# Unmasking AI-Powered Deception: Staying Safe in a Fake Reality

Cybersecurity Awareness Month 2025 Video

National Nuclear Security Administration

The Office of the Associate Administrator
for Information Management and
Chief Information Officer

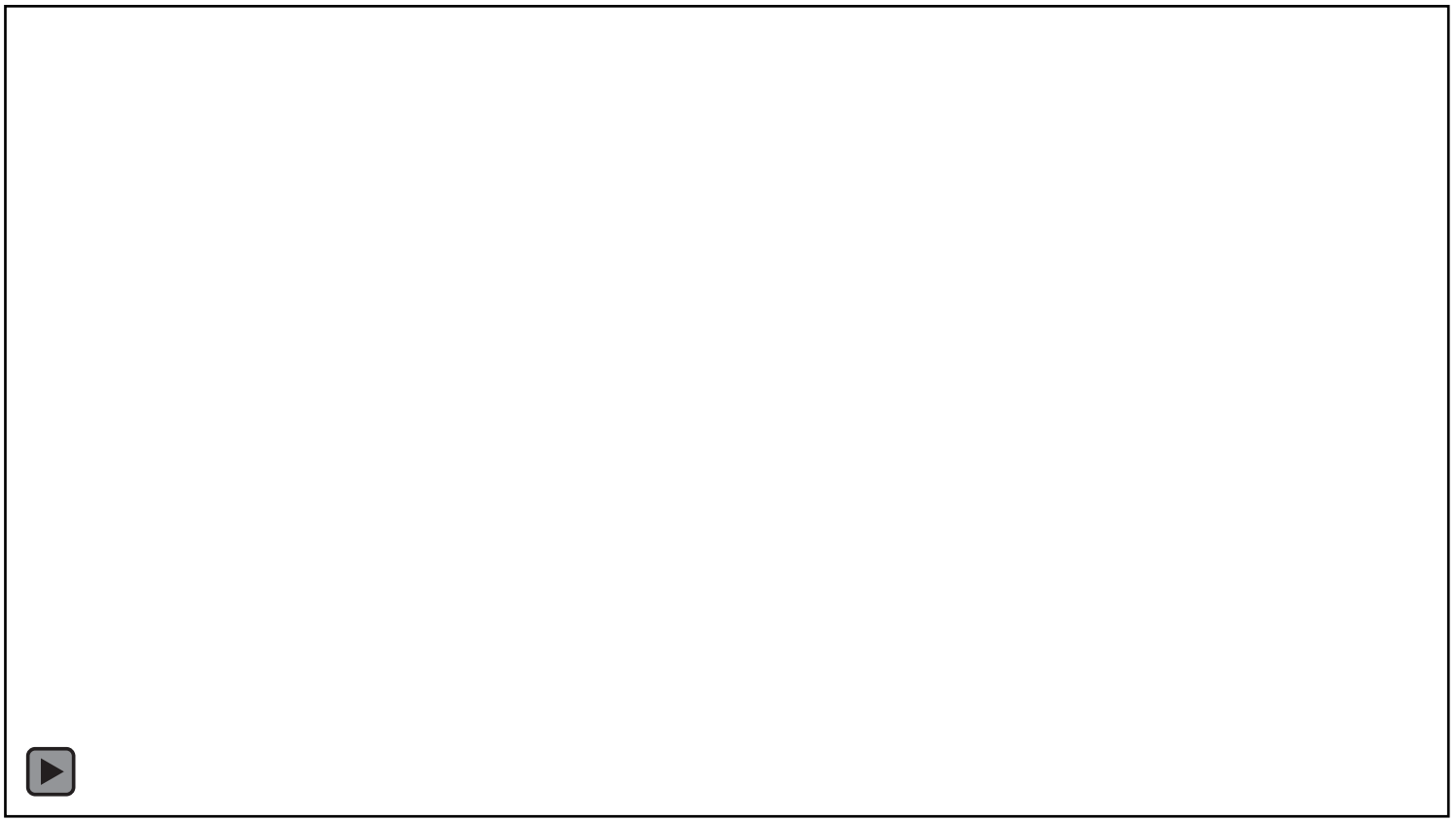
# The Problem: Cybercrime's New Frontier

- **Beyond Systems:** Cyber criminals are increasingly "hacking people," targeting human vulnerabilities rather than just technical flaws.
- **AI-Driven Sophistication**: Threats are now personalized, highly persuasive, and generated by AI – making them incredibly difficult to detect.
- **Voice Cloning & Deepfakes:** Familiar voices (e.g., from leadership) can be cloned with AI, creating urgent, false requests that bypass traditional trust.
- **Flawless Phishing:** AI generates near-perfect email messages, leveraging personal information, rendering old phishing red flags obsolete.
- **Critical Risk:** This "fake reality" poses a significant and immediate risk to organizational security, data integrity, and national interests.

# Our Solution:
# Dynamic Threat, Dynamic Response

- **Targeted Awareness:** For Cybersecurity Awareness Month 2025, we created an engaging video to directly confront the rising wave of AI-powered deception.
- **Why Video?** Multimedia allows us to vividly demonstrate complex threats (like voice cloning) and provide immediate, memorable guidance, far beyond static text.
- **Empowering Action:** The video isn't just about identifying threats; it's about equipping our federal workforce with actionable strategies to defend against them.
- **Clear Call to Vigilance:** Our message is direct: "Stay vigilant, stay skeptical, stay CyberSecure, and together we can protect what's real for our organization and our nation.

# Experience the Solution



# Learn More & Connect

- **Program Inquiries:** For further details on this cybersecurity awareness campaign or other initiatives, please contact the NA-IM Training Team at NA-IMTraining@nnsa.doe.gov