CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

EMERGENCY COMMUNICATIONS COORDINATOR REPORT FEBRUARY 2025

Chris Maiers
February 13, 2025

Compromised Critical Infrastructure Advisory

- CISA, NSA and FBI assess that People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on critical IT networks.
  - Disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.
- New cybersecurity advisory outlines threat and targeted systems such as communications and utilities.
  - Outlines tactics and techniques
  - Includes incident response recommendations and options for reporting.

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

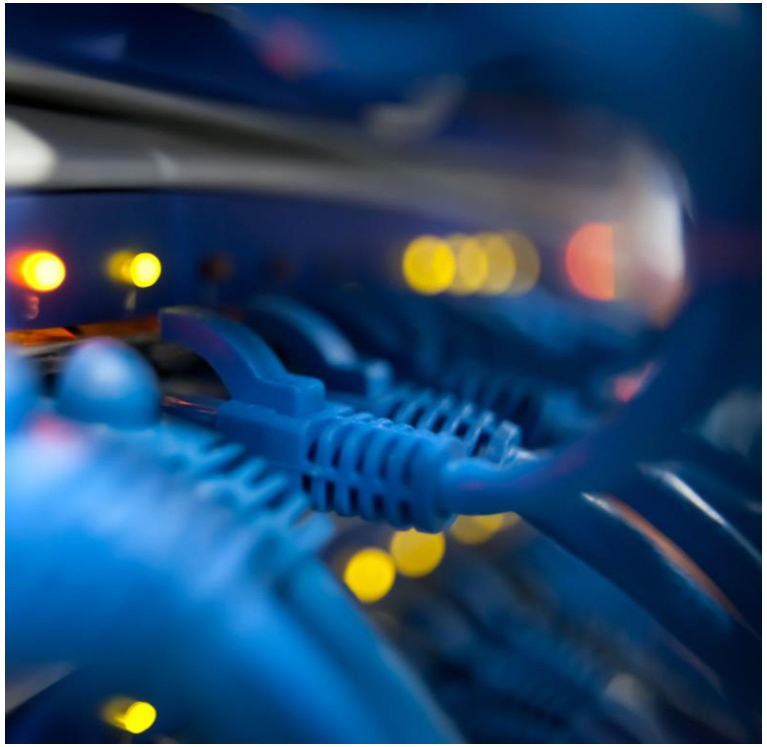
This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Guidance & Strategy to Protect Edge Devices

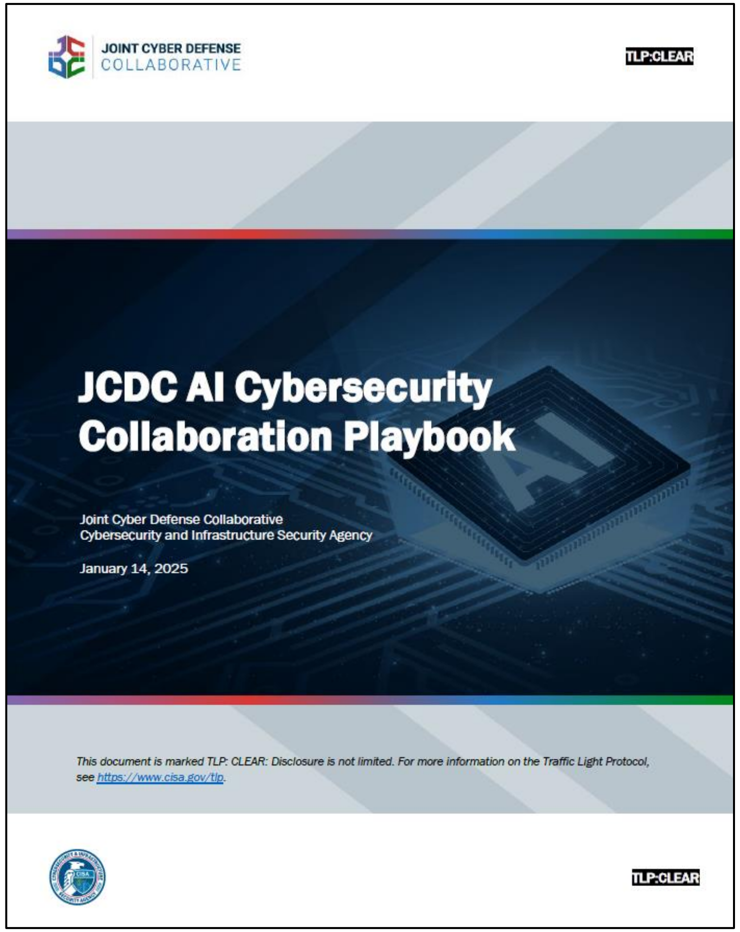
- Collection of guidance from worldwide cybersecurity authorities to protect network edge devices:
  - Firewalls, routers, VPN gateways, IoT devices, servers and other OT devices.
- Four documents:
  - *Security Considerations for Edge Devices*
  - *Digital Forensics Monitoring Specifications for Products of Network Devices and Applications*
  - *Mitigation Strategies for Edge Devices: Executive Guidance*
  - *Mitigation Strategies for Edge Devices: Practitioner Guidance*
- Aligns with Secure by Design concepts.



https://www.cisa.gov/resources-tools/resources/guidance-and-strategies-protect-network-edge-devices

AI Cybersecurity Collaboration Playbook

- Published on January 10, 2025 by Joint Cyber Defense Collaborative (JCDC).
- Guidance to organizations across the AI community (providers, developers, and adopters) for voluntarily sharing AI-related cybersecurity information with CISA and JCDC.
  - Facilitate collaboration among federal agencies, private industry, international partners, and other stakeholders to raise awareness of AI cybersecurity risks and improve the resilience of AI systems.
  - Guide JCDC partners on how to voluntarily share cybersecurity incident information & vulnerabilities associated with AI systems.
  - Delineate information sharing protections and mechanisms.
  - Outline CISA's actions upon receiving shared information to strengthen collective defense.



JOINT CYBER DEFENSE COLLABORATIVE

TLP:CLEAR

JCDC AI Cybersecurity Collaboration Playbook

Joint Cyber Defense Collaborative
Cybersecurity and Infrastructure Security Agency

January 14, 2025

This document is marked TLP: CLEAR: Disclosure is not limited. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

TLP:CLEAR

https://www.cisa.gov/resources-tools/resources/ai-cybersecurity-collaboration-playbook

Secure by Demand: Information & Guidance

- *Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products* released on January 13, 2025.
  - Warns that cyber threat actors target particular operational technology (OT) products rather than specific organizations.
  - Commonly have weaknesses to include weak authentication, known software vulnerabilities, limited logging, insecure default settings and passwords, and insecure legacy protocols.
- Encourages implementation of 12 key security elements into procurement processes when purchasing industrial automation and control systems and other OT products.

Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
European Commission
Bundesamt für Sicherheit in der Informationstechnik
National Cyber Security Centre
Ministry of Security and Justice
Te Tira Tiaki
Government Communications Security Bureau
National Cyber Security Centre
PART OF THE GCSB
National Cyber Security Centre
a part of GCHQ
JOINT CYBER DEFENSE COLLABORATIVE

TLP:CLEAR

Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products

January 13, 2025

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
U.S. Environmental Protection Agency
U.S. Transportation Security Administration
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
Directorate General for Communications Networks, Content and Technology, European Commission
Germany's Federal Office for Information Security
Netherlands' National Cyber Security Centre
New Zealand's National Cyber Security Centre
United Kingdom's National Cyber Security Centre

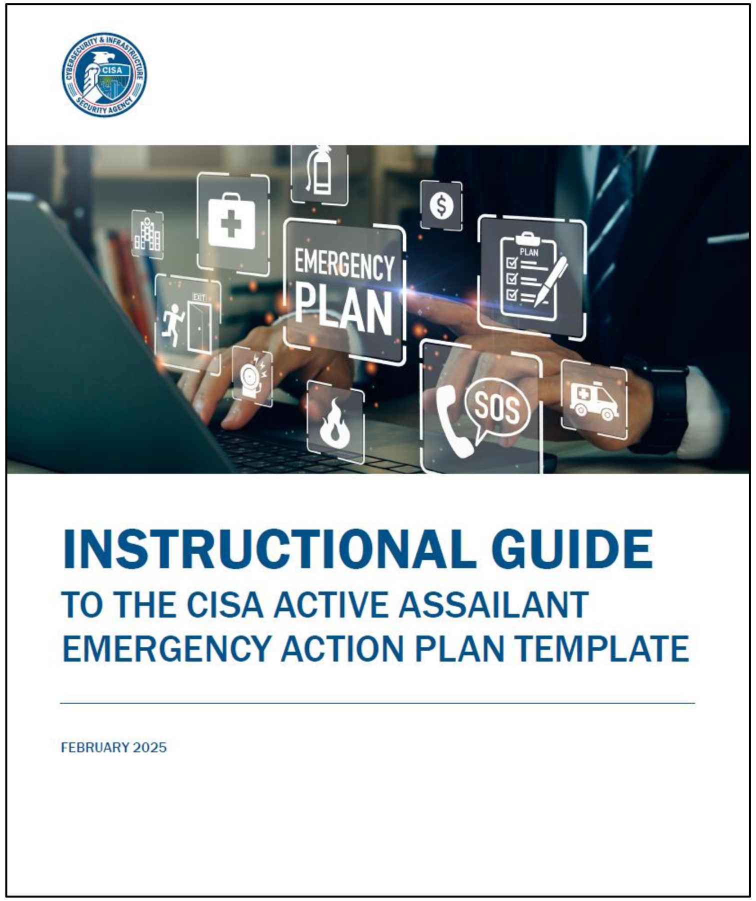
This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

https://www.cisa.gov/resources-tools/resources/secure-demand-priority-considerations-operational-technology-owners-and-operators-when-selecting

Active Assailant Emergency Action Plan (EAP)

- The *Active Assailant Emergency Action Plan Template* and companion *Instructional Guide to the CISA EAP Template*:
- Provide organizations and venue operators with tangible guidance to assist users with developing a comprehensive and implementable EAP that includes:
  - Fillable and tailorable template and guidance to assist users with developing an implementable EAP.
  - Comprehensive options for considerations and tangible examples of various EAP elements.
  - Numerous other applicable resources aligned to each section of the EAP template.



INSTRUCTIONAL GUIDE

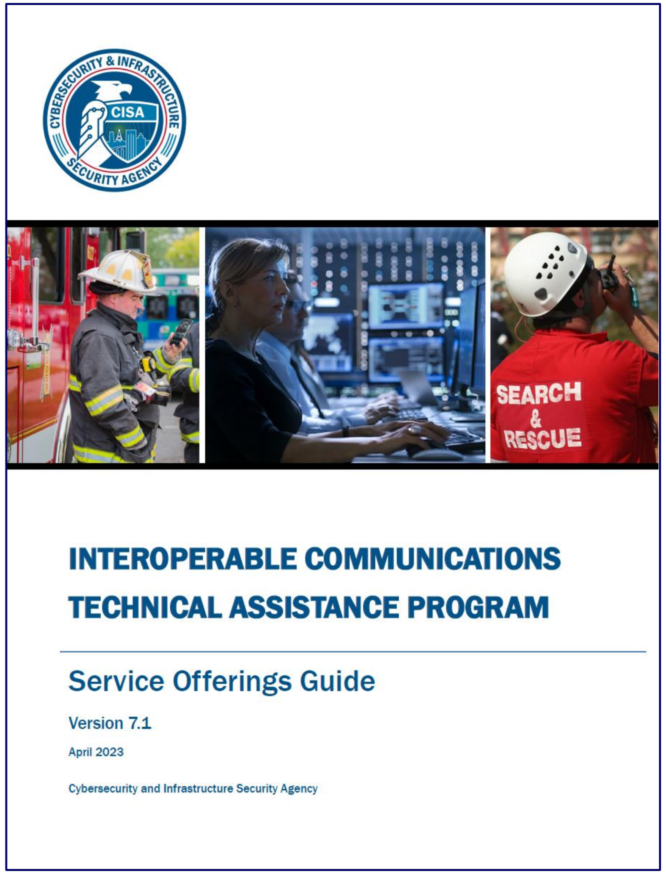
TO THE CISA ACTIVE ASSAILANT EMERGENCY ACTION PLAN TEMPLATE

FEBRUARY 2025

https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite

Technical Assistance

- Submission Update Status:
  - Priority #2 – #5 TA requests from October 2024 will generally not be awarded in the October 2024 to April 2025 period.
- Next Technical Assistance Submission Period
  - New submissions accepted April 1 – April 30
  - If no new submissions received, October 2024 list will be used.
  - Previous #2 request will be assumed to be main priority.
  - Previous guidance on state-sponsored, regional, and special event TA requests still stands.



INTEROPERABLE COMMUNICATIONS TECHNICAL ASSISTANCE PROGRAM

Service Offerings Guide

Version 7.1

April 2023

Cybersecurity and Infrastructure Security Agency

https://www.cisa.gov/safecom/ictapscip-resources

Regional News of Note

- Scheduled Technical Assistance –
  - Missouri:
    - INTD – March 11-14 in Bethany.
    - INCM – March 18-20 in Bethany.
  - Kansas City Metro:
    - COMT – March 3-7 in Lee’s Summit
  - More announcements coming soon.
- Next Technical Assistance Submission Period April 1-30
  - If no new submissions received, Oct. 2024 list will be used.
  - Previous guidance on state-sponsored, regional, and special event TA requests still stands.
- Multi-Region RECCWG Plenary on April 15-17 in Jonesboro, AR.

For more information:

Chris Maiers
Christopher.Maiers@cisa.dhs.gov
202-701-3235