

2023
**CHEMICAL
SECURITY
SUMMIT**

August 29-31, 2023

[#ChemicalSecurity](#)



CHEMICAL SECURITY SUMMIT

August 30, 2023

Artificial Intelligence and Advancing Technology

Dr. Sean Warnick

Senior Technical Advisor and Advanced Computing SME
Technology Center, Science and Technology Directorate, DHS

Dr. Erin Walsh

Chief, Risk Management Planning Branch
National Risk Management Center (NRMCC), CISA

Dr. Ryan Donaghy

Associate Director (Acting)
Planning and Innovation, Infrastructure Security, CISA

Moderator: Dr. Erika McClure

Policy Analyst, Policy, Rulemaking, and Engagement Branch
CISA Chemical Security



#ChemicalSecurity

ARTIFICIAL INTELLIGENCE: NATIONAL LEVEL POLICY AND CISA LINES OF EFFORT

AUGUST 2023



Agenda

1. **Environment:** National Policy; Strategy Development
2. **AI Security:** Taxonomy
3. **CISA Perspective:** AI Challenges
4. **Current CISA Activities on AI:** Lines of Effort



Environment: National Policy

Recent policy developments highlight AI as an administration and congressional priority; CISA will play an important coordinating role.

National AI Initiative (NAII) Act of 2020:

Coordinated complementary AI R&D, demonstration activities among FCEB, DOD, IC.

AI in Government Act of 2020:

Established the AI Center of Excellence within GSA.



EO 13859: Maintaining American Leadership in AI (2019): Established federal principles and strategies to strengthen the nation's capabilities in AI.

EO 13960: Promoting the Use of Trustworthy AI in the Federal Gov't (2020): Required Agencies to inventory and share AI use cases.

EO 14067: Federal Policy on Ensuring Responsible Development of Digital Assets (2022): Requires systemic risk evaluations for digital (financial) assets.



Environment: AI Strategy Development

CISA is developing an AI strategy while contributing to interagency efforts.

DHS AI Strategy: Strategic vision for DHS role in policy development, governance, use of AI, and risk mitigation.



Implementation Plan for a National AI Research

Resource: Memorializes findings of National Artificial Intelligence Research Resource (NAIRR) Task Force on national AI research infrastructure.



OGA Strategies: FDA, Nuclear Regulatory Commission, and others have released AI strategies tailored to specific mission areas.

National Priorities for AI RFI: OSTP RFI on key themes to inform Administration's updated National AI Strategy.



CISA Perspective on AI Challenges

- **AI technologies are ubiquitous in information systems and are continuing to evolve in ways that will transform society...**
...their evolution will have predictable and unpredictable implications on multiple aspects of the CISA mission.
- **Security issues around AI are, in most cases, extensions of existing cybersecurity challenges facing the U.S....**
...which is why our AI efforts should be integrated into existing programs, to the maximum extent practical.
- **Addressing these challenges could require a significant long-term investment by CISA...**
...so the sooner we identify key outcomes the better we can plan for the future.



AI Security Taxonomy

AI Security is an umbrella term used for several different categories of cybersecurity.

Three Key Categories of AI Security:

- 1. Applications of AI for Cybersecurity:** CISA is actively leveraging AI and ML tools for threat detection, prevention, and vulnerability assessments.
- 2. Cybersecurity of AI-Enabled Systems:** CISA currently has limited ability to protect and secure AI-enabled systems outside of traditional cybersecurity.
- 3. Threats from Adversarial Use of AI:** CISA needs to research (via S&T), develop and/or acquire tools to actively to protect from adversarial threats across the Federal Civilian Executive Branch Agencies and critical infrastructure.



CISA Lines of Effort (LOEs): Overview

LOE 1:

**Responsibly Use
AI to Support our
Mission**

LOE 2:

**Assure AI
Systems**

LOE 3:

**Protect Critical
Infrastructure
from Adversary
Use of AI**

LOE 4:

**Contribute to
DHS-led and
Interagency
Processes on AI**

LOE 5:

**Expand AI
Expertise in our
Workforce**



