CYBER BRIDGE 2026 TABLETOP EXERCISE

Situation Manual

July 23, 2026

THIS PAGE INTENTIONALLY LEFT BLANK

EXERCISE OVERVIEW

Exercise Name	Cyber Bridge 2026
Exercise Dates	July 23, 2026
Scope	This exercise is a tabletop exercise, planned for four (4) hours at the Contra Costa County Emergency Operations Center.
Focus Area(s)	Prevention, Response and Recovery
Capabilities	Prevention: Cybersecurity Response: Intelligence and Information Sharing Response: Operational Communications Response/Recovery: Operational Coordination
Objectives	**Objective 1:** Assess the ability of participating jurisdictions and regional stakeholders to identify, validate, and share cyber threat intelligence, indicators of compromise, and situational awareness information across agencies within established coordination processes during an escalating AI-enabled cyber incident affecting multiple Bay Area jurisdictions. **Objective 2:** Evaluate the ability of participating organizations to coordinate regional operational response actions, including executive notifications, resource prioritization, cross-jurisdiction coordination, and decision-making processes, in response to cascading cyber impacts affecting critical services, infrastructure, and public operations. **Objective 3:** Evaluate the ability of participating organizations to implement internal and external communications procedures, including leadership notifications, interagency coordination, mission partner engagement, and public information considerations, during a rapidly evolving cyber incident involving AI-enabled threats and operational disruptions. **Objective 4:** Assess the ability of participating jurisdictions and regional partners to analyze and implement cybersecurity response, continuity, and recovery actions aligned with the NIST Cybersecurity Framework functions of Identify, Protect, Detect, Respond, and Recover during a coordinated cyberattack targeting regional systems, infrastructure, and public services.

Threat or Hazard	AI-led Cybersecurity Incursion
Scenario	Over the past six months, tensions have increased between the United States and China following restrictions on semiconductor exports, advanced computing technologies, and artificial intelligence systems. A Chinese-sponsored cyber group, APT Dragon Typhoon, has quietly embedded itself within government and industry networks throughout the Bay Area using stealthy techniques designed to avoid detection.
Sponsor	San Francisco Bay Area UASI
Relevant Plans	California Emergency Support Function 18-Cybersecurity NIST Cybersecurity Framework 2.0
Point of Contact	Amy Ramirez Project Manager SF Bay Area UASI amy.ramirez@sfgov.org (415) 412-8313

GENERAL INFORMATION

Exercise Objectives and Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team.

Exercise Objectives	Capability
Assess the ability of participating jurisdictions and regional stakeholders to identify, validate, and share cyber threat intelligence, indicators of compromise, and situational awareness information across agencies within established coordination processes during an escalating AI-enabled cyber incident affecting multiple Bay Area jurisdictions.	**Intelligence and Information Sharing**: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.
Evaluate the ability of participating organizations to coordinate regional operational response actions, including executive notifications, resource prioritization, cross-jurisdiction coordination, and decision-making processes, in response to cascading cyber impacts affecting critical services, infrastructure, and public operations.	**Operational Coordination**: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Exercise Objectives	Capability
Evaluate the ability of participating organizations to implement internal and external communications procedures, including leadership notifications, interagency coordination, mission partner engagement, and public information considerations, during a rapidly evolving cyber incident involving AI-enabled threats and operational disruptions.	**Operational Communications**: Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between affected communities in the impact area and all response forces.
Assess the ability of participating jurisdictions and regional partners to analyze and implement cybersecurity response, continuity, and recovery actions aligned with the NIST Cybersecurity Framework functions of Identify, Protect, Detect, Respond, and Recover during a coordinated cyberattack targeting regional systems, infrastructure, and public services.	**Cybersecurity**: Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Table 1. Exercise Objectives and Associated Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers:** Do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators:** Provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Evaluators:** Are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following three modules:

- Module 1: Early Indicators
- Module 2: Emerging Regional Impacts
- Module 3: Information Integrity Crisis

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in functional group discussions of appropriate response issues.

After these functional group discussions, participants will engage in a moderated plenary discussion in which a spokesperson from each group will present a synopsis of the group's actions, based on the scenario.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent-setting and may not reflect your jurisdiction's/ organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response efforts. Problem-solving efforts should be the focus.
- The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned capabilities, capability targets, and critical tasks, which are documented in Exercise Evaluation Guides (EEGs). Evaluators have EEGs for each of their assigned areas. Additionally, players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and compile the After-Action Report (AAR)/Improvement Plan (IP).

Exercise Instructions and Links

During the exercise we are asking one person per County to be a data collector and input information about the current issues and attacks that your county is facing.

We have designed a data collector form and a digital dashboard which you can use to input this information and feed the dashboard. This will be critical information for us to analyze at the end of the exercise so please be as detailed as possible regarding your operational impact areas, impact severity, action taken and any resources needed or resource requests you may have.

All exercise links are case sensitive so please match the links exactly

- **Exercise Page Link: bit.ly/Cyberbridge26**
  - This page contains all pre-exercise documents, link to a digital Sitman, and the module injects for each county.

- **ArcGIS Survey123 Link: bit.ly/Cyberbridge26collector**
  - This link will direct you to the data collector tool to input your county incidents and impacts.

- **ArcGIS Data Dashboard Link: bit.ly/Cyberbridge26data**
  - This link will direct you to the dashboard where you can live view the data and impacts across the region.

MODULE 1: EARLY INDICATORS

Day 0 through Day 1

Scenario

Tensions between the United States and China continue to intensify following additional export restrictions on advanced semiconductor manufacturing equipment, artificial intelligence technologies, and cloud computing services. Federal intelligence agencies have issued several classified and unclassified reports indicating that Chinese cyber actor **APT Dragon Typhoon** is increasing reconnaissance activities against U.S. critical infrastructure sectors and technology organizations.

Over the past several weeks, cybersecurity personnel across Northern California have observed increased suspicious activity targeting internet-facing systems, remote access portals, cloud services, managed service providers and third-party vendors supporting government and critical infrastructure operations. At the same time, Bay Area public agencies and private-sector partners have reported sophisticated AI-generated phishing, impersonation attempts, suspicious authentication activity and indicators that adversaries may be exploiting trusted vendor relationships.

Federal intelligence partners provide additional reporting indicating that Chinese-sponsored cyber operators may be positioning themselves for access within supply chain vendors that provide cloud hosting, managed services, transportation logistics software, and operational technology support to organizations throughout the Bay Area. Intelligence reporting further suggests that Chinese cyber actors may be preparing coordinated cyber and influence operations designed to undermine public confidence, disrupt operations, and demonstrate the vulnerability of U.S. technology hubs.

No significant service disruptions have occurred; however, multiple indicators suggest adversaries may be establishing access and conducting preparatory activities in advance of a larger campaign.

Key Issues

- **Threat Recognition and Escalation**: When organizations should determine that early recognition and response to scattered cyber indicators, vendor anomalies, AI-enhanced cyber threats, and isolated service disruptions should be treated as a coordinated regional campaign rather than isolated issues.
- **Risk Assessment**: Organizations may receive multiple indicators of malicious activity, but no confirmed compromise. Leaders must determine whether these events represent impacts to collateral systems or functions and the potential for disruptions to those normalities due to cascading circumstances.
- **Intelligence Sharing and Situational Awareness**: Agencies and private-sector partners are receiving conflicting information from public-facing systems, internal

dashboards, vendor platforms, field reports and social media. Federal intelligence, cybersecurity partners, and private industry begin sharing threat information that may affect multiple sectors.

- **AI-Enabled Misinformation and Impersonation:** False service alerts, AI-generated phishing, fake webpages, and realistic information from public sources are complicating public messaging and internal decision-making.
- **Supply Chain and Vendor Security:** Disruptions appear connected to trusted third-party vendors, cloud services, managed service providers, software updates, transportation platforms or operational technology support systems.

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 1. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

Intelligence & Information Sharing

1. How are cyber threat indicators shared among jurisdictions and sectors?
2. What thresholds trigger regional notifications?
3. How is information validated before dissemination?

Executive Decision-Making

1. At what point should leadership be briefed?
2. What actions can be taken prior to confirming an intrusion?

AI Governance

1. How does your organization identify AI-generated phishing attempts?
2. What policies exist regarding AI-enabled threats?

MODULE 2: EMERGING REGIONAL IMPACTS

Day 3 through Day 5

Scenario

In the days following reports of increased cyber reconnaissance activity and AI-enabled phishing campaigns, organizations across the Bay Area begin experiencing a growing number of operational disruptions affecting government services, transportation systems, public safety communications, utilities, healthcare, community services and shared technology partners.

What initially appeared to be isolated technical issues has expanded into a broader regional concern. Public agencies are reporting offline portals, authentication failures, e-mail disruptions, degraded collaboration platforms, and unreliable access to business-critical applications. Residents and businesses are experiencing delays in permitting, payments, licensing, record requests, public assistance transactions, and other routine services as agencies shift to manual processes.

Transportation and infrastructure impacts are also increasing. Airport, port, BART, traffic management, autonomous vehicle, EV charging, and logistics systems are producing conflicting or unreliable information, creating passenger delays, cargo slowdowns, station overcrowding, traffic bottlenecks, and broader community disruption. Utility and water system operators are also reporting inconsistent system data, false alarms and the need to manually verify field conditions.

AI-generated misinformation is amplifying the operational impacts. Spoofed emails, fake websites, fraudulent text alerts, synthetic voice messages, manipulated social media posts, clone service portals, and deepfake-style videos are causing residents, employees, businesses, and partner agencies to question which information sources can be trusted.

Federal partners continue to assess Dragon Typhoon-affiliated cyber activity targeting critical infrastructure sectors across the region. Intelligence reporting indicates that threat actors may be using compromised vendor relationships, cloud services, and AI-enabled tactics to disrupt operations, test response procedures, and undermine confidence in public institutions and technology systems.

While the full scope and attribution remain under investigation, the cascading impacts from compromised technology are becoming an increasingly critical response operation. The immediate challenge for regional leaders is to sustain essential services, validate trusted information, coordinate public messaging, protect vulnerable populations, and prioritize maintaining lifeline services to for the public while technical teams determine the extent of the compromise and restore services.

Key Issues

- **Regional Incident Recognition**: Previously isolated technical issues begin affecting multiple jurisdictions and sectors simultaneously, requiring a coordinated information-sharing and response structure.

- **Critical Infrastructure Coordination**: Transportation, utilities, communications, and public safety emergency communications are experiencing increasing interruptions, leading to additional disruptions in emergency response coordination and services.
- **Shared Technology Dependencies**: Multiple organizations identify potential compromises involving shared vendors, cloud platforms, identified systems, managed service providers, or compromised software supply chains.
- **Continuity of Essential Services**: Government entities and private sector partners must sustain critical functions while technology systems are degraded, unavailable, or unreliable. This includes shifting to manual processes, maintaining public access to essential services, supporting vulnerable populations and identifying which services require immediate restoration or alternate delivery methods.
- **AI-Enabled Misinformation and Impersonation:** Deepfake media, spoofed emergency alerts, cloned websites, fraudulent service portals, synthetic voice messages and manipulated social media content are undermining confidence in official information.

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 2. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

Operational Coordination

1. How are incidents correlated across sectors?
2. Who determines whether a regional activation is required?
3. What information should be included in a common operating picture?
4. Who owns the development of the regional common operating picture?

Resource Management

1. What cyber mutual aid mechanisms are available?
2. How are scarce cyber resources prioritized?

Infrastructure Protection

1. What critical services receive priority protection?
2. How are cascading impacts assessed?

Public Safety

1. How are public safety operations maintained if technology systems degrade?
2. What continuity plans are activated?

MODULE 3: INFORMATION INTEGRITY CRISIS

Day 7 through Day 12

Scenario

As government agencies and private-sector partners begin restoring systems across the Bay Area, the incident enters a new, more difficult phase. Core services are gradually returning but recovery is uneven. Many agencies continue to face backlogs, data integrity concerns, account access problems, and manual record reconciliation, and experience uncertainty about which systems can safely return to service. Public confidence is not recovering as quickly as the technology. Residents, businesses, employees, elected officials, and partner agencies continue to question whether restored systems, warning systems, service updates, records, maps, dashboards, and official communications can be trusted. In multiple jurisdictions, agencies can restore technical functionality but still cannot immediately confirm whether records, transactions, permissions, operational data, or AI-generated content were altered during the incident.

The information environment continues to complicate recovery. AI-generated videos, spoof text messages, fake public notices, cloned websites, fraudulent support portals, deepfake voice messages, false social media posts, and fabricated news reports continue circulating even as many systems return to normal. Some false reports recycle earlier misinformation, while others exploit recovery activities by directing employees, residents, businesses, and customers to fraudulent portals or fake instructions. Domestic fraudsters and opportunistic individuals are also taking advantage of the situation by trying to sell products or services to businesses and individuals to protect them from these technology issues, while never intending to deliver any actual service.

Federal intelligence agencies assess that Dragon Typhoon operators are actively conducting information operations to amplify confusion, undermine confidence in government institutions, and delay coordinated responses. Analysts believe artificial intelligence tools are being used to generate convincing deepfake audio recordings, manipulated videos, fabricated documents, and highly targeted social media content.

As operational disruptions continue to unfold, leaders must now manage both the cyber incident itself and a rapidly evolving crisis of information integrity.

Key Issues

- **Restoration Prioritization**: Government agencies and private-sector partners must determine which systems, services, facilities, users, and lifeline functions should be restored first, especially when access, staffing, vendor support, and validation capacity are limited.
- **Lifeline Stabilization and Cascading Impacts**: As systems are restored or eliminated, workaround procedures, vendor support, and validation capabilities are needed to restore and resume normal service delivery.
- **Common Operating Picture**: Real incidents become increasingly difficult to distinguish from misinformation and deception.

- **Countering Deepfakes and Misinformation**: Artificial intelligence is being used to create convincing fake videos, audio recordings, and official communications.
- **Public Information and Confidence**: Public trust begins to deteriorate as conflicting reports circulate.
- **Intelligence Integration and Attribution**: Federal, state, regional, private sector and local agency partners may provide different assessments regarding threat activity, attribution, vendor compromise and ongoing risk. Leadership must act on incomplete intelligence without over-committing to conclusions that may later change.

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 3. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

Information Verification

1. How is information authenticated before action is taken?
2. What procedures exist for validating executive communications?

Public Information

1. How are false narratives identified and countered?
2. Who has the authority to issue regional messaging?
3. How are unified messages coordinated across jurisdictions?

Executive Leadership

1. How do leaders make decisions when intelligence conflicts?
2. What level of confidence is required before public notification?

AI Governance

1. What safeguards exist to detect deepfakes?
2. How should AI-generated content be incorporated into decision-making?

Trust and Confidence

1. How is public trust maintained during uncertainty?
2. What actions are taken if misinformation causes public behavior changes?

APPENDIX A: EXERCISE SCHEDULE

09:00 AM-09:30 AM	Registration & Check-in
09:30 AM-10:00 AM	Welcome and Exercise Overview
10:00 AM-11:00 AM	Module 1 - Early Indicators
11:00 AM-12:00 PM	Module 2 - Emerging Regional Impacts
12:00 PM- 1:00 PM	Break/Lunch
1:00 PM- 2:00 PM	Module 3 - Information Integrity Crisis
2:00 PM- 2:45 PM	Hotwash
2:45 PM- 3:00 PM	Closing Comments/Adjourn

APPENDIX B: INVITED EXERCISE PARTICIPANTS

Invited Organizations
Alameda County (CISO, AI/Innovation, EM, ITD)
Bay Area Urban Area Security Initiative (BA UASI)
California Governor's Office of Emergency Services (Cal OES)
City of Carmel (IT Security)
City of Oakland (IT Security, EM)
City of San Francisco (CISO, Tech. Risk & Resilience, TIS, DEM IT, EM, OA)
City of San Jose (CISO, EM)
Contra Costa County (CISO, EM, Cybersecurity)
Department of Homeland Security (CISA)
Marin County (CISO, IT, EM)
Monterey County (CISO, EM, IT Security)
Napa County (CISO, EM)
Northern California Regional Intelligence Center (NCRIC)
San Benito County (CISO, EM, OES)
San Mateo County (EM)
Santa Clara City
Santa Clara County (IT Security, EM)
Santa Cruz County (CISO, EM)
Solano County (IT, Cyber Security, EM)
Sonoma County (IT, EM)
The Association of Bay Area Health Officials (ABAHO)

APPENDIX C: ACRONYMS

Acronym	Term
AAR	After Action Report
AI	Artificial Intelligence
APT	Advanced Persistent Threat
BART	Bay Area Rapid Transit
EEG	Exercise Evaluation Guide
EV	Electric Vehicles
HSEEP	Homeland Security Exercise and Evaluation Program
IP	Improvement Plan
NIST	National Institute of Standards and Technology
SitMan	Situation Manual
SMEs	Subject Matter Experts
TTX	Tabletop Exercise
UASI	Urban Area Security Initiative
WMDs	Weapons of Mass Destruction

APPENDIX D: GLOSSARY OF CYBER TERMS

Term	Definition
Advanced Persistent Threat (APT)	A sophisticated threat actor that maintains long-term access to targeted systems.
Artificial Intelligence (AI)	Technology that allows computer systems to perform tasks that normally require human judgment, such as recognizing patterns, analyzing data, generating text or images, making recommendations, or supporting decisions.
Credential Harvesting	Stealing usernames, passwords, MFA codes or other login information.
Deepfake	AI-generated or manipulated audio/video that makes someone appear to say or do something they did not.
Denial of Service (DoS)	An attack or condition that makes a system unavailable to users.
Distributed Denial of Service (DDoS)	A denial-of-service attack launched from many sources at once.
Living off the Land (LOTL)	Attackers using normal system tools and legitimate administrative functions to avoid detection.
Managed Service Provider (MSP)	A third-party company that manages IT, cloud, software, security, or network services for organizations.
Operational Technology (OT)	Technology that monitors or controls physical processes, equipment, utilities, transportation systems or facilities.
Phishing	Fraudulent messages designed to trick users into clicking links, opening files, sharing credentials, or taking action.
Privilege Escalation	When an attacker gains higher-level access than they originally had.
Ransomware	Malware that locks or encrypts systems and demands payment to restore access or prevent data release.
Service Degradation	A system is still operating but slower, unreliable, incomplete or producing errors.
Social Engineering	Manipulating people into revealing information or taking unsafe actions
Synthetic Media	AI-created or AI-manipulated media, including fake images, videos, voice recordings, documents or screenshots.
Threat Actor	The person, group, or organization responsible for malicious activity.
Vendor Compromise	When a third-party provider is breached or manipulated in a way that affects its customers.

Term	Definition
Virtual Private Network (VPN)	A secure connection used by staff to remotely access internal systems.
Zero Day	A previously unknown vulnerability that does not yet have a fix available.

APPENDIX E: CYBER PREPAREDNESS/RESPONSE RESOURCES

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

https://www.cisa.gov/

https://www.fbi.gov/investigate/cyber

https://www.ic3.gov/ContactFBICyber

https://ncric.ca.gov/ncric/

APPENDIX F: PRE-EXERCISE GROUND TRUTH

THIS IS AN EXERCISE

THE BAY AREA TIMES

MONDAY, JULY 20, 2026 | SERVING NORTHERN CALIFORNIA SINCE 1874 | BAYAREATIMES.COM | $2.00

TRANSPORTATION

Oakland Port Expects Record Cargo Volume This Summer

The Port of Oakland is projecting a 7% increase in cargo traffic over the previous year, driven by strong imports and continued growth in agricultural exports.

Officials say increased shipping demand is expected to place pressure on regional transportation networks throughout the summer.

LOCAL, A2

BART

BART Approves Late-Night Service Pilot

The BART Board approved a six-month pilot program extending weekend train service past midnight on select lines.

Transportation officials hope the change will improve mobility and support downtown economic activity.

LOCAL, A2

Tensions Rise as Dragon State Condemns U.S. Technology Restrictions

Federal officials say there is no indication of an imminent threat, but experts warn geopolitical tensions are increasingly playing out in cyberspace and through influence campaigns.

Continued on A3

The Bay Area's concentration of technology, transportation, and critical infrastructure has made the region an economic powerhouse—and an increasing focus of geopolitical competition.

PHOTO: JESSICA CHRISTENSEN / BAY AREA TIMES

CYBERSECURITY

Cybersecurity Experts Urge Organizations to Review Preparedness

Federal and industry partners are encouraging organizations to review cybersecurity governance, cybersecurity procedures, and continuity plans amid an increase in global cyber espionage and influence operations.

Recent reports cite:

- AI-generated phishing campaigns
- Social media impersonation
- Increased reconnaissance activity
- Credential theft targeting government and industry

Officials emphasized there is no evidence these activities are connected or represent an imminent threat.

Experts say basic cybersecurity hygiene and information sharing remain the best defenses.

TECHNOLOGY, C1

BAY AREA WEATHER

MONDAY — High 94°

TUESDAY — High 97°

WEDNESDAY — High 98°

Complete forecast on B8

SPORTS

Giants Beat Mariners 5–3

The Giants complete a three-game sweep Sunday afternoon behind strong pitching and a late two-run homer.

SPORTS, B1

BUSINESS

Local Tech Hiring Rebounds

Several Bay Area technology firms announced hiring increases this week after a slow start to the year.

Industry analysts say demand for artificial intelligence and cloud computing talent remains strong.

BUSINESS, C1

THIS IS AN EXERCISE

AROUND THE BAY

ALAMEDA COUNTY

Port officials investigating several cargo terminal congestion issues. A4

CONTRA COSTA COUNTY

Refineries report increased cyber awareness after recent operations. A4

MARIN COUNTY

County supervisors approve wildfire mitigation grants for local communities. A5

SANTA CLARA COUNTY

New pediatric wing opens at Children's Hospital in San Jose. A5

SAN MATEO COUNTY

Officials announce upgrades to county cybersecurity risk management framework. A6

SANTA CRUZ COUNTY

Officials warn of rough surf and high rip current advisories. A6

NAPA COUNTY

Summer concert series begins Friday in downtown Napa. A7

SONOMA COUNTY

Wine industry projects strong harvest season across the county. A7

MONTEREY COUNTY

Tourism officials expect record summer attendance along the coast. A8

SUMMER OUTDOORS — BAY AREA —

Festivals, hikes, and outdoor adventures across the Bay Area

SPECIAL SECTION INSIDE

INSIDE

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	PERSISTENCE	CREDENTIAL ACCESS	DISCOVERY	DEFENSE EVASION
• Spear phishing • AI-assisted phishing campaigns • Credential theft • Exploitation of trusted vendors • Public-facing application exploitation	• Legitimate administrative tools • Scheduled Tasks • Remote administration utilities • VPN credential reuse • Cloud administrative functions	• Password spraying • MFA fatigue attacks • Browser credential harvesting • OAuth token theft	• Active Directory reconnaissance • Cloud environments • Identity providers • Enterprise networks • GIS environments • Operational Technology assets	• 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

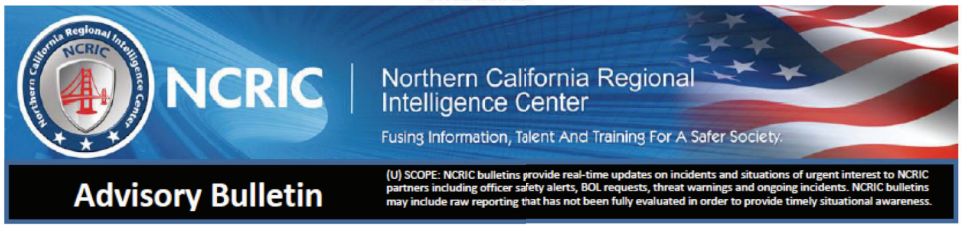
This advisory was developed exclusively for Operation Cyber Bridge 2026.

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.

THIS IS AN EXERCISE

THIS IS AN EXERCISE

UNCLASSIFIED



21 July 2026

(U) Aggressive Phishing Campaign Targeting Public and Private Sector Organizations

((U) Summary: Threat actors are conducting a widespread phishing campaign targeting government agencies, critical infrastructure, healthcare organizations, educational institutions, financial services, transportation entities, and private businesses. The campaign uses credential harvesting, business email compromise, malicious attachments, and spoofed cloud service login portals.

(U) Threat Activity: Observed tactics include fraudulent Microsoft 365 and Google Workspace login pages, account security notifications, payroll and HR-themed emails, vendor impersonation, invoice fraud, and MFA fatigue attacks. Adversaries are leveraging publicly available information to increase legitimacy and improve targeting.

(U) Potential Impacts: Successful compromise may result in credential theft, unauthorized network access, ransomware deployment, data exfiltration, operational disruption, financial fraud, and compromise of sensitive information.

(U) Indicators: Unexpected login requests, urgent requests for action, suspicious attachments, domains closely resembling legitimate organizations, unsolicited MFA prompts, and requests to change payment or account information.

(U) Considerations: Organizations should reinforce phishing awareness training, validate email authentication controls (SPF, DKIM, DMARC), implement phishing-resistant MFA, monitor authentication logs, and promptly investigate reported phishing attempts.

(U) Reporting: Report suspicious cyber activity through organizational reporting channels. Significant cyber incidents should be reported to appropriate law enforcement and cybersecurity partners. Preserve email headers, attachments, and relevant logs for investigative purposes.

UNCLASSIFIED

THIS IS AN EXERCISE

The Olson Group, Ltd.
209 Madison Street
Suite 410
Alexandria, VA 22314
(703) 518-9982