UASI Bay Area Training & Exercise Program

Dates and Location

Cohort 1: Virtual courses offered July 13–August 11, 2026

Cohort 2: Combination of virtual and in-person sessions offered August 13–27, 2026 (see page 2)

Tuition and Registration

This series of courses is provided at no cost by the UASI Bay Area Training & Exercise Program (BATEP).

Register at: https://bayareauasi-ca.gov/

Virtual Courses

Registered participants will receive meeting links and course materials prior to each class

Target Audience

Public-sector cybersecurity practitioners, IT professionals, emergency managers, and decision-makers across Bay Area jurisdictions.

Prerequisites

N/A

Certification

Certificate of completion provided for each course.

Attendance Policy:

A no-show may result in a temporary suspension of your BATEP account. If you are unable to attend after being accepted into the class, please advise the course point of contact as soon as possible so the class can be offered to another student on the waitlist.

Special Considerations

Contact DEM-BATEP@sfgov.org regarding accessibility needs at least 96 hours before the class.

For More Information

Please contact Corinne Bartshire at corinne.bartshire@sfgov.org or

UASI AI CYBERSECURITY TRAINING PROGRAM

Program Overview

The UASI AI Cybersecurity Training Program is a comprehensive **five-course curriculum** designed to equip Bay Area public-sector stakeholders with the knowledge and skills needed to safely leverage artificial intelligence while defending against AI-enabled cyber threats.

Participants will develop a shared understanding of AI governance frameworks and responsible use, explore how machine-learning techniques support anomaly detection and predictive analytics, practice AI-enhanced incident response and investigative workflows, learn to architect secure AI and cloud environments, and synthesize these capabilities into a regional resilience strategy.

By blending strategic context with hands-on operational exercises, the program fosters collaboration across jurisdictions, strengthens regional preparedness, and supports the early identification and mitigation of terrorism-related cyber activity.

Key Benefits

- Build a foundational understanding of AI governance and cybersecurity ethics
- Gain practical skills in AI-powered threat detection, response, and investigation
- Learn secure deployment and cloud security practices for AI systems
- Develop regional resilience and long-term operational readiness
- Foster collaboration and shared vocabulary across jurisdictions

This document was prepared under a grant from FEMA's Grant Programs Directorate, U.S. Department of Homeland Security. Content is derived from the Bay Area Training and Exercise Program and does not necessarily represent the official position or policies of FEMA's Grant Programs Directorate or the U.S. Department of Homeland Security.

Course Offerings and Schedule

Course Title	Cohort 1 (Delivery & Dates)	Cohort 2 (Delivery & Dates)
Course 1 — AI, Cybersecurity, Governance, and the Emerging Threat Landscape	Virtual, 2 x 4-hour sessions July 13, 2026 and July 14, 2026	In-Person, 8-hour session August 13, 2026
Course 2 — Applied AI and Machine Learning for Cybersecurity Operations	Virtual, 2 x 4-hour sessions July 15, 2026 and July 16, 2026	Virtual, 2 x 4-hour sessions August 17, 2026 and August 18, 2026
Course 3 — AI-Driven Threat Detection, Incident Response, and Investigations	Virtual, 2 x 4-hour sessions July 20, 2026 and July 21, 2026	Virtual, 2 x 4-hour sessions August 19, 2026 and August 20, 2026
Course 4 — Secure AI Infrastructure, Cloud Security, and Defensive Architecture	Virtual, 2 x 4-hour sessions July 27, 2026 and July 28, 2026	Virtual, 2 x 4-hour sessions August 24, 2026 and August 25, 2026
Course 5 — Regional AI Cyber Resilience and Operational Readiness Workshop	Virtual, 2 x 4-hour sessions August 10, 2026 and August 11, 2026	In-Person, 8-hour session August 27, 2026

Course Descriptions

Course	High-Level Summary	Description	Curriculum Role / Progression
Course 1 — AI, Cybersecurity, Governance, and the Emerging Threat Landscape	Foundational overview of AI, cybersecurity, governance, procurement, and emerging AI-enabled threats for public-sector audiences.	Establishes a shared regional foundation regarding the rapidly evolving AI ecosystem, emerging AI-enabled cyber threats, AI governance, responsible use frameworks, AI procurement considerations, and secure AI deployment practices. Topics include current AI systems and foundation models, AI governance and oversight, NIST AI RMF alignment, ethical and privacy considerations, AI as both a defensive capability and attack surface, adversarial AI concepts, AI-enabled cyber threats, AI procurement and vendor risk, AI supply chain security, and secure lifecycle management practices derived from safe model deployment principles. The course also introduces emerging cyber capabilities and operational implications associated with advanced AI systems, including public-sector considerations related to systems such as Anthropic and GPT cyber-enabled models.	Serves as the strategic and conceptual foundation for the entire curriculum by establishing common vocabulary, governance understanding, operational awareness, and regional context before progressing into more technical and operational cybersecurity applications. Designed for both technical and non-technical audiences across Bay Area jurisdictions.
Course 2 — Applied AI and Machine Learning for Cybersecurity Operations	Practical introduction to how AI and machine learning support cybersecurity operations and public-sector cyber defense.	Establishes operational understanding of how AI and machine learning technologies are applied within cybersecurity environments. Topics include AI and machine-learning fundamentals, cybersecurity use cases, anomaly detection, predictive risk analytics, AI-assisted detection mechanisms, automated defense concepts, data requirements, operational integration tradeoffs, human-machine collaboration, and public-sector implementation considerations. The course examines how AI technologies can support threat identification, operational awareness, and cyber defense activities across public-sector environments.	Builds upon Course 1 by transitioning participants from strategic understanding into practical cybersecurity applications of AI and machine learning technologies. Establishes the operational and technical baseline necessary for later instruction involving incident response, investigations, infrastructure security, and resilience operations.

Course	High-Level Summary	Description	Curriculum Role / Progression
Course 3 — AI-Driven Threat Detection, Incident Response, and Investigations	Operational cybersecurity course focused on AI-enhanced detection, incident response, investigations, and digital forensics.	Focuses on operational cybersecurity workflows involving AI-enhanced threat detection, incident response, digital forensics, and investigative analysis. Topics include AI-assisted threat detection, SIEM integration, event correlation, false-positive reduction, incident triage, response automation, escalation workflows, AI-augmented investigations, digital evidence analysis, timeline reconstruction, pattern recognition, intelligence coordination, and investigative rigor. The course incorporates operational case studies and discussion-based scenarios focused on coordinated cyber incidents affecting public-sector organizations.	Advances participants from foundational AI cybersecurity understanding into operational cyber defense and investigative activities. Integrates detection, response, investigative analysis, and interagency coordination concepts relevant to public-sector cyber operations and regional incident management.
Course 4 — Secure AI Infrastructure, Cloud Security, and Defensive Architecture	Focuses on cloud security, identity management, secure AI deployment, and resilient defensive infrastructure.	Focuses on the infrastructure, identity, cloud, and operational security controls necessary to securely deploy and manage AI-enabled systems. Topics include cloud security architecture, identity and access management, authentication, privilege management, AI-driven identity analytics, anomaly detection, zero-trust principles, secure configuration management, governance controls, AI infrastructure security, secure deployment practices, lifecycle monitoring, supply chain security, and operational resilience considerations for cloud-hosted AI environments.	Builds upon earlier operational cybersecurity concepts by focusing on the infrastructure and defensive architecture necessary to securely support AI-enabled operational environments. Prepares participants to understand long-term operational hardening, cloud security, identity governance, and infrastructure resilience.
Course 5 — Regional AI Cyber Resilience and Operational Readiness Workshop	Capstone workshop focused on operational resilience, practical implementation, coordination, and sustaining long-term cybersecurity readiness.	Serves as the capstone course for the curriculum by integrating prior course concepts into a practical regional resilience and operational readiness workshop. Topics include synthesis of prior material, practical AI implementation strategies, maintaining adaptive cybersecurity posture, operational resilience planning, continuity considerations, public-sector AI applications, cross-sector coordination, preparedness planning, emerging threat trends, governance evolution, and long-term cyber resilience strategies. The course incorporates operational discussions, facilitated scenario-based conversations, practical implementation guidance, and multi-disciplinary collaboration focused on sustaining resilient AI-enabled cybersecurity capabilities across Bay Area jurisdictions.	Concludes the curriculum by integrating strategic, operational, investigative, and infrastructure concepts into a forward-looking resilience and preparedness framework. Reinforces practical implementation, operational coordination, and long-term regional cybersecurity maturity.