EMERGENCY COMMUNICATIONS COORDINATOR REPORT JULY 2025

Chris Maiers
July 10, 2025

Maintain Vigilance

New DHS NTAS Bulletin followed by co-sealed fact sheet urging vigilance for cyber threats related to foreign activity.

- Iranian-affiliated cyber actors, other state-sponsored actors and hacktivist groups may still conduct malicious cyber activity.
- Exploit unpatched or outdated software or the use of default or common passwords on internet-connected accounts and devices.

Mitigations recommended in the joint Fact Sheet:

- Identifying and disconnecting operational technology and industrial control systems devices from the public internet;
- Protecting devices and accounts with strong, unique password;
- Applying the latest software patches;
- Implementing phishing-resistant multifactor authentication for access to OT networks.

NTAS Bulletin: https://go.dhs.gov/wF4

Joint Fact Sheet: https://go.dhs.gov/wjJ

TLP:CLEAR

Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the Department of Defense Cyber Crime Center (DC3), and the National Security Agency (NSA) (hereafter referred to as the authoring agencies) strongly urge organizations to remain vigilant for potential targeted cyber activity against U.S. critical infrastructure and other U.S. entities by Iranian-affiliated cyber actors. Despite a declared ceasefire and ongoing negotiations towards a permanent solution, Iranian-affiliated cyber actors and hacktivist groups may still conduct malicious cyber activity. The authoring agencies are continuing to monitor the situation and will release pertinent cyber threat and cyber defense information as it becomes available.

Threat Activity

Based on the current geopolitical environment, Iranian-affiliated cyber actors may target U.S. devices and networks for near-term cyber operations. Defense Industrial Base (DIB) companies, particularly those possessing holdings or relationships with Israeli research and defense firms, are at increased risk. Hacktivists and Iranian-government-affiliated actors routinely target poorly secured U.S. networks and internet-connected devices for disruptive cyberattacks.

Iranian-affiliated cyber actors and aligned hacktivist groups often exploit targets of opportunity based on the use of unpatched or outdated software with known Common Vulnerabilities and Exposures (CVEs) or the use of default or common passwords on internet-connected accounts and devices. (**Note:** See CISA's Known Exploited Vulnerabilities Catalog for more information on vulnerabilities that have been exploited in the wild). These malicious cyber actors commonly use techniques such as automated password guessing, cracking password hashes using online resources, and inputting default manufacturer passwords. When specifically targeting operational technology (OT), these malicious cyber actors also use system engineering and diagnostic tools to target entities such as engineering and operator devices, performance and security systems, and vendor and third-party maintenance and monitoring systems.

Over the past several months, Iranian-aligned hacktivists have increasingly conducted website defacements and leaks of sensitive information exfiltrated from victims. These hacktivists are likely to significantly increase distributed denial of service (DDoS) campaigns against U.S. and Israeli websites due to recent events.

Iranian-affiliated cyber actors may also conduct ransomware attacks in collaboration with other cybercriminal groups. These actors have been observed working directly with ransomware affiliates to conduct encryption operations, as well as steal sensitive information from these networks and leaking it online.

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

cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of June 30, 2025

Emergency Communications System Lifecycle

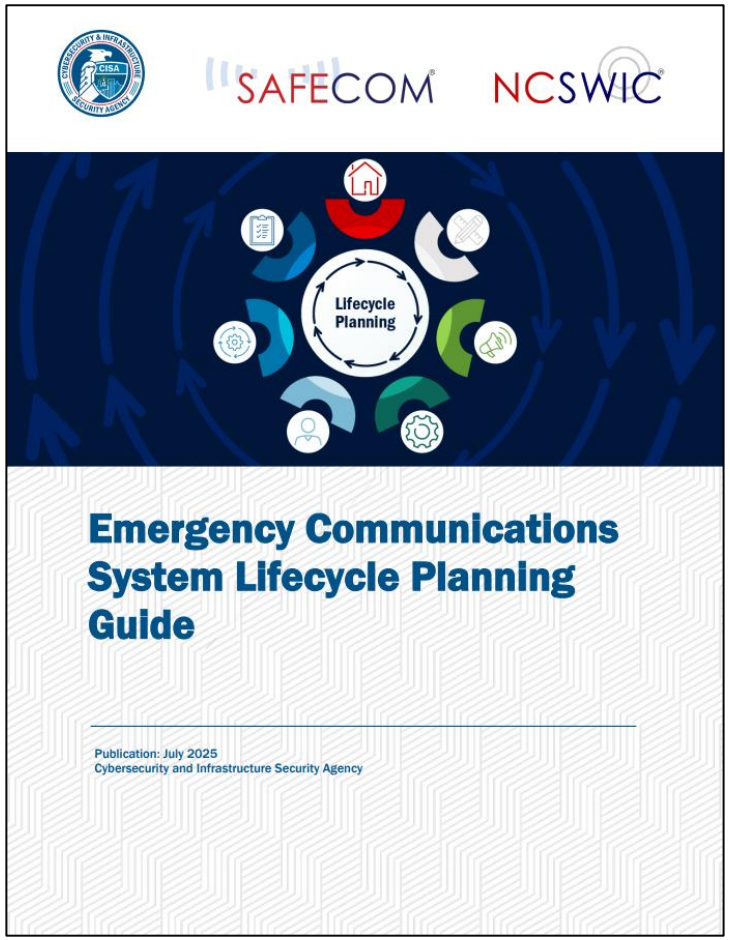
Updated Lifecycle Planning Guide

- Supersedes 2018 revision.
- Discusses actions related to building, maintaining, replacement & decommissioning emergency communications systems.
  - Pre-planning, Project Planning, Requests for Proposals an Acquisition, Implementation, Support/Maintenance/Sustainment, End-of-Lifecycle Assessment and Replacement, and Disposition.

Life Cycle Planning Tool

- Complements the Planning Guide.
- Features checklists for each phase of communications system lifecycle.

Both found at https://www.cisa.gov/safecom/funding under "**Sustaining Public Safety Communications Systems**"



Regional News of Note

Scheduled Technical Assistance

- Kansas City Metro (FIFA 2026 Preparations):
  - Rescheduling – Communications Unit Leader Course
  - July 21-23, 2025 – Incident Communications Manager Course
  - Aug 26-27, 2025 – First Communications Exercise
- Cape Girardeau COMMEX (Missouri)
  - Aug 18-20, 2025
- Missouri TICP Train-the-Trainer – August 6, 2025

Red River COMU Boot Camp – Oct 12-17, 2025

- Potential opportunities for new instructors to get their teaching credentials.

For more information:

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