UASI AI CYBERSECURITY TRAINING PROGRAM

CURRICULUM OVERVIEW • FIVE-COURSE PROGRAM

AI Cybersecurity Training Program

A cohesive executive education program that progressively builds knowledge from foundational AI concepts through operational implementation and regional resilience for a mixed public-sector audience across Bay Area jurisdictions.

FORMAT	STRUCTURE	AUDIENCE
Interactive workshops	5 courses · 2 sessions each	Public-sector, mixed

IN THIS OVERVIEW

Program overview · Overall approach · Course deliverables · Curriculum themes · Course progression · Syllabus overview for Courses 1–5 · FBI Cyber Threat Response · Operation Winter Shield

PROGRAM

Program Overview

The training curriculum represents a cohesive executive education program that progressively builds participants' knowledge from foundational concepts through operational implementation and regional resilience.

The curriculum is designed for a mixed public-sector audience — including cybersecurity practitioners, IT professionals, emergency managers, public safety personnel, and organizational leaders — and emphasizes practical application, collaboration, and organizational readiness.

Overall Approach

Rather than relying primarily on lecture, each course is structured as an interactive workshop that combines:

- 🎓 **Expert instruction**
- 💬 **Facilitated peer discussions**
- 📁 **Real-world case studies**
- 🎤 **Optional guest speakers**
- 🧩 **Practical organizational exercises**
- 🤝 **Regional roundtable discussions**

The emphasis is on helping participants understand not only *what* AI technologies are, but *how* they should be strategically adopted, governed, secured, and operationalized within public-sector organizations.

Program Notes

Case Study Approach

Each course incorporates two to four real-world case studies drawn from recent cybersecurity events to reinforce key concepts and encourage practical discussion across government and critical infrastructure sectors.

Guest Speakers

Time is reserved within each course for an optional guest speaker depending on availability — federal, public-sector, critical infrastructure, academia, or industry. Speakers enhance, but are not required for, delivery.

End Goal

Deliver an executive-level curriculum that satisfies UASI training requirements and equips public-sector leaders with practical frameworks, tools, and shared language to strengthen responsible AI adoption and cybersecurity readiness.

Curriculum Themes

The curriculum consistently reinforces several core themes throughout all five courses:

- AI is transforming both government operations and cybersecurity.
- Successful AI adoption requires organizational strategy, governance, and cybersecurity working together.
- AI governance includes responsible AI, AI cybersecurity, privacy, and risk management.
- AI should be adopted through a deliberate organizational roadmap aligned with mission priorities.
- AI serves as a force multiplier for both defenders and adversaries.
- Regional collaboration is essential to strengthening preparedness and resilience.

Course Progression

1	Strategic foundation for AI, governance, organizational adoption, and the evolving cyber threat landscape.
2	Practical application of AI and machine learning within cybersecurity operations.
3	AI-enabled threat detection, incident response, investigations, and digital forensics.
4	Secure AI infrastructure, cloud security, identity, and defensive architecture.
5	Capstone workshop focused on operational resilience, implementation, and regional collaboration.

SYLLABUS OVERVIEWS

Course Syllabus Overview — Courses 1 through 5

A one-page overview of each course in the program — course focus, learning objectives, and the four core topic modules.

1 · Strategic Foundation
2 · Applied Operations
3 · Detection & Response
4 · Secure Infrastructure
5 · Capstone Workshop

COURSE 1 · STRATEGIC FOUNDATION

1 AI, Cybersecurity, Governance, and the Emerging Threat Landscape

COURSE OVERVIEW

Establishes the strategic foundation for the program by introducing the evolving AI landscape, organizational AI strategy, AI governance, AI-enabled cyber threats, and practical approaches for adopting AI responsibly while strengthening cybersecurity and organizational resilience.

LEARNING OBJECTIVES

01 Explain how AI is transforming cybersecurity, public safety, and government operations.

02 Evaluate strategy, governance, and cybersecurity considerations for successful AI adoption.

03 Recognize emerging AI-enabled cyber threats, defenses, and secure deployment practices.

04 Apply foundational concepts to assess AI opportunities and risks within their organizations.

COURSE MODULES

1 The AI Revolution

AI evolution & capabilities · Foundation models · Agentic AI · Public-sector opportunities

2 AI-Ready Organization

AI strategy · Governance · Responsible AI · AI cybersecurity · Adoption roadmap

3 The New Cyber Battlefield

AI-powered defense · AI-enabled threats · Adversarial AI · Nation-state use

4 Procurement to Deployment

AI procurement · Vendor evaluation · Secure deployment · Supply chain · Monitoring

FORMAT

Interactive workshop · 2 sessions × 4 hours · Foundational level · Expert instruction, facilitated discussion, real-world case studies, and optional guest speakers.

COURSE 2 · APPLIED OPERATIONS

2 Applied AI and Machine Learning for Cybersecurity Operations

COURSE OVERVIEW

Building on Course 1, this course examines how AI and machine learning are practically applied across cybersecurity operations — exploring common use cases, the strengths and limitations of machine learning, AI-assisted decision support, and how to prioritize capabilities that improve cyber resilience while maintaining appropriate human oversight.

LEARNING OBJECTIVES

01 Explain how AI and machine learning are transforming modern cybersecurity operations.

02 Evaluate where AI can provide the greatest operational value within their organizations.

03 Distinguish between AI that augments analysts versus AI requiring human oversight.

04 Identify practical opportunities to integrate AI into cybersecurity workflows while managing risk.

COURSE MODULES

1 ML Fundamentals

AI vs. ML · Supervised & unsupervised learning · Foundation models · Security applications

2 AI Across the Lifecycle

SOCs · Threat intelligence · Vulnerability management · Identity security · Predictive analytics

3 Human-AI Collaboration

Security copilots · Analyst augmentation · Automation · Human oversight · Decision support

4 Planning AI Operations

Operational implementation · Prioritizing capabilities · Workforce readiness · Adoption

FORMAT

Interactive workshop · 2 sessions × 4 hours · Applied level · Expert instruction, practical demonstrations, facilitated discussion, and collaborative exercises.

COURSE 3 · DETECTION & RESPONSE

3 AI-Driven Threat Detection, Incident Response, and Investigations

COURSE OVERVIEW

Examines how AI is transforming modern cyber defense operations. Participants explore AI-enhanced threat detection, security operations, incident response, digital forensics, and investigative workflows, and how organizations can combine AI capabilities with human expertise to improve cyber resilience and operational readiness.

LEARNING OBJECTIVES

01 Explain how AI is improving cyber threat detection, investigations, and incident response.

02 Evaluate how AI can augment SOCs and investigative workflows with human oversight.

03 Assess how AI is changing the tactics, techniques, and procedures of cyber adversaries.

04 Apply practical approaches for strengthening incident response and investigative capabilities.

COURSE MODULES

1 AI-Enabled Detection

SOCs · Threat intelligence · Anomaly detection · Threat hunting

2 AI-Assisted Response

Incident triage · Investigation · Response automation · Human decision-making

3 Digital Forensics & AI

Evidence collection · Data correlation · Timeline reconstruction · Investigative analysis

4 Building IR Programs

Operational planning · Playbooks · Workforce readiness · Continuous improvement

FORMAT

Interactive workshop · 2 sessions × 4 hours · Operational level · Expert instruction, demonstrations, operational case studies, and collaborative exercises.

COURSE 4 · SECURE INFRASTRUCTURE

4 Secure AI Infrastructure, Cloud Security, and Defensive Architecture

COURSE OVERVIEW

Explores the infrastructure and architectural foundations required to securely deploy and manage AI-enabled systems. Participants examine cloud security, identity and access management, Zero Trust principles, AI supply chain security, and practical approaches for designing resilient AI-enabled environments.

LEARNING OBJECTIVES

01 Explain the infrastructure and architectural components required to securely support AI systems.

02 Evaluate cloud, identity, and Zero Trust strategies that strengthen cybersecurity.

03 Assess infrastructure risks from AI deployment, third-party AI services, and supply chains.

04 Apply practical approaches for improving the resilience and security of AI environments.

COURSE MODULES

1 Secure Foundations

AI infrastructure · Cloud architecture · Shared responsibility · Organizational readiness

2 Identity & Zero Trust

Identity governance · Authentication · Privileged access · Zero Trust architecture

3 Securing the Lifecycle

Secure deployment · AI supply chain · Continuous monitoring · Third-party risk

4 Resilient Environments

Resilience planning · Secure architecture · Operational monitoring · Future-state planning

FORMAT

Interactive workshop · 2 sessions × 4 hours · Operational level · Expert instruction, architecture discussions, demonstrations, and collaborative planning exercises.

COURSE 5 · CAPSTONE WORKSHOP

5 Regional AI Cyber Resilience and Operational Readiness Workshop

COURSE OVERVIEW

As the capstone course, this workshop brings together the concepts introduced throughout the curriculum to help participants develop practical strategies for strengthening organizational resilience and enhancing regional preparedness — sustaining secure AI adoption while improving operational readiness across Bay Area jurisdictions.

LEARNING OBJECTIVES

01 Integrate AI strategy, governance, cybersecurity, and operational planning into a resilience framework.

02 Evaluate organizational preparedness for emerging AI threats and evolving operational risks.

03 Develop practical priorities for long-term cybersecurity resilience and responsible AI adoption.

04 Identify opportunities for cross-jurisdiction collaboration and information sharing.

COURSE MODULES

1 Integrating Resilience

Lessons learned · Organizational maturity · AI governance · Strategic alignment

2 Future Threat Landscape

Emerging threats · Nation-state activity · AI-enabled cybercrime · Future technologies

3 Regional Collaboration

Information sharing · Mutual support · Exercises · Public-private partnerships

4 Organizational Roadmap

Action planning · Capability priorities · Continuous improvement · Next steps

FORMAT

Capstone workshop · 2 sessions × 4 hours · Facilitated discussion, peer collaboration, planning exercises, case studies, and regional knowledge sharing.

Instructor and Facilitator Bios



Dennis Chornenky, MBA MPH MS

Dennis Chornenky is the Founder and CEO of Domelabs AI and a nationally recognized leader in artificial intelligence, cybersecurity, and technology strategy. He previously served as a Senior Advisor and Presidential Innovation Fellow at the White House and as Chief AI Officer at UnitedHealth Group, where he led enterprise AI adoption initiatives. Dennis has advised governments, federal agencies, Fortune 500 companies, and leading academic medical centers on AI strategy, governance, and cybersecurity. He holds degrees from MIT, Harvard, Oxford, and UC Berkeley and is a graduate of the FBI CISO Academy.



Jason Haupt, PhD

Jason Haupt is a product and strategy leader at Domelabs AI and former Chief Data Scientist at Optum. He is an experienced technology leader who helps organizations in regulated sectors accelerate responsible AI adoption while maintaining strong governance and security. His experience spans AI strategy, enterprise architecture, cybersecurity, product development, and applied machine learning, with a focus on translating emerging AI technologies into practical operational capabilities for complex organizations.



Pieter Nel, MBA MS

Pieter Nel is an experienced technology executive specializing in artificial intelligence, cybersecurity, and enterprise technology strategy. Previously a technology leader at McKinsey & Company, CloudFactory, Ocrolus, and other high-growth technology companies, Pieter has advised organizations worldwide. He holds an engineering degree from Stellenbosch University and an MBA from MIT.



George Chewning, MBA

George Chewning is a U.S. Army veteran and national security leader. As a White House Presidential Innovation Fellow, he helped stand up the VA's National AI Institute. He has held leadership roles advancing AI, technology modernization, and public-sector innovation, helping government organizations adopt emerging technologies to strengthen mission effectiveness, operational resilience, and national security.



Marco Smit, MS

Marco Smit is the Chief Operating Officer of Domelabs AI, where he oversees operations and customer delivery for AI governance, AI adoption, and cybersecurity. He has extensive experience leading enterprise technology, helping organizations implement secure, responsible AI solutions while strengthening governance, operational resilience, and organizational readiness.

About Domelabs AI

Domelabs is transforming AI adoption, governance, and cybersecurity in mission-critical sectors by delivering proactive, mission-aligned, and data-driven modernization solutions tailored for CIOs, CISOs, Chief AI Officers, and their executive teams.

Trusted by federal agencies, Fortune 500 companies, and top academic medical centers, Domelabs combines deep policy expertise with operational experience to offer a unified suite of advisory services and enterprise technology capabilities. Domelabs' solutions empower organizations to safely, securely, and strategically adopt transformative technologies—accelerating mission outcomes while maintaining compliance and control.

APPENDIX

Supplemental Cyber Resilience Resources

The following reference materials are attached for participants: the FBI Cyber Threat Response guide and the Operation Winter Shield "Ten Actions to Improve Cyber Resilience" handout.

- **A** FBI Cyber Threat Response
- **B** Operation Winter Shield — Ten Actions to Improve Cyber Resilience

APPENDIX A · FBI CYBER

Cyber Threat Response and Assistance

FBI Cyber employs a global network of cyber threat experts to investigate cybercriminals, disrupt malicious cyber activity, seek justice, and prevent crime. FBI Cyber provides information, experts, and capabilities to inform your cyber threat response — including notifying targeted entities who may be unaware they have been compromised and, when possible, assisting in freezing, seizing, and returning stolen and extorted funds.

FACT VS. FICTION

- ✓ Provides information to help you respond to intrusions — **does not** restore systems or data.
- ✓ Works with your IT team to collect evidence, with your consent — **does not** search for unrelated activity.
- ✓ Coordinates with your attorneys — **does not** give legal or regulatory advice.
- ✓ Works with your press team upon request — **does not** publicize your intrusion.
- ✓ Shares data with federal partners with a need-to-know, like CISA — **does not** seek information for regulatory purposes.

PRE-INTRUSION TIPS

Connect

Determine who to contact before an intrusion. Include your local FBI field office in your incident response plan and invite them to tabletop exercises. Choose private incident response firms in advance.

Stay Informed

Read the latest federal cyber alerts and implement their recommendations — IC3.gov, StopRansomware.gov, and CISA.gov.

POST-INTRUSION TIPS

REPORT	Notify the FBI with relevant intrusion details.
PRESERVE	Collect indicators of compromise — malware samples, logs, and other intrusion data.
COMMUNICATE	Keep lines of communication open between your team and the FBI.
SHARE	The FBI relies on shared data to investigate and disrupt perpetrators.

HOW TO CONTACT

Local or International FBI Field Offices — **fbi.gov/contact-us**
FBI Internet Crime Complaint Center (IC3) — **ic3.gov**

Reproduced from the FBI Cyber "Cyber Threat Response and Assistance" informational handout.

APPENDIX B · OPERATION WINTER SHIELD

Ten Actions to Improve Cyber Resilience

Objective: Operation Winter Shield distills the FBI's 10 most impactful actions organizations can take to improve resilience against cyber intrusions. These recommendations were developed with domestic and international partners and draw on recent investigations to reflect adversary behavior and defensive gaps.

1 Adopt phish-resistant authentication

Many breaches start with stolen passwords. Prioritize admin/executive accounts; deploy FIDO2 keys or device-bound passkeys; require number-matching (avoid push-only); eliminate SMS MFA and legacy authentication.

2 Implement risk-based vulnerability management

Adversaries exploit known, unaddressed vulnerabilities. Maintain a complete asset inventory with owners; set remediation timelines by risk (critical in days); use authenticated internal scans; document exceptions with fixed dates.

3 Track and retire end-of-life technology

EOL systems no longer receive security updates and are routinely targeted. Keep a rolling 12-month EOL forecast reviewed quarterly; track by product, owner, and retirement date; replace or isolate EOL assets with firm decommission dates.

4 Manage third-party risk

Security extends only as far as your least-protected vendor. Maintain a list of third parties with access and named owners; require strong authentication and least privilege; disable unused accounts; contractually require rapid breach notification and annual control verification.

5 Protect and preserve security logs

Preserved logs are essential for detection, response, and attribution. Centralize logs in a SIEM and export daily to immutable storage; retain per legal/response needs (12 months is common); synchronize clocks; run quarterly reviews to find gaps.

Actions 1–5 · continued →

6 Maintain offline, immutable backups & test restoration

Backups are targeted early in intrusions; resilience depends on isolation and tested recovery. Follow the 3-2-1 rule (one copy offline and immutable); secure backup platforms with separate admin accounts; define recovery requirements; test restorations and measure recovery time.

7 Protect internet-facing systems and services

Unnecessary exposure creates low-effort entry points. Maintain a list of all internet-reachable systems with owners; remove unnecessary exposure and require authenticated gateways; use brokered access instead of direct RDP; regularly scan public IP space.

8 Strengthen email authentication & content protections

Email remains a favored initial access vector. Publish and enforce DMARC, SPF, and DKIM; progress DMARC from monitor to quarantine to reject; quarantine high-risk attachments and block internet-sourced macros; enable time-of-click link protection.

9 Reduce administrator privileges

Broad, persistent admin access enables rapid escalation. Minimize admin accounts; require just-in-time admin access from secured devices; restrict where admin logins are permitted; monitor privilege changes; remove local admin rights with expiring exceptions.

10 Exercise your incident response plan with stakeholders

Practiced organizations respond faster and reduce impact. Maintain a concise IR playbook defining roles and decision authority; run a focused 60-minute tabletop quarterly with technical, legal, comms, operations, and leadership teams; include law enforcement contacts such as your local FBI field office.

Reproduced from the FBI's Operation Winter Shield "Ten Actions to Improve Cyber Resilience" handout.