9110-9P

DEPARTMENT OF HOMELAND SECURITY

Cybersecurity Information Sharing Act of 2015 Final Guidance Documents – Notice of Availability

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice of Availability.

SUMMARY: DHS is announcing the availability of Cybersecurity Information Sharing Act of 2015 (CISA) Final Guidance Documents jointly issued with the Department of Justice (DOJ) in compliance with the Act, which authorizes the voluntary sharing and receiving of cyber threat indicators and defensive measures for cybersecurity purposes, consistent with certain protections, including privacy and civil liberty protections.

ADDRESSES: The CISA final guidance documents may be found on www.us-cert.gov/ais.

FOR FURTHER INFORMATION CONTACT: If you have questions about this notice, email cisaimplementation@hq.dhs.gov or call Matthew Shabat at (703) 235-5338. Questions may also be directed by mail to Matthew Shabat, 245 Murray Lane SW., Mail Stop 0610, Washington, DC 20528-0610.

SUPPLEMENTARY INFORMATION: The CISA requires the Secretary of DHS and the Attorney General to jointly develop and make publicly available—

- guidance to assist non-Federal entities and promote sharing of cyber threat indicators with the Federal Government;
- interim and final guidelines for the protection of privacy and civil liberties; and

- interim and final procedures related to the receipt of cyber threat indicators and defensive measures by the Government, which happen principally through the existing DHS-operated Automated Indicator Sharing (AIS) initiative, web form and email communications to DHS, and through direct submissions to Federal agencies.

Authority and Background

On December 18, 2015, the President signed into law the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, which included at Division N, Title I the Cybersecurity Information Sharing Act of 2015 (CISA). Congress designed CISA to establish a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators and defensive measures while protecting privacy and civil liberties. The CISA requires various Executive Branch agencies to coordinate and create, within 60 days of enactment (i.e., not later than February 16, 2016), four guidance documents to facilitate this voluntary cybersecurity information sharing process. The CISA also requires the final versions of two of these documents to be issued and made publicly available within 180 days of enactment (i.e., not later than June 15, 2016). See generally Pub. L. No. 114-113, Div. N, Title I secs. 103, 105).

Overview of the 180 Day Guidance Required Under CISA

The Cybersecurity Information Sharing Act sec. 105(a)(2) requires the Secretary of DHS and the Attorney General, in consultation with the heads of designated Federal

entities,[1] to jointly develop and issue interim (within 60 days of enactment) and final (within 180 days of enactment) policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government. These internal operational procedures describe general rules applicable to DHS and other Federal agencies and the operative processes of the DHS AIS system, including the statutory requirement for Federal agencies that receive cyber threat indicators and defensive measures to share them with other appropriate agencies. DHS and DOJ updated this guidance.

Section 105(b) of the CISA requires the Secretary of Homeland Security and the Attorney General, in consultation with the Department Heads and Chief Privacy and Civil Liberty Officers of the designated Federal entities and such private entities with industry expertise as the Attorney General and the Secretary consider relevant, to jointly develop and make publicly available interim (within 60 days of enactment) and final (within 180 days of enactment) guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity. These privacy and civil liberties guidelines are consistent with the Fair Information Practice Principles (FIPPs) set forth in Appendix A of the "National Strategy for Trusted Identities in Cyberspace," published by the President in April 2011. DHS and DOJ updated this guidance based on feedback from within the Federal Government, the privacy advocacy community, and other relevant private entities.

---

[1] The CISA defines Appropriate Federal Entities as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence. See CISA sec. 102(3).

Overview of Updates to Non-Federal Entity Sharing Guidelines

Section 105(a)(4) of the CISA requires the Secretary of Homeland Security and the Attorney General to jointly develop and make publicly available guidance to assist non-Federal entities with sharing cyber threat indicators with Federal entities. This guidance includes explanations of how non-Federal entities can identify and share cyber threat indicators and defensive measures with the Federal Government in accordance with CISA and describes the protections non-Federal entities receive under CISA for sharing cyber threat indicators and defensive measures, including targeted liability protection and other statutory protections. As required by CISA, DHS initially made this guidance available on February 16, 2016 at www.us-cert.gov/ais. Based on stakeholder input and feedback, DHS and DOJ have further updated this guidance.

Issuance of Agency Guidance required under CISA

The CISA-mandated final procedures and guidance, as well as an updated version of the non-federal entity sharing guidance, may be found at www.us-cert.gov/ais.

Dated: June 6, 2016.

Andy Ozment,
Assistant Secretary,
Department of Homeland Security.

[FR Doc. 2016-13742 Filed: 6/14/2016 8:45 am; Publication Date: 6/15/2016]