Statement for the Record

TO: House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection
FROM: The Operational Technology Cybersecurity Coalition (OTCC)
DATE: May 15, 2025
RE: The House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection Hearing Entitled, "In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense" Regarding the Importance of Extending the Cybersecurity Information Sharing Act of 2015 (CISA 2015).

The Operational Technology Cybersecurity Coalition, a dedicated group of cybersecurity vendors committed to safeguarding our nation's critical infrastructure, writes to urge the reauthorization of the Cybersecurity Information Sharing Act of 2015 (CISA 2015).

Since its enactment following the Office of Personnel (OPM) data breach, CISA 2015 has provided a vital framework for voluntary public-private cyber threat information sharing, thereby strengthening our collective national cyber defenses. On November 12, 2024, your full House Committee on Homeland Security released a cyber threat snapshot that detailed a 30% increase in cyberattacks targeting critical infrastructure since 2023. The report also cited the Cybersecurity and Information Security Agency's findings that ransomware reports across all sectors increased over 70% from 2022 to 2023. The escalating sophistication of cyber threats, underscored by recent attacks on critical infrastructure including Volt Typhoon and Salt Typhoon, and on federal agencies in incidents like SolarWinds, Storm 0558, and MOVEit, highlight the persistent and critical need for this legislation.

CISA 2015 has successfully facilitated collaboration by providing legal protections, including antitrust exemptions, necessary for companies to confidently share threat indicators and defensive measures with both governmental partners and other private entities. This collaborative environment has demonstrably improved the speed and capacity with which our nation can respond to large-scale cyber incidents such as the Log4j JNDI attack and the CrowdStrike/Microsoft incident of 2024. In 2022, the latest year for which there is published data, 413,834 cyber threat indicators were shared with the

Cybersecurity and Information Security Agency. For operational technology assets of critical infrastructure, this speed is essential to effectively mitigate cyberattacks, which is the core mission of our Coalition.

We firmly believe that a lapse in the CISA 2015 framework would inevitably and immediately reduce the crucial flow of information, leaving the United States—civilian, military, commercial, et al—more vulnerable to the malicious activities of nation-state actors and cybercriminals. These established communication channels are essential for maintaining situational awareness and enabling rapid, effective responses to security incidents which are crucial to protecting operational technology. Furthermore, the provisions of CISA 2015 are foundational to other significant cyber laws, including the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), making its reauthorization essential for the stability of our broader cybersecurity legislative landscape.

The Operational Technology Cybersecurity Coalition champions an open, vendor-neutral approach to cybersecurity, a principle that is bolstered by voluntary information sharing frameworks like the one established by CISA 2015. Echoing our formal communication sent to Congress on March 21, 2025, we reiterate the urgent call for the extension of the Cybersecurity Information Sharing Act of 2015. Preserving this framework is paramount to maintaining and enhancing the crucial information sharing capabilities that protect our nation's critical infrastructure and ensure our national security against ever-evolving cyber threats.

We thank the Subcommittee for your leadership on this important matter and remain committed to working alongside you.

Sincerely,

The Operational Technology Cybersecurity Coalition