OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

NEWS RELEASE

Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015

(December 2019) The Offices of the Inspectors General (OIGs) for the Departments of Energy, Homeland Security, Justice, Defense, Commerce, Energy, and the Treasury, and the Office of the Director of National Intelligence (ODNI), assessed the implementation of the *Cybersecurity Information Sharing Act of 2015* (CISA) for Calendar Years 2017 and 2018 (Unclassified Report AUD-2019-005-U).[1] The objective of the assessment was to review the actions taken over the prior, most recent, two-year period to carry out the requirements of CISA.

On December 18, 2015, Congress passed Public Law 114-113, the *Consolidated Appropriations Act of 2016*, which includes Title I - the Cybersecurity Information Sharing Act of 2015. CISA was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information. CISA creates a framework to facilitate and promote the voluntary sharing of cyber threat indicators and defensive measures among and between Federal and non-Federal entities.

CISA requires the inspectors general of the "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the ODNI, "in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight," to jointly report to Congress by December 18—every two years—on the actions taken over the most recent two-year period to carry out CISA. This report meets the joint, biennial reporting requirement.

The OIGs determined that sharing of cyber threat indicators and defensive measures has improved over the past two years and efforts are underway to expand accessibility to information. Sharing cyber threat indicators and defensive measures increases the amount of information available for defending systems and networks against cyber attacks. In April 2017, the Intelligence Community Security Coordination Center (IC SCC) deployed a capability to increase sharing of cybersecurity threat intelligence among Federal entities at the top secret security level. According to the Director of the IC SCC, the deployment has enabled cyber analysts to more rapidly share high-quality cyber threat information and has enabled analytic collaboration. Also, in CYs 2017 and 2018, entities continued to share cyber threat information through various reporting means, including email, written reports, and websites. In addition, efforts are underway to further enhance accessibility to cyber threat information and reports. Given the availability of the secret and unclassified government computing clouds, the IC SCC is in the planning and development stages for the deployment of its capability at the secret and unclassified security classification levels. Although progress has been made to improve cyber threat information sharing, using the Automated Indicator Sharing (AIS)—the capability development by the Department of Homeland Security to

[1] A separate, classified report—*Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2019-005)—has been provided to the appropriate Congressional Committees and Federal Entity Officials.

receive cyber threat information from non-governmental entities—remains a challenge. Specifically, the number of non-governmental entities using AIS is minimal, and other challenges with AIS information deter its use.

The report also addressed CISA reporting requirements, including: information sharing policies and procedures, classification of shared information, the timeliness of sharing, and barriers to sharing. The report did not include any recommendations.

The Intelligence Authorization Act for Fiscal Year 2010 established the Office of the Inspector General of the Intelligence Community within the Office of the Director of National Intelligence. The ICIG's mission is to provide independent and objective oversight of the programs and activities within the responsibility and authority of the Director of National Intelligence, to initiate and conduct independent audits, inspections, investigations, and reviews, and to lead and coordinate the efforts of the Intelligence Community Inspectors General Forum. The ICIG's goal is to have a positive and enduring impact throughout the Intelligence Community, to lead and coordinate the efforts of an integrated Intelligence Community Inspectors General Forum, and to enhance the ability of the United States Intelligence Community to meet national security needs while respecting our nation's laws and reflecting its values. The Forum consists of the twelve statutory and administrative Inspectors General having oversight responsibility for an element of the Intelligence Community. The Chair of the Forum is the Inspector General of the Intelligence Community.

For more information about the ICIG, please contact IC_IG_PAO@dni.gov or visit the ICIG's websites:
Secure: https://go.ic.gov/ICIG | Unclassified: https://www.dni.gov/icig
For career opportunities with the ICIG, please visit:
Secure: https://go.ic.gov/ICIGjob | Unclassified: https://www.dni.gov/careers

To report allegations of waste, fraud, or abuse, please contact the ICIG:
Secure: ICIG Hotline 933-2800 | Unclassified: ICIG Hotline 855-731-3260
Secure Email: ICIGHOTLINE@dni.ic.gov | Unclassified Email: ICIGHOTLINE@dni.gov