Record	15
Presentation Title:	**Impact of AI Generated Media on Homeland Security**
Type of Presentation	Single Presenter
Intended Audience	All Conference Attendees Cybersecurity/IT Professionals Law Enforcement
Presentation Abstract	As technology improves, deepfakes and AI generated content are becoming more accessible and realistic while barriers to creation are lowering. Spreading disinformation, particularly about current events and politics, has become a popular use for deepfakes, making it easier than ever to manipulate public opinion in the modern age of social media. We created authentic content and, using open-source software, deepfake content in video and audio form. We carefully controlled timing, messaging, and demographics to ensure data integrity. A total of 244 subjects participated, with 40 attending in-person for biometric data collection using tools at the SMARTLab, specifically eye-tracking and emotion recognition.Participants rated credibility, persuasiveness, and trustworthiness with no statistical difference between synthetic and authentic media. Our findings also indicated that deepfakes are difficult to detect. We've found that deepfakes can quietly shape public opinion without raising many questions. Misinformation is no longer confined to traditional propagandists or media manipulators; it can now be created and spread by anyone with an internet connection.
Indicate up to 3 learning objectives that will be presented:	1.) AI Deepfakes 2.) Misinformation 3.) Election Security
Speaker Name:	Brandon Amacher
Speaker Title:	Director
Speaker Organization Name:	Utah Valley University, Emerging Tech Policy Lab
Speaker Bio	**Brandon Amacher** Brandon Amacher is the director of the Emerging Tech Policy Lab for the Intermountain Intelligence and Industry Consortium (I3SC) and an instructor at the UVU Center for National Security Studies, where he teaches cybersecurity policy, advanced tech security policy, and cyberwarfare. Brandon comes from a background in the private sector, where he worked as a cyber intelligence analyst and a strategic consultant for various leading cybersecurity organizations, including FireEye and Mandiant. Brandon's areas of expertise include

	nation-state cyber operations, advanced persistent threats, artificial intelligence, security policy, intellectual property theft, the internet of things, and quantum information sciences.