—Any subpoena issued by the Director under this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the recipient of the subpoena to determine that the subpoena was issued by the Agency and has not been altered or modified since it was issued by the Agency.

(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued by the Director under this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of the subpoena.

(7) PROCEDURES.—Not later than 90 days after the date of enactment of this subsection, the Director shall establish internal procedures and associated training, applicable to employees

and operations of the Agency, regarding subpoenas issued under this subsection, which shall address—

(A) the protection of and restriction on dissemination of nonpublic information obtained through a subpoena issued under this subsection, including a requirement that the Agency shall not disseminate nonpublic information obtained through a subpoena issued under this subsection that identifies the party that is subject to the subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information of the entity at risk with another Federal agency if—

(i) the Agency identifies or is notified of a cybersecurity incident involving the entity, which relates to the vulnerability which led to the issuance of the subpoena;

(ii) the Director determines that sharing the nonpublic information with another Federal agency is necessary to allow that Federal agency to take a law enforcement or national security action or actions related to mitigating or otherwise resolving such incident;

(iii) the entity to which the information pertains is notified of the Director's determination, to the extent practicable consistent with national security or law enforcement interests; and

(iv) the entity consents, except that the entity's consent shall not be required if another Federal agency identifies the entity to the Agency in connection with a suspected cybersecurity incident;

(B) the restriction on the use of information obtained through the subpoena for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 6 (6 U.S.C. 1501);

(C) the retention and destruction of non-public information obtained through a subpoena issued under this subsection, including—

(i) destruction of information obtained through the subpoena that the Director determines is unrelated to critical infrastructure immediately upon providing notice to the entity pursuant to paragraph (5); and

(ii) destruction of any personally identifiable information not later than 18 months after the date on which the Director receives information obtained through the subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent;

(D) the processes for providing notice to each party that is subject to the subpoena and each entity identified by information obtained under a subpoena issued under this subsection;

(E) the processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued under this subsection; and

(F) the information to be provided to an entity at risk at the time of the notice of the vulnerability, which shall include—

(i) a discussion or statement that responding to, or subsequent engagement with, the Agency, is voluntary; and

(ii) to the extent practicable, information regarding the process through which the Director identifies security vulnerabilities.

(8) REVIEW OF PROCEDURES.—Not later than 1 year after the date of enactment of this subsection, the Privacy Officer of the Agency shall—

(A) review the procedures developed by the Director under paragraph (7) to ensure that

(i) the procedures are consistent with fair information practices; and

(ii) the operations of the Agency comply with the procedures; and

(B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review.

(9) PUBLICATION OF INFORMATION.—Not later than 120 days after establishing the internal procedures under paragraph (7), the Director shall publish information on the website of the Agency regarding the subpoena process under this subsection, including regarding—

(A) the purpose for subpoenas issued under this subsection;

(B) the subpoena process;

(C) the criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena;

(D) policies and procedures on retention and sharing of data obtained by subpoena;

(E) guidelines on how entities contacted by the Director may respond to notice of a subpoena; and

(F) the procedures and policies of the Agency developed under paragraph (7).

(10) ANNUAL REPORTS.—The Director shall annually submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report (which may include a classified annex but with the presumption of declassification) on the use of subpoenas under this subsection by the Director, which shall include—

(A) a discussion of—

(i) the effectiveness of the use of subpoenas to mitigate critical infrastructure security vulnerabilities;

(ii) the critical infrastructure security risk assessment process conducted for subpoenas issued under this subsection;

(iii) the number of subpoenas issued under this subsection by the Director during the preceding year;

(iv) to the extent practicable, the number of vulnerable covered devices or systems mitigated under this subsection by the Agency during the preceding year; and

(v) the number of entities notified by the Director under this subsection, and their response, during the previous year; and

(B) for each subpoena issued under this subsection—

(i) the source of the security vulnerability detected, identified, or received by the Director;

(ii) the steps taken to identify the entity at risk prior to issuing the subpoena;

(iii) a description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.

(11) PUBLICATION OF THE ANNUAL REPORTS.—The Director shall publish a version of the annual report required by paragraph (10) on the website of the Agency, which shall, at a minimum, include the findings described in clauses (iii), (iv) and (v) of paragraph (10)(A).

(12) PROHIBITION ON USE OF INFORMATION FOR UNAUTHORIZED PURPOSES.—Any information obtained pursuant to a subpoena issued under this subsection shall not be provided to any other Federal agency for any purpose other than a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 3 1501).

○