CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

JCDC INTERNATIONAL

International Best Practices

Dr. Patricia Soler
Section Chief, JCDC International

Meet the Mission

The Joint Cyber Defense Collaborative (JCDC) International works with **Computer Emergency Readiness Team (CERT)** counterparts worldwide to **bilaterally and multilaterally exchange actionable information** to increase and enhance the security of the cyber ecosystem.

JCDC International **shares unique products** with operations counterparts overseas and aims to increase the number of trusted international parts to:

- **Encourage bilateral sharing of information useful to CISA's mission**
- **Foster good intentions internationally through sharing of actionable information**
- **Increase CISA and JCDC's brand awareness**

Core Responsibilities

JCDC International is **unique in its ability to share operational information** with key CERT counterparts to allow **proactive prevention** of and **rapid reaction** to cyber incidents.

Product Sharing

Ensuring CISA's partners are aware of any major releases from CISA, including occasional pre-releases or TLP:RED information.

Victim Notification

Leveraging information from industry partners and interagency to notify international partners if their constituents may have been affected by cyber incidents.

CERT Engagement

Engaging with international partners, in cooperation with other CISA partners, to share best practices with developing CERTs.

Technical Inputs

Reviewing relevant technical inputs to CISA products or taskers, to ensure correct adjudication of technical comments.

Patricia Soler
November 17, 2022

What JCDC Does

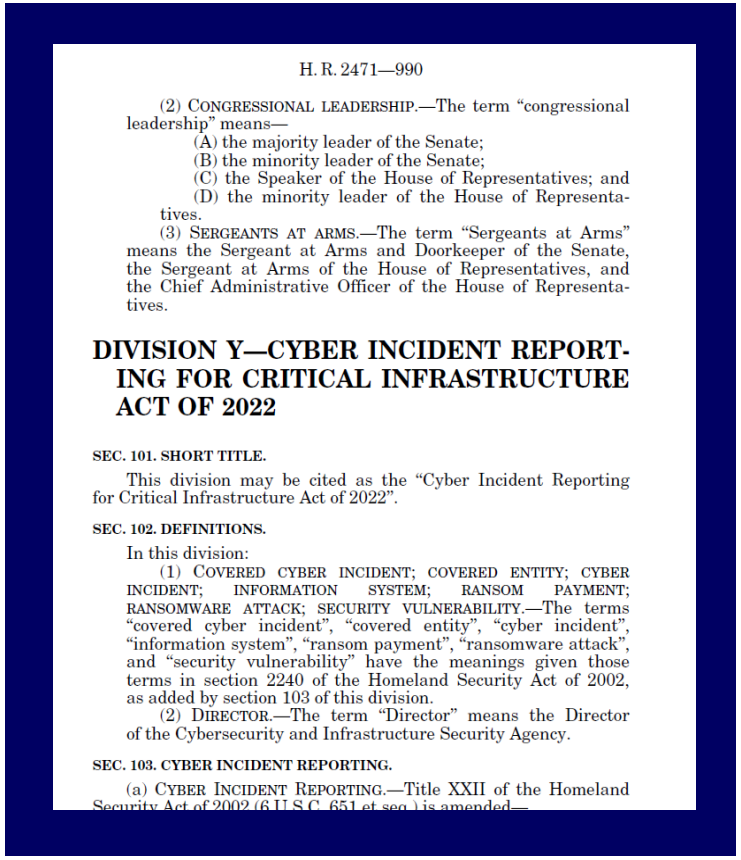
The Joint Cyber Defense Collaborative (JCDC) **leads collaborative, public-private sector cyber defense planning,** cybersecurity **information fusion**, and the purposeful **dissemination of cyber defense** guidance in order to **reduce risk** to National Critical Functions.

Core Functions:

- Coordinate **operational planning** and execution
- Drive collaborative public-private sector cybersecurity **information fusion** that benefits the broader ecosystem
- Produce and disseminate **cyber defense guidance** across all stakeholder communities

Patricia Soler
November 17, 2022

CIRCIA Overview



H. R. 2471—990

(2) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" means—
(A) the majority leader of the Senate;
(B) the minority leader of the Senate;
(C) the Speaker of the House of Representatives; and
(D) the minority leader of the House of Representatives.
(3) SERGEANTS AT ARMS.—The term "Sergeants at Arms" means the Sergeant at Arms and Doorkeeper of the Senate, the Sergeant at Arms of the House of Representatives, and the Chief Administrative Officer of the House of Representatives.

DIVISION Y—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

SEC. 101. SHORT TITLE.

This division may be cited as the "Cyber Incident Reporting for Critical Infrastructure Act of 2022".

SEC. 102. DEFINITIONS.

In this division:
(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms "covered cyber incident", "covered entity", "cyber incident", "information system", "ransom payment", "ransomware attack", and "security vulnerability" have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 103 of this division.
(2) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

SEC. 103. CYBER INCIDENT REPORTING.

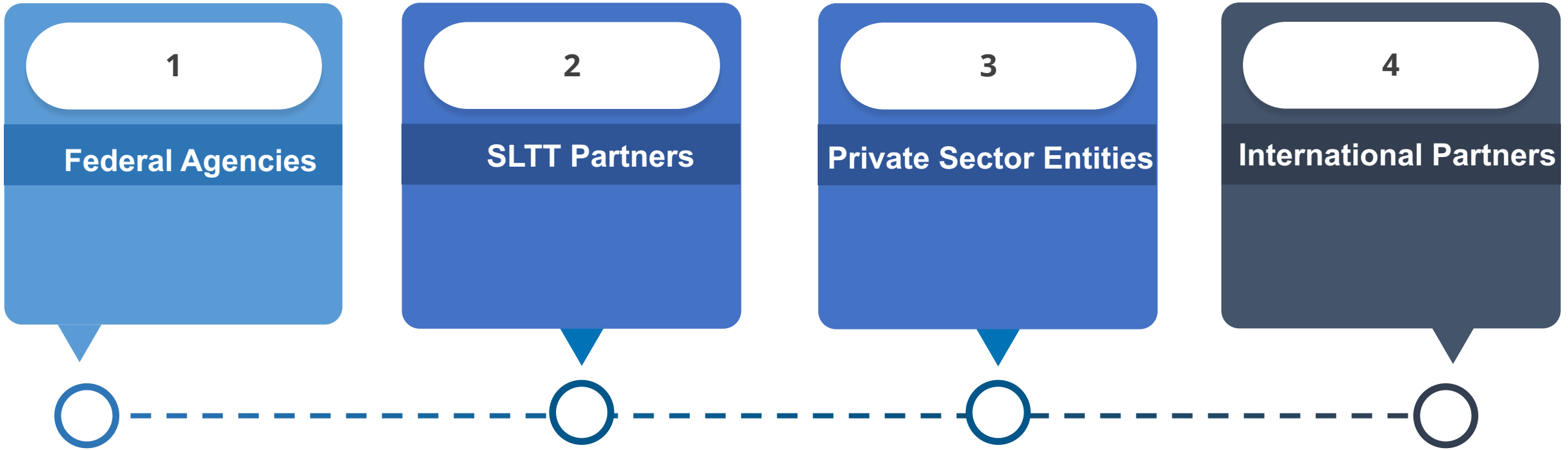
(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

- In March 2022, Congress enacted the ***Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)***
- Requires the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate with Federal partners and others on various cyber-incident reporting and ransomware-related activities
- Requires CISA to establish a new regulatory program requiring reporting of certain cybersecurity-related items
- Allow CISA to better understand the threats we are facing, to spot adversary campaigns earlier, and to take more coordinated action with our public and private sector partners in response.

Patricia Soler
November 17, 2022

JCDC Partners

CISA will promote national resilience by coordinating actions across:



JCDC will identify, protect against, detect, plan for and respond to malicious cyber activity targeting U.S. critical infrastructure

JCDC Partners Continued

JCDC works with Alliance Partners, industry partners who are **fully integrated into JCDC's cyber defense planning and operations** and have committed personnel, tools, or other resources on an ongoing basis and regularly collaborate with all JCDC entities.

JCDC Alliance Partners include:

- Akamai Technologies, Inc.
- AT&T Services, Inc.
- Broadcom, Inc. (formerly, Symantec Corporation)
- CISCO Systems, Inc.
- CloudFlare, Inc.
- CrowdStrike Inc. (CrowdStrike Services, Inc.)
- Google Cloud
- International Business Machines Corporation (IMB)
- Juniper Networks (US), Inc.
- Lumen Technologies, Inc (formerly known as CenturyLink)
- Mandiant
- Microsoft
- Oracle America Inc.
- Palo Alto Networks, Inc.
- SecureWorks, Inc.
- Splunk, Inc.
- Tenable Public Sector LLC.
- Trelix
- Verizon Communications, Inc.
- VMware, Inc.

JCDC Interagency Partners

DHS

DoD

DoJ

ODNI

NSA

FBI

Working Together

Should potential US victims be found during a forensic investigations in your country - please share the details with CISA for notification to the entity.

Submission of advanced malware or malware used by sophisticated actors to https://www.malware.us-cert.gov/

Disclosure of vulnerabilities that may have an impact on US interests

Tips of malicious State-Sponsored infrastructure located in the United States.

Sharing cyber threats and/or impacts to Federal agencies by advanced persistent threats.

Threat information related to Russian, Chinese, Iranian, North Korean, or other sophisticated State-Sponsored actor sets.

Reporting related to impacts to critical infrastructure and industrial control systems. Specifically, if there are threats or potential impacts to the energy sector, aviation, and/or water assets.

For more information:
www.cisa.gov

Questions?
Email: CyberLiaison_intl@cisa.dhs.gov

Patricia Soler
November 17, 2022