CISA PRESENTATION FOR NIST SECURE SOFTWARE DEVELOPMENT WORKSHOP FOR GENERATIVE AI

- Jonathan (Jono) Spring
- Martin Stanley

CISA Secure AI

- CISA recently published an agency AI Roadmap with five Lines of Effort:
  - **LINE OF EFFORT 1: Responsibly use AI to support our mission**
  - **LINE OF EFFORT 2: Assure AI systems**
  - **LINE OF EFFORT 3: Protect critical infrastructure from malicious use of AI**
  - **LINE OF EFFORT 4: Collaborate with and communicate on key AI efforts with the interagency, international partners and the public**
  - **LINE OF EFFORT 5: Expand AI expertise in our workforce**
- Updates to the SSDF are supportive of these efforts as well as specific initiatives related to secure software

Generative AI is Software – Recent CISA Efforts

- Under EO 14028 CISA recently completed the comment period (12/18/23) on updates to the self-attestation on SSDF which applies for entities providing services to the federal government.
  - Request for Comment on Secure Software Development Attestation Common Form | CISA

- Guidance recently issued in coordination with the UK, CISA, and 21 other partner agencies provides a baseline for a common approach.
  - CISA and UK NCSC Unveil Joint Guidelines for Secure AI System Development | CISA

Secure Software Development Attestation Common Form Update

- EO 14028 - *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*
- Based on NIST SSDF (SP) 800-218v1.1
- Updates to the SSDF for GenAI should be incorporated into the Common Form Update

Jonathan Spring
January 17, 2024

CISA and Partner Nation Guidelines for Secure AI Development

- Co-sealed by 23 domestic and international cybersecurity organizations, this publication marks a significant step in addressing the intersection of artificial intelligence (AI), cybersecurity, and critical infrastructure.
  - https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development
- Emphasis on supporting Secure by Design Principles.
  - With the October 2023 Secure by Design document, CISA and 17 partner organizations explicitly put AI in the scope of Secure by Design
  - Secure by Design | CISA

Jonathan Spring
January 17, 2024


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA