Cyber AI Profile Workshop #2 – January 14, 9:00 AM – 5:00 PM EST

Morning Sessions (in-person and online)

Time	Topic	Location	Speaker(s)
8:30 – 9:00	Arrival and Check-in		N/A
9:00 – 9:10	Welcome and Opening Remarks	Room 1H220 + livestream	Cherilyn Pascoe, NIST
9:10 – 9:30	About the Cyber AI Profile Project and Workshop #2	Room 1H220 + livestream	Katerina Megas, NIST
9:30 - 10:30	Panel: AI and Cybersecurity Projects at NIST • AI Risk Management Framework (AI RMF) • Center for AI Standards and Innovation (CAISI) • Adversarial Machine Learning • Dioptra • Secure Software Development Framework (SSDF) AI Profile • PETs Test Bed • DevSecOps • Agent Identities • NCCoE Chatbot	Room 1H220 + livestream	Moderator: Barbara Cuthill, NIST Panelists: • Martin Stanley, NIST • Maia Hamin, NIST • Apostol Vassilev, NIST • Harold Booth, NIST • Gary Howarth, NIST • Michael Ogata, NIST • Ryan Galluzzo, NIST • Daniel Lee, MITRE/NIST NCCoE
10:30 – 10:45	Networking Break		N/A
10:45 – 11:00	AI Accelerators	Room 1H220 + livestream	Craig Schlenoff
11:00 – 11:30	Overview of the Cyber AI Profile Preliminary Draft	Room 1H220 + livestream	Julie Snyder, MITRE
11:30 – 11:50	Control Overlays for Securing AI Systems (COSAiS)	Room 1H220 + livestream	Victoria Pillitteri, NIST
11:50 – 12:00	Morning Wrap-up and Afternoon Breakout Session Plans	Room 1H220 + livestream	Katerina Megas, NIST
12:00 - 1:00	Lunch (On Your Own – MITRE Cafeteria)		N/A

Overview of Afternoon Breakout Session Tracks (see map on the next page for room locations)

The breakout sessions provide an opportunity for participants to share insights and feedback to inform the next version of the Cyber AI Profile. Participants will rotate to complete three of the four sessions.

- **Track A – Secure Focus Area:** The Secure Focus Area supplements existing cybersecurity and risk management best practices to address novel, expanded, and altered attack surfaces associated with the integration of AI systems into an organization, its ecosystems, and its infrastructure. This covers the AI systems themselves, their supply chains, including data and machine learning infrastructure, and the other systems and data that the AI system relies on. The purpose of this track is to review Secure Focus Area content presented in the Cyber AI Profile preliminary draft and discuss feedback for creating the final version of this section.
  Presenter: *Noah Schiro, MITRE,* ***Facilitator:*** *Christina Sames, MITRE*

- **Track B – Defend Focus Area:** The Defend Focus Area concentrates on identifying opportunities for the use of AI in supporting cybersecurity processes and activities and understanding the challenges that come with leveraging AI to assist in defensive operations. Opportunities to enhance cyber defense capabilities using AI include mission assurance, predictive and proactive applications, investigation and analysis, and response and remediation. The purpose of this track is to review Defend Focus Area content presented in the Cyber AI Profile preliminary draft and discuss feedback for creating the final version of this section.
  Presenter: *Keith Manville, MITRE,* ***Facilitator:*** *Jonathan Keisler, MITRE*

- **Track C – Thwart Focus Area:** The Thwart Focus Area addresses how AI can enhance adversary capabilities, how these attacks could impact the entire cybersecurity landscape, and what organizations can do to bolster their systems against these emerging threats. The purpose of this track is to review Thwart Focus Area content presented in the Cyber AI Profile preliminary draft and discuss feedback for creating the final version of this section.
  Presenter: *Marissa Dotter, MITRE,* ***Facilitator:*** *John Dombrowski*

- **Track D – COSAiS:** NIST is developing a series of NIST SP 800-53 Control Overlays for Securing AI Systems (COSAiS). To facilitate discussion during this breakout track, NIST recently released an annotated outline (discussion draft) of Control Overlays for Securing AI Systems: Using and Fine-Tuning Predictive AI. Discussions during this breakout session, along with comments on the outline, will inform a series of NIST Interagency Reports (IR) regarding COSAiS.
  Presenter: *Vicky Pillitteri, NIST,* ***Facilitator:*** *Alicia Dawson, MITRE*

	Topic	Location
1:00 - 2:05	Breakout Sessions – Round #1: • A: Secure Focus Area • B: Defend Focus Area • C: Thwart Focus Area • D: COSAiS	A: 1H220 B: 1H300 C: 1H280 D: 1H301
2:05 - 2:15	Transition/Break	
2:15 - 3:20	Breakout Sessions – Round #2: • A: Secure Focus Area • B: Defend Focus Area • C: Thwart Focus Area • D: COSAiS	A: 1H220 B: 1H300 C: 1H280 D: 1H301
3:20 - 3:30	Transition/Break	
3:30 - 4:35	Breakout Sessions – Round #3: • A: Secure Focus Area • B: Defend Focus Area • C: Thwart Focus Area • D: COSAiS	A: 1H220 B: 1H300 C: 1H280 D: 1H301
4:35 - 4:40	Transition	
4:40 - 5:00	Close-out • Breakout session readouts • Next steps	1H220

Map of Breakout Session Track Locations