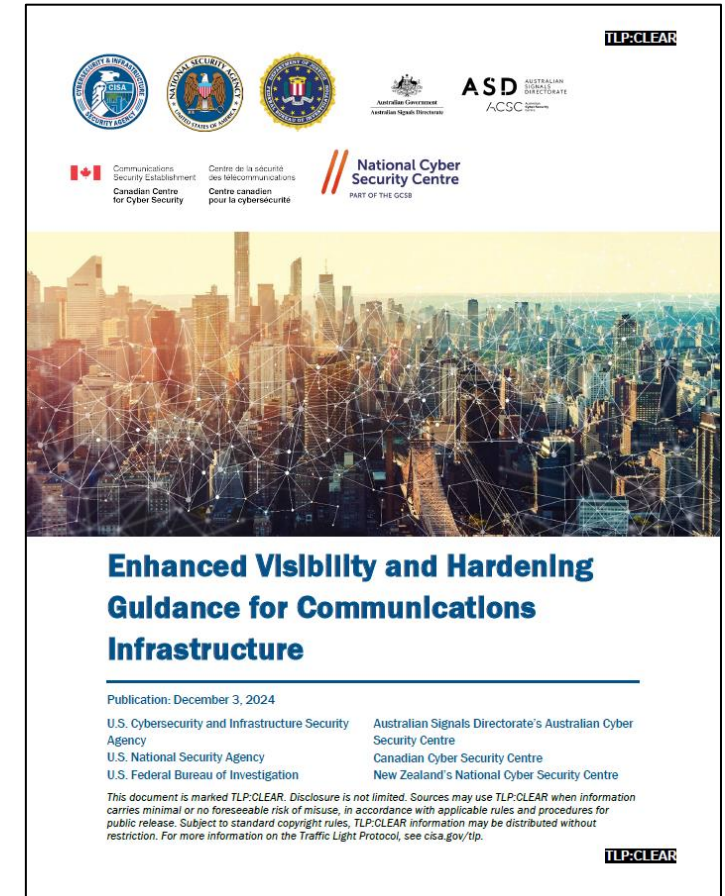# After-Action on LMR Ransomware Intrusion

- Public safety trunked land mobile radio system suffered a ransomware intrusion in 2024 that included a ransomware deployment on their radio system cores.
  - Affected primary and backup core sites.

- Key Lessons from Response:
  - How the county coordinated with partners:
    - Local agencies, state, vendors, and federal agencies.
  - Steps the county took to facilitate recovery in under ten (10) days.
  - How to assess network for additional vulnerabilities.
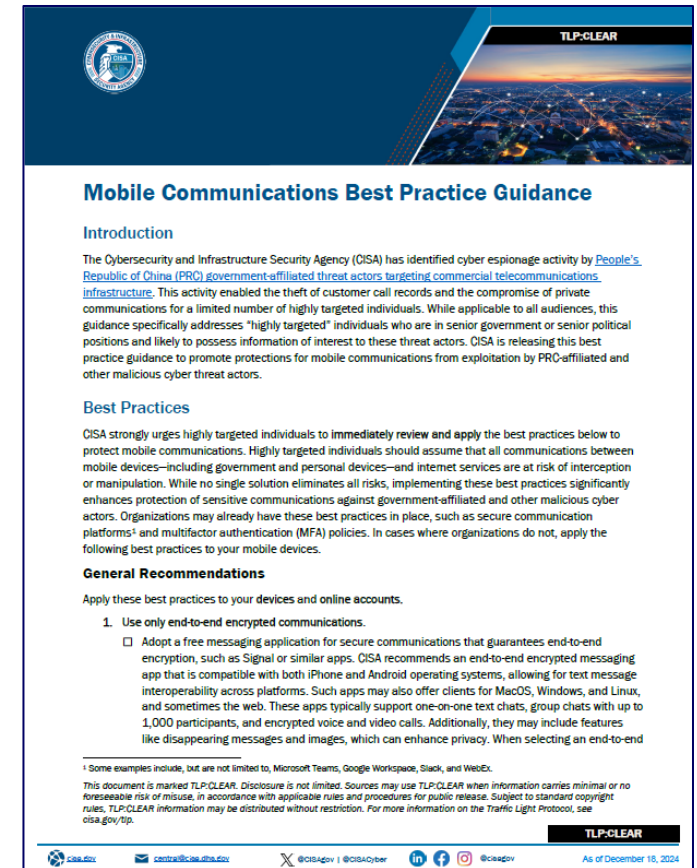 - Potential avenues for improvement.

Guide to Protect Comms Infrastructure

- Provides best practices to protect against a People's Republic of China (PRC)-affiliated threat actor that has compromised networks of major global telecommunications providers.
  - Recommended actions to quickly identify anomalous behavior, vulnerabilities and threats and to respond to a cyber incident.
  - Information to reduce existing vulnerabilities, improve secure configuration habits, and limit potential entry points.

- https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

- https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

Enhanced Visibility and Hardening Guidance for Communications Infrastructure

Publication: December 3, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation

Australian Signals Directorate's Australian Cyber Security Centre
Canadian Cyber Security Centre
New Zealand'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.

Mobile Comms Best Practice Guidance

- Mobile communications practices to protect against exploitation by PRC-affiliated and other cyber threat actors.

- PRC actors identified in cyber espionage activity targeting commercial telecommunications infrastructure.

- Outlines "highly targeted" individuals who likely possess information of interest.

- Customer call records theft and private comms compromise.

- Several best practices for personnel included updated multifactor authentication and VPN suggestions.

- https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance

Mobile Communications Best Practice Guidance

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) has identified cyber espionage activity by People's Republic of China (PRC) government-affiliated threat actors targeting commercial telecommunications infrastructure. This activity enabled the theft of customer call records and the compromise of private communications for a limited number of highly targeted individuals. While applicable to all audiences, this guidance specifically addresses "highly targeted" individuals who are in senior government or senior political positions and likely to possess information of interest to these threat actors. CISA is releasing this best practice guidance to promote protections for mobile communications from exploitation by PRC-affiliated and other malicious cyber threat actors.

Best Practices

CISA strongly urges highly targeted individuals to immediately review and apply the best practices below to protect mobile communications. Highly targeted individuals should assume that all communications between mobile devices—including government and personal devices—and internet services are at risk of interception or manipulation. While no single solution eliminates all risks, implementing these best practices significantly enhances protection of sensitive communications against government-affiliated and other malicious cyber actors. Organizations may already have these best practices in place, such as secure communication platforms[1] and multifactor authentication (MFA) policies. In cases where organizations do not, apply the following best practices to your mobile devices.

General Recommendations

Apply these best practices to your devices and online accounts.

1. Use only end-to-end encrypted communications.
   - Adopt a free messaging application for secure communications that guarantees end-to-end encryption, such as Signal or similar apps. CISA recommends an end-to-end encrypted messaging app that is compatible with both iPhone and Android operating systems, allowing for text message interoperability across platforms. Such apps may also offer clients for MacOS, Windows, and Linux, and sometimes the web. These apps typically support one-on-one text chats, group chats with up to 1,000 participants, and encrypted voice and video calls. Additionally, they may include features like disappearing messages and images, which can enhance privacy. When selecting an end-to-end

[1] Some examples include, but are not limited to, Microsoft Teams, Google Workspace, Slack, and WebEx.

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.

Chris Maiers
January 9, 2025

4

Expanded Cyber Resilient 911 Offerings

- CR911 Offerings Include:
  - 9-1-1/PSAP Cyber Awareness Webinar (CYB-AWR911PSAP)
    - General overview & advanced operations & administration
  - LMR Cyber Awareness Webinar
  - One-Day Cyber Awareness Workshop
  - Two-Day Threat Assessment and Response Workshop
  - Full Cyber Assessment
  - Rapid Cyber Assessment
  - Post Assessment Workshop
  - Post Cyber Incident AAR
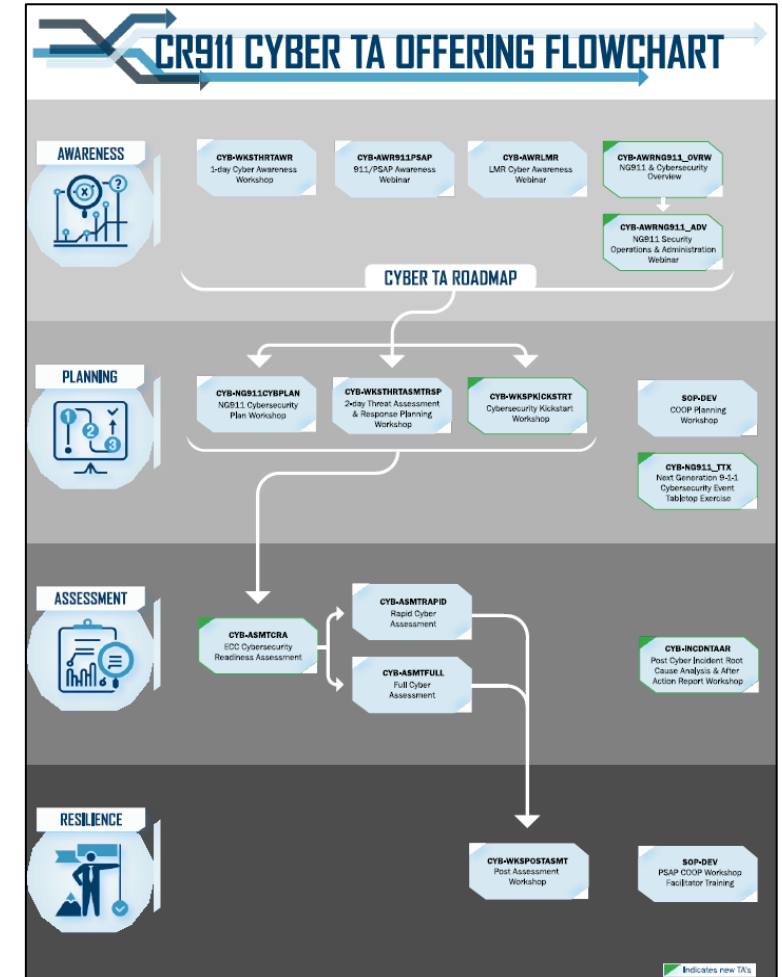
Regional News of Note

- Technical Assistance Update –
  - Scoping calls are taking place.
  - Course announcements will sent out soon by stakeholders.
  - Other regional areas that have submitted:
    - Kansas City – FIFA 2026 Planning and Training endorsed by Kansas and Missouri SWICs
    - FIFA-related trainings in Kansas City will be open for regional attendance.

For more information:

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