2024 Agenda

Tuesday, November 5

1:0 0 p.m. - 5:00 p.m. Critical Infrastructure Tabletop (Jac k Voltaic - like)
Exercise Opening Presented by the AFCEA Atlanta Chapter President Paul Wertz
Exercise led by Klint Walker, Supervisory Cybersecurity Advisor - Region IV, Cybersecurity and Infrastructure Security Agency
Expected participating parties:

- Department of Homeland Security CISA
- Federal Bureau of Investigation
- FirstNet Authority
- U.S. Army
- U.S. Air Force
- Georgia National Guard
- Georgia Cyber Center of Excellence
- Georgia Tech Authority
- Georgia Emergency Management Agency
- The city of Atlanta's Office of Emergency Preparedness
- And more!

5:00 p.m. - 6:00 p.m. Networking Reception

Wednesday, November 6

7:30 a.m. - 5:00 p.m. Registration Open

8:00 a.m. – 8:15 p.m. Conference Opening and Welcome Speakers:
BG Paul Fredenburgh, USA (Ret.), Executive Vice President for National Security and Defense AFCEA International
Sebastian Barron, Metro Atlanta Representative, Office of Governor Kemp

8:15 a.m. - 8:45 a.m. City of Atlanta Welcome and Keynote Speaker:
City of Atlanta TBD

8:45 a.m. – 9:15 a.m. Keynote Speaker:
TBA

9:15 a.m. Exhibits open
Sessions:

LtCol Christopher Miles, USMC

National Defense: Embracing the Warrior's Mindset – Empowering individuals to take responsibility for the nation's security. From Global terrorism to emerging cyberthreats, collaboration and information sharing is more important than ever.

Tanya Simms, Chief of the Office of the National Manager within NSA's Cybersecurity Directorate

Latest priorities and initiatives from the White House. Empowered by the White House for National Security Systems Accountability, the Office of the National Manager (ONM) for National Security Systems (NSS) exercises presidential authority by issuing guidance and mitigations for critical cyber threats and vulnerabilities to NSS owners and operators. ONM guidance supports not only critical mission execution but also resilience.

John Clements, Homeland Defense and Security Information Analysis Center

Misinformation and disinformation have been leveraged by bad actors widely. Just as importantly, our own poor communication has hampered our ability to mitigate consequences at important times. We will examine some historical failures, as well as successes, in emergency public communication. Exploring newer methods of mass communication, such as targeting specific groups through social media platforms for public health concerns. It will attempt to bust some of the myths of the "mob mentality" and educate on specific programs for secure communication.

Joseph Friar, Cybersecurity and Information Systems Information Analysis Center (CSIAC)

Extended reality (XR) is an all-encompassing term that groups three similar technologies: (1) virtual reality (VR), (2) augmented reality (AR), and (3) mixed reality (MR). XR has been in development in the U.S. Department of Defense (DoD) since the late 1960s, and this transformative technology has already made an impact across the DoD and holds considerable potential for Homeland Security.

Shane M. Barney Chief Information Security Officer, USCIS Office of Information Technology / Management Directorate

How Generative AI and curated Large Language Models (LLM) are impacting U.S. Citizenship and Immigration Services - will explore several key topics, including the development, applications, ethical considerations, and future directions of these technologies.

5:0 0 p.m. - 6:0 0 p.m. | Networking Reception

Thursday, November 7

7:30 a.m. - 5:00 p.m. Registration Open
8:00 a.m. – 8:15 p.m. Conference Opening and Welcome Speakers

Sessions are still being refined, with times to be assigned soon.

Dr. Scott Fisher, Major, US Army Reserve, is special projects officer for the 151st Theater Information Operations Group

Find It, Vet It, Share It: Effective Open-Source Information Sharing - Information sharing, especially during a crisis, features three main challenges: collecting relevant data, vetting the data for authenticity and applicability, and then getting relevant data into the hands of those who need it as quickly and effectively as possible. Using lessons learned while serving at US European Command during Russia's 2022 invasion of Ukraine, this presentation discusses the needs and requirements for a platform capable of swiftly and effectively sharing open-source data during a crisis.

Dr. Rigoberto Garcia, Cloud and Security Architect

AI-Enhanced Drones for Long-Distance Reconnaissance: A New Paradigm in Surveillance Technology – integration of advanced artificial intelligence (AI) algorithms in drone technology to revolutionize long distance reconnaissance missions. By implementing deep learning and computer vision techniques, drones are now capable of autonomous navigation in challenging terrains and environments. The integration of AI in drone technology signifies a substantial leap in surveillance capabilities, particularly for border security and monitoring remote areas.

Dr. Tim Lunn, Partner PA Consulting,

Scalable implementation of data verification in hardware and software - Transferring data between networks of different trust levels requires a cross-domain solution to preserve the security and integrity of the more-trusted network. Some examples include importing sensor data from an OT network into a centralized monitoring location or importing log files into your security operations center. Architecture designed to be secure and scalable is needed. This architecture will enable the secure import of the above-mentioned data, and allow organizations to use that data to improve their security posture, make informed decisions, and optimize their processes

Marcus D. Hall, Amazon Senior Regional IT Manager

A look at how supply chain logistics play a key role in supporting Critical Infrastructure. From disaster response to emergency support we look at what's going on in the big picture.

Tara Dean, CompTIA Sr. Account Director

With direction from the White House to focus on skills-based hiring to build the cybersecurity workforce. The question becomes, what frameworks can you use to then build appropriate education pathways? We will focus on two key frameworks: The NICE Framework, and the Defense Cybersecurity Workforce Framework (DCWF). Both frameworks are useful and have received recent updates. Join us to learn about how to map appropriate work roles to your workforce and understanding the ins and outs of using appropriate frameworks.

Ken Riordan, Principal Architect, Nokia Federal Solutions

Enabling Homeland Security with Private 5G - there are times and locations when public networks cannot reliably satisfy mission requirements. Furthermore, these same unreliable situations are often encountered when the need for effective team communications is most vital. Whether responding to a natural disaster which has crippled communications infrastructure or operating in remote areas to secure our nation's borders, the need for secure, reliable, and rapidly deployable networks is of paramount importance. On the one hand, we have a critical need for resilient communications in remote areas and emergency situations. On the other, we see an ever-increasing volume of data. At the intersection of these two trends lies an opportunity: Private 5G.

Matt Wilson, Prisma Cloud Solutions Architect with Palo Alto Networks

Securing Federal Agency Multi-Cloud Environments with Comprehensive Cloud Security Platforms - requires a comprehensive and cohesive approach to manage and mitigate risks across diverse cloud platforms. Modern cloud security platforms offer an integrated set of features to address these unique challenges, providing robust protection and ensuring compliance with federal regulations.

Nick Summers, founder and CEO of ComplAi Inc.

Data-First Approach to Sensitive Information and Cybersecurity Compliance - how AI can help organizations transform sensitive information, achieve faster compliance, and maintain security while allowing the continued use of non-compliant assets and applications without business disruption or significant architectural changes. A data-first approach offers detailed visibility into the types of sensitive information a company owns, holds, controls, and uses. A data-first delivery methodology is comprehensive and easy to implement through a 4-step process discussed in this session.

Kevin E. Greene, CTO OpenText

Hunt or Be Hunted - The Keys to Disrupting Threat Actors Activities - Cyberattacks have accelerated and given threat actors an unfair advantage in achieving their tactics. Shifting the balance with responsive cyber defense provides active/actionable threat intelligence by leveraging adversary signals and early warning capabilities to disrupt threat actors' activities. These signals and early warnings are known as Warnings of Attack (WoA) and Warnings of Compromise (WoC) and are foundational for formalizing proactive threat hunting, which allow organizations to hunt for signals associated with threat actors' behaviors and activities, and not IoCs.

Robert Marcoux, Principal Security Architect, Secure AI

Evaluating and Deployment of Emerging Technologies (AI) Enterprises increasingly turn to Machine Learning (ML) and Artificial Intelligence (AI) to address sophisticated cybersecurity challenges. This talk explores the hurdles in achieving consistent fidelity with ML and AI in cybersecurity applications. While ML and AI offer powerful tools for cybersecurity, their deployment requires careful consideration of data integrity, adversary tactics, and the capabilities of internal response teams.

Vic Macias Vice President of National Strategy, TeamWorx Security.

A moderated discussion panel for Discuss how collaboration and leveraging their unique authorities can fortify US critical infrastructure defenses, enhance cyber incident response, and prevent cybercrime. Key topics include: Each organization's authorities and how combined efforts amplify their impact. - Real-world examples showcasing the power of collaboration. - Proactive measures against evolving cyber threats, including information sharing with foreign partners.

Matt Shea Chief Strategy Officer of MixMode AI

Novel Cyber Attacks are 80% of the successful attacks and the most damaging, doing Trillions of dollars in damage. Advancing the real-time detection of them is paramount to homeland security. The scientific method used to advance that understanding ran into ˜unsolvable problems" when addressing the now famous 3 Body Problem, recently covered in the Netflix series and sci-fi novels of the same name. Similarly, the detection of forthcoming novel nation state attacks are also believed to be ˜unsolvable" with current technology. This talk will cover the history of these advancements and explore recent breakthroughs in Dynamical Systems for powering context aware and DARPA defined Third Wave AI.

Adam Maruyama Field CTO for Garrison Technology

Can you distinguish an email from your Director from one written by AI? Can you tell a capital I from a lower-case l? Administrators can apply a combination of isolation controls that prevent inadvertent execution of malicious webcode and security indicators that let users know that they are in a higher risk environment than expected. As open Internet access becomes increasingly critical to gaining the information advantage in a connected world and fulfilling citizens' service requests, it's critical that homeland secure organizations take an empowering rather than punitive approach to phishing protection.

Erik Little Senior Vice President of Replenishment Operations at Cencora

Building Resilience and Equity: State Preparedness for Disasters through Pharmaceutical Reserve Programs In this session we will explore the critical role of pharmaceutical reserve programs in disaster preparedness and promoting health equity. We will engage in an informative conversation that highlights effective state preparedness strategies while ensuring equitable access to vital medications during disasters. The role of diversity, equity, and inclusion in shaping resilient pharmaceutical reserve strategies.

John Dunn Senior Solutions Architect, CACI

Enabling mission agility through commercial solutions for classified (CSfC) mobile access Government agencies have experienced a sharp increase in requirements for employees to work from home, or in disparate facilities. While remote work might be a new concern, securely extending network access to users has been a long-standing challenge. What if a minimal investment in a CSfC distribution back-bone, compared to the significant costs and manhours spent to maintain current stove-piped networks, was applied across a small community of interest (COI)? Such a pursuit could facilitate and enable classified data communications to almost any need in the federal government. During this technical presentation we intend to explore the concept of a next generation Access-As-a-Service to Classified Data to fill communications gaps in the future.

Lee Koepping Chief Technologist for ScienceLogic

In today's rapidly evolving technological landscape, the convergence of emerging technologies is revolutionizing how we approach IT Operations (ITOps). The advent of Generative AI stands out as a transformative force. This talk will explore integration with other cutting-edge technologies and their potential impact on the Department of Homeland Security. Enhance cybersecurity measures by simulating potential threats and developing robust defense mechanisms. Artificial Intelligence in ITOps (AIOps) Beyond Generative AI, the broader scope of AI encompasses machine learning, neural networks, and deep learning. Enabling automation for further reduced MTTR and unlocking the potential for self-healing. Generative AI, in tandem with these emerging technologies, holds immense potential to revolutionize ITOps. For the Department of Homeland Security, adopting these advancements can lead to enhanced operational efficiency, improved security, and better resource management.

Kyle Fox, CTO of SOSi

Chinese Smart Cities and the PRC’s Dream of Global Surveillance. This brief describes the People’s Republic of China’s (PRC’s) promotion of smart cities technologies to compete in ˜the global race toward building an intelligent and data-driven society” and to advance its goals for digital mass surveillance capabilities. The presentation discusses the PRC’s smart cities development both at a policy and operational level, describe PRC assessments of progress (or lack thereof) in their smart cities development, and highlight the potential risks to personal security and national security that these efforts pose to individuals and critical infrastructure around the world.

Chris Gogoel, VP and GM Public Sector Quokka.io

What's Lurking in Your Phone? Navigating the Risks in Mobile Apps? Where does that file scanning app actually share my PDFs? Does that new game your kid downloaded harvest more info than their high score? As cyber threats continue to evolve and mobile usage continues to increase, a robust and proactive security approach is essential. This presentation delves into the unique challenges of mobile app security, shedding light on the various ways in which mobile apps can intentionally or unintentionally expose sensitive information. Attendees will hear real world examples of security risks discovered in mobile apps and gain actionable insights and best practices for app vetting.

Andrew Whelchel, (CISSP-ISSAP, ISSEP, CCSP, CGRC, CSSLP) Lead Solution Engineering, Saviynt

Generative AI, like machine learning and other AI models, depend on untampered data and assured access to ensure outcomes meet the needs of the mission. Identity security when aligning with AI tools and data ensures the training data, models and response outcomes operate with reduced risk for the mission. This session enables attendees to leverage zero standing privilege for AI environments to reduce risk, provide speed of access via governed service agent access and provide insider threat mitigation.

Panels and Special Sessions

Shivaji Sengupta, Board Member and Chair, Innovative Technology Subcommittee, AFCEA International; Founder and CEO, NXTKey Corporation Speaker

Exploring Acquisition Trends for State and Local Government

Smart Cities Panel composed of Atlanta Regional Smart Cities Officials

Smart cities use technology with a new approach to urban development. Here we will address how the integration of smart technologies into many homeland security areas, reduces risk and helps teams respond to threats. Connected infrastructure, will use data analytics, and real-time monitoring to improve response to threats, from natural disasters to cyber-attacks and terrorism.

A Word from the Contracting Officers

A panel of local contracting officers discussing the current contracting environment. Issues, protests, RFIs/RFPs, and fulfilling the contracts.

HSWERX

One of the newest incubators is getting the word out and discussing how it relies on Innovators to help solve some of DHS's most challenging problem sets. We will discuss ways to get involved and where we need help.

Small Business Innovation Research Program - Department of Homeland Security

A program specifically designed to address the needs of the Department of Homeland Security the SBIR program encourages U.S. small businesses with fewer than 500 employees to provide quality research and to develop new processes, products and technologies in support of the missions of the U.S. government. What are the hot issues?

Small Business Matchmaking

A highly anticipated follow up from last year's successful matchmaking event, this year it will be bigger and better!

NASA's SEWP Trajectory

Since 2015, with 147 companies, more than $60 billion in contracts, what are the ingredients that make this GWAC (Government Wide Acquisition Contract), so successful and what is the recipe for the next steps?

Adjourn