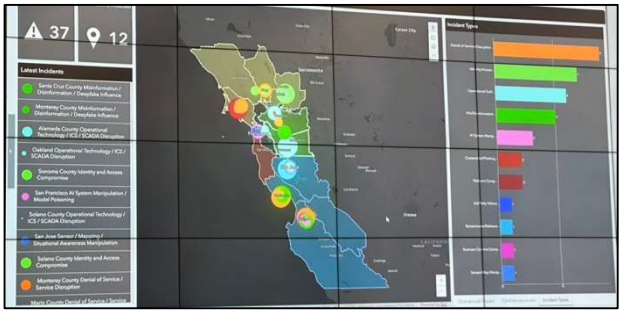
Cyber Bridge 2026
Exercise After-Action Report
Executive Summary



The Cyber Bridge 2026 Tabletop Exercise was conducted at the Contra Costa County Emergency Operations Center on July 23, 2026, providing 83 participants from more than two dozen counties, cities and infrastructure operators with an opportunity to consider local and regional responses to an AI-powered cyberattack. The exercise was built around a scenario involving a multi-target attack against the Bay Area by a foreign government seeking to disrupt essential public services in the region while discrediting official sources of information. Participants discussed their plans and actual capabilities to detect and deal with a series of attacks. They compared practices across jurisdictions and disciplines, including a discussion of information-sharing challenges.

Participants addressed four core capabilities:

- Intelligence and Information Sharing
- Operational Coordination
- Operational Communications
- Cybersecurity

The exercise demonstrated the value of regional collaboration in preparing for increasingly complex cyber incidents while identifying actionable opportunities to strengthen coordination, planning, and operational readiness across the Bay Area.

Exercise participants recommended actions to help achieve those goals:

Intelligence and Information Sharing

- Establish common regional thresholds for validating, sharing, and escalating cyber threat information.
- Strengthen regional situational awareness and share a common operating picture to support timely and coordinated decision-making.

Operational Coordination

- Update jurisdiction/agency cyber incident response/recovery plans addressing technical, operational, policy, continuity, and public information roles and responsibilities.
- Integrate IT personnel into appropriate EOC/incident management roles in response to cyber-attacks.

Operational Communications

- Strengthen regional Joint Information Center coordination.
- Develop outreach to counter phishing, deepfakes, and misinformation.
- Share procedures for validating, escalating, and coordinating responses to disinformation.

Cybersecurity

- Plans should ensure clarity in recovery priorities and identify regional interdependencies.
- Continue training on detection and prevention of cyber-attacks (e.g., phishing, malware, stuffing, etc.).
- Expand focus of cyber preparedness beyond financial systems to include cloud-based portals, customer-facing services, and public websites.

Exercise participants applauded the exercise for providing an opportunity to work across jurisdictions, agencies, departments, and professional disciplines.

Cyber Bridge 2026 was funded by the Bay Area Urban Areas Security Initiative, a grant from the U.S. Department of Homeland Security. This document does not necessarily represent the official position or policies of the U.S. Department of Homeland Security.