AGENDA

2025 Day of Information Sharing
June 12, 2025

8:15	Doors Open Registration, Displays, FBI Store, Continental breakfast
9:00	WELCOME, OPENING REMARKS
9:15	KEYNOTE SPEAKER: Mike Driscoll *"National Security Today: Threats, Regulations, and the Role of Executives"*
10:15	Break
10:30	KEYNOTE SPEAKER: Jennifer Williams *"United States v. Khalid: Prosecuting a teenage terror conspirator"*
11:25	Break
11:40	KEYNOTE SPEAKER: Rob Petrosino ***"**Mitigating Risks When Implementing Artificial Intelligence**"***
12:35	Lunch
1:35	KEYNOTE SPEAKER: Carlos Garcia *"Welcome to 1984: Bored Teenagers with Nation-State Capabilities"*
2:35	Break
2:45	BREAKOUT SESSIONS Sunny Notani – *"Fighting the Worst Online Scams"* Eric Robuck – "*Inside the Perimeter: Advanced OSINT on Corporate Targets"*
3:40	Break
3:50	BREAKOUT SESSIONS Eric Patterson – *"Inside the Minds of Persons of Interest"* Alex Fuchs – "*A secure by design architecture to combat the Cyber Threat Landscape"*
4:50	Adjourn

All times approximate; agenda subject to change

ABSTRACTS/BIOS

National Security Today: Threats, Regulations, and the Role of Leaders

Get ready for a candid assessment of today's escalating national security threats, including cyber attacks and supply chain vulnerabilities, that impact the private sector. Mike Driscoll will also examine recent regulatory changes and executive orders that mandate new national security and cybersecurity practices – and the crucial role business leaders must play to navigate this evolving landscape through proactive risk management and public-private collaboration.

Mike Driscoll served as the Assistant Director in Charge of the FBI's New York Field Office as well as Chief of the Violent Crimes Section (which leads the FBI's Crimes Against Children program), director of New York's Counterintelligence and Cyber Division – *and as Special Agent in Charge of the Philadelphia Field Office!* He became a special agent in 1996, and held several other posts including Assistant Legal Attaché in London and Special Agent in Charge of New York's Criminal Division.

He currently leads the National Security offering at FTI Consulting, where he advises on a range of issues including cyber attacks, insider threats, corporate espionage, CFIUS reviews, sanctions, cross-border data sharing and intellectual property. He ensures that organizations adhere to corresponding national security requirements and regulation and provides support for investigations, foreign direct investment reviews, and other regulatory enforcement actions when national security threats arise.

United States v. Khalid: Prosecuting a teenage terrorism conspirator

In 2011, the United States indicted the first-ever juvenile for terror-related crimes. Mohammad Hassan Khalid was excelling academically in high school and had been offered a full scholarship to Johns Hopkins University. But beginning at age 14, he was also secretly participating in a conspiracy to support Al Qaeda and fellow conspirator Colleen LaRose (better known as "Jihad Jane"). As the U.S. Attorney for Eastern Pennsylvania, Jennifer Arbittier Williams prosecuted Mr. Khalid and will present a case study about this fascinating and challenging investigation and prosecution. She will include details about techniques and hurdles unique to national security investigations, the charging strategy in this complex conspiracy, and the challenge of sentencing a national security defendant who would still be young when released from incarceration.

Jennifer Arbittier Williams is currently vice president of the InfraGard Philadelphia Board of Governors. She brings to us her experience as the United States Attorney for the Eastern District of Pennsylvania in 2021-2022, having previously served as Assistant and First Assistant U.S. Attorney for more than 18 years. She has received numerous awards, including the Anti-Defamation League's SHIELD Award and the Federal Trade Commission's National Criminal Liaison Award, recognizing her exceptional commitment to consumer protection in partnership. She has also been lauded for helping create and lead the Threat Intervention and Prevention Network (TIP Network), a public-private partnership that helps organizations assess and mitigate potential threats of targeted violence.

Ms. Williams is currently a Partner at Freeh Sporkin & Sullivan LLP, where her practice focuses on national security, global risk management, cyber security and compliance. She also serves as an Adjunct Professor at the University of Pennsylvania Carey Law School, where she teaches National Security Investigations and Prosecutions. She earned a B.A. in American History from the University of Pennsylvania in 1992 and her J.D. from the University of Pennsylvania Law School in 1995.

Mitigating Risks When Implementing Artificial Intelligence

As AI accelerates from a buzzword to a battlefield asset, its dual-use potential has never been more critical. In this session, Rob Petrosino dives deep into the practical, operational, and ethical risks associated with deploying AI in today's high-stakes environments. From deepfakes and disinformation campaigns to rogue shadow AI usage to large-scale automated cyberattacks, you'll gain a no-hype, real-world framework for identifying risks, designing governance models, and aligning cross-agency teams for safe and scalable adoption. Using examples pulled from defense, surveillance, and enterprise rollouts, Rob outlines the "Explore, Search, Test, Run" methodology — a structured and repeatable approach to reduce friction and increase trust in AI implementation. Whether you're exploring LLMs or already deploying smart surveillance, this session will equip you lead responsibly in an AI-first era.

Rob Petrosino is a distinguished digital innovation expert who serves as a Strategic Engagement Advisor for Artificial Intelligence at the FBI, focusing on AI's impact on national security. He is also Chief Innovation Officer at PeakActivity, where he leads initiatives in spatial computing, digital twins, generative AI and machine learning to drive innovation across sectors like retail, manufacturing, B2B and education. Rob has more than 10 years of experience guiding Fortune 100 companies and defense organizations through technological advancements. His insights have been featured in Forbes, and he has appeared on the Today Show, where he discussed the latest advancements in technology. Rob's passion for demystifying emerging technologies and transforming complex tech trends into actionable business strategies has made him a sought-after speaker who inspires organizations globally, positioning him as a leading voice in digital innovation.

Welcome to 1984: Bored Teenagers with Nation-State Capabilities

This session provides an exciting introduction to the field of Ubiquitous Technical Surveillance (UTS) – the collection and long-term retention of data. Carlos Garcia will introduce you to UTS-enabled adversaries, capabilities, vulnerabilities, and threat vectors through a series of real-world case studies and live technical demonstrations. You'll walk away with a better understanding of the degree to which nation-state capabilities are now available to motivated individuals with even limited technical skills. Carlos will demonstrate the democratization of advanced technology: "Yesterday's nation-state capability is today's YouTube tutorial."

Carlos Garcia is a former Olympic soccer team member and touring musician turned independent researcher and FBI supervisory special agent. A native of Central America, his journey into the tech space began in the days before the internet even existed. While in graduate school he was awarded a Graduate Assistance in Areas of National Need (GAANN) Doctoral Fellowship for his pioneering work in the field of computer science, which launched his career in public service. An academic by background, Carlos's professional experience extends far beyond labs and conference rooms. In fact, he has spent much of his career operating in unpredictable environments, managing and executing covert operations. He currently serves as one of the foremost globally recognized subject matter experts in the field of Ubiquitous Technical Surveillance.

Fighting the worst online scams

Sunny Notani provides an updated look at two of the most nefarious online scams – "Pig Butchering" and Business Email Compromise, with *reported* losses in the billions of dollars in just the past year. Using actual case studies, Sunny will show that despite repeated warnings, these frauds continue to grow – and measures the Secret Service is using to fight the trend.

Hari "Sunny" Notani has worked as a Special Agent for The United States Secret Service for 22 Years. He was initially assigned to the New York Field Office for eight years, specializing in Financial Institution Fraud, Electronic Crimes, Network Intrusions and Social Engineering. Special Agent Hotani was later assigned to the Vice Presidential l Protection Detail (VPD) for six-and-a-half years, during which he conducted over 20 high profile protection lead advances for the Vice President. He is currently a Supervisory Special Agent at the Secret Service's Philadelphia Field Office, managing the financial fraud division consisting of 15 Special Agents, and is the Program Manager for the Philadelphia Electronic Crimes Task Force.

Inside the Perimeter: Advanced OSINT on Corporate Targets

In today's threat landscape, understanding your adversaries—and even yourself—through open-source intelligence is critical. This session will focus on advanced techniques for collecting and analyzing publicly available information on organizations. Tailored for IT leaders protecting critical infrastructure and federal partners, the talk moves beyond tool overviews to demonstrate how OSINT can expose organizational vulnerabilities, support threat modeling, and enhance proactive defense. Learn how adversaries see your enterprise—and how to stay a step ahead.

Eric Robuck is founder and President of The Valander Group, where he and his team deliver cybersecurity solutions to business owners. He served as a Warrant Officer, focusing on information technology and security in the Army, Navy and Defense Department, focusing on complex cybersecurity challenges and strategies. Eric is a graduate of Kutztown University, with advanced study in cybersecurity and leadership at Duquesne University and Liberty University. In addition to his leadership of Valander, he is also Adjunct Professor of Computer Science and Cybersecurity at Alvernia University and is passionate about helping develop the next generation of cybersecurity professionals. His professional certifications are an alphabet soup that includes the CISSP, CEH, Security+ and AWS Practitioner.

Preventing Targeted Violence - Evolving Threats and Evolving Solutions

What motivates active shooters and terrorists to engage in an act of targeted violence? How can we help prevent those acts? Special Agent Eric Patterson (FBI) serves as the Threat Management Coordinator and the Community Anti-Threats Officer (CATO) Program Coordinator for FBI-Philadelphia. Eric and his colleagues have studied the psychology of persons of interest and the often-complex picture of their pathway to targeted violence. In this session, you'll gain fascinating insights into behavioral factors that lead to threats of targeted violence (physical and cyber) and how identifying these factors can actually prevent targeted acts of violence – an important aspect of our mission to protect our critical infrastructure, national security, and our most important asset, our people.

Eric R. Patterson is a Special Agent with the FBI in Philadelphia. He joined the FBI in 2002 and currently serves as Threat Management Coordinator for the FBI in Philadelphia, where he is responsible for designing and implementing the Preventing Targeted Violence Strategy. Special Agent Patterson serves as Coordinator for the FBI's Community Anti-Threats Officer (CATO) Program, which trains local, county, state and federal law enforcement officers on best practices for preventing targeted acts of violence. A member of the Pennsylvania Threat Assessment Steering Committee (PA-TASC), Special Agent Patterson also serves as Co-Coordinator for the Community Anti-Threat Team (CATT) Program, which provides best practices and training for multi-disciplinary Threat Assessment Threat Management (TATM) Teams throughout the Commonwealth of Pennsylvania.

Eric Patterson earned his B.A. degree in English from St. Joseph's University and his Master of Applied Positive Psychology from the University of Pennsylvania, and now serves as an Academic Advisor for that program. He also previously served as an Adjunct Professor at Penn State Harrisburg's Criminal Justice Program.

Adopting a secure by design architecture to combat the Cyber Threat Landscape

The Cyber Threat Landscape is getting increasingly more complex. Gartner predicts that we'll spend almost $220 billion this year alone) on cybersecurity measures. Yet, despite that, 50-70% of all breaches are still uncovered by someone outside of the affected organization – a sign that the growing complexity of attacks isn't a problem we can spend our way out of.

Alex Fuchs will address the importance of adopting a secure by design architectural approach, including:

- Assuming a breach and implement a strategy of Zero Trust
- Ensuring all sensitive data follows the principles of least privilege
- Performing proper east / west inspection of internal traffic to limit the spread of any malware
- Having a well-practiced incident response plan that is up to date
- Conducting post-incident debriefs and making changes based on lessons learned when appropriate
- Utilizing outside auditors to assess your environment

Alex Fuchs has more than a decade of experience managing diverse technology teams in verticals ranging from Retail to Healthcare. He currently serves as a Systems Engineer at Fortinet, where he supports Enterprise Customers. He previously served as vice president of IT at The Paper Store retail chain where he implemented Fortinet. In his most recent role, Alex deployed Fortinet's full network and security stack to more than 120 stores, plus multiple data centers. He is dedicated to helping organizations drive their secure digital transformation initiatives and while navigating the complexities of their cyber security practices.