THIS IS AN EXERCISE

THIS IS AN EXERCISE

JOINT CYBERSECURITY ADVISORY

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
FEDERAL BUREAU OF INVESTIGATION (FBI)

TLP:CLEAR

Release Date: July 20, 2026
Alert Number: AA26-0720

PRC-ALIGNED CYBER ACTIVITY TARGETING U.S. CRITICAL INFRASTRUCTURE AND GOVERNMENT NETWORKS

EXECUTIVE SUMMARY

CISA and the FBI are issuing this advisory to inform network defenders of increased cyber activity associated with cyber actors aligned with the People's Republic of China (PRC). Recent intelligence reporting indicates these actors continue conducting cyber reconnaissance and pre-positioning activities targeting U.S. state and local governments, transportation systems, technology organizations, healthcare providers, and other critical infrastructure sectors.

While no intelligence currently indicates an imminent coordinated disruptive cyberattack, organizations should maintain heightened awareness and continue sharing cyber threat information through established coordination channels.

CURRENT ASSESSMENT

THREAT LEVEL:

ELEVATED

Federal agencies assess that PRC-aligned cyber actors continue conducting reconnaissance and access development activities targeting U.S. government and critical infrastructure networks.

There is no current intelligence indicating an imminent coordinated disruptive attack, although organizations should remain vigilant and continue information sharing with regional partners.

CURRENT THREAT ENVIRONMENT

Federal agencies have observed an increase in cyber activity directed toward organizations supporting:

- State & Local Government
- Emergency Management
- Transportation Systems
- Airports
- Maritime & Ports
- Healthcare
- Public Safety Communications
- Cloud Service Providers
- Technology Companies

RECENT REPORTING

Over the past several weeks, organizations have reported increases in:

- AI-generated phishing campaigns
- Executive impersonation attempts
- Cloud authentication anomalies
- Suspicious vendor activity
- Credential harvesting
- Network reconnaissance
- Attempts to compromise managed service providers
- Increased scanning of public-facing applications

OBSERVED TECHNIQUES

INITIAL ACCESS

- Spear phishing
- AI-assisted phishing campaigns
- Credential theft
- Exploitation of trusted vendors
- Public-facing application exploitation

PERSISTENCE

- Legitimate administrative tools
- Scheduled Tasks
- Remote administration utilities
- VPN credential reuse
- Cloud administrative functions

CREDENTIAL ACCESS

- Password spraying
- MFA fatigue attacks
- Browser credential harvesting
- OAuth token theft

DISCOVERY

- Active Directory reconnaissance
- Cloud environments
- Identity providers
- Enterprise networks
- GIS environments
- Operational Technology assets

DEFENSE EVASION

- Living off the land (LOTL)
- Log clearing
- Encrypted channels
- Remotse management software
- Cloud-native administrative functions

EMERGING AI THREATS

Organizations should anticipate increasing use of AI to support cyber operations, including:

- Executive impersonation and voice cloning
- Synthetic media and deepfake content
- AI-generated phishing emails
- Automated social media influence campaigns
- False emergency messaging and information manipulation

ORGANIZATIONS SHOULD REVIEW

- ☑ Review privileged account activity
- ☑ Validate multifactor authentication
- ☑ Review VPN authentication logs
- ☑ Audit cloud administrator accounts
- ☑ Test incident response procedures
- ☑ Review continuity plans
- ☑ Validate emergency notification systems
- ☑ Confirm contact information for regional cyber partners
- ☑ Review public information coordination procedures

INDICATORS WARRANTING ADDITIONAL REVIEW

Organizations should investigate:

- Administrator logins from unusual workstations
- Repeated failed authentication attempts
- Unexplained outbound network traffic
- Disabled accounts becoming active
- Creation of new privileged accounts
- Unexpected cloud latency
- Unexplained GIS or operational data changes
- Reports of AI-generated communications claiming to represent trusted organizations

REPORTING

Organizations observing suspicious cyber activity should report through established procedures and coordinate with:

- Regional Fusion Centers
- FBI Cyber Task Force
- CISA Regional Office
- State Cybersecurity Coordination Centers

Reporting early and sharing information helps protect your organization and our communities.

EXERCISE USE ONLY

This advisory was developed exclusively for Operation Cyber Bridge 2026.

This document is fictional and is intended solely for training and exercise purposes. It does not represent an actual advisory issued by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), or any other U.S. Government agency.