

## 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 (NRMC), 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



# ARTIFICIAL INTELLIGENCE: NATIONAL LEVEL POLICY AND CISA LINES OF EFFORT

AUGUST 2023



## Agenda

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



### **Environment: National Policy**

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

#### National Al Initiative (NAII) Act of 2020:

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



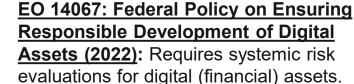
EO 13859: Maintaining American
Leadership in Al (2019): Established
federal principles and strategies to
strengthen the nation's capabilities in Al.

#### Al in Government Act of 2020:

Established the Al Center of Excellence within GSA.



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





## **Environment: Al Strategy Development**

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

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

Implementation Plan for a

findings of National Artificial

Resource (NAIRR) Task Force

**National Al Research** 

Intelligence Research

on national AI research

**Resource:** Memorializes



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.



infrastructure.

## **CISA Perspective on AI Challenges**

- Al 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 Al 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.

## **Al Security Taxonomy**

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

#### **Three Key Categories of Al Security:**

- 1. Applications of Al for Cybersecurity: CISA is actively leveraging Al and ML tools for threat detection, prevention, and vulnerability assessments.
- 2. Cybersecurity of Al-Enabled Systems: CISA currently has limited ability to protect and secure Al-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 Al to Support our Mission **LOE 2:** 

Assure Al Systems

**LOE 3**:

Protect Critical Infrastructure from Adversary Use of Al **LOE 4**:

Contribute to DHS-led and Interagency Processes on Al

**LOE 5**:

Expand Al
Expertise in our
Workforce



