

EVENT SCHEDULE

TIME SLOT	SESSION TITLE AND PRESENTER
9:00 AM to 9:20 AM	Welcome Remarks Lara Luetkehans, Steven Hovan, Timothy Flowers, Waleed Farag - Indiana University of PA
9:20 AM to 10:00 AM	The Navy Innovation Ecosystem Joey Mathews - US Naval Research Laboratory
10:05 AM to 10:45 AM	Cybersecurity Careers Start Here: HUBZone, CMMC, and the Talent Pipeline Christina Hunt - Cinteot
10:50 AM to 11:30 AM	AI, Digital Competencies, and Societal Resilience: The Human Factor in Cybersecurity Joseph Squillace - Penn State, Roland Kelemen - Széchenyi István University
11:35 AM to 12:05 PM	Department of War Cyber Service Academy Alice Smitley - DoW Chief Information Officer's Workforce Innovation Directorate
12:05 PM to 1:05 PM	Lunch Break
1:05 PM to 1:15 PM	President's Remarks Michael Driscoll - Indiana University of PA
1:15 PM to 2:00 PM	Skills-Based Hiring Matt Isnor - DoW Cyber Workforce Development
2:10 PM to 2:55 PM	Nobody Cares About Cybersecurity...Until Everything Stops Joe Harford - Reclamere
3:05 PM to 3:50 PM	Microsoft-native Security Operations, Modern Attack Patterns, and Practical Career Pathways into SOC Work Mike Frank, Nick Christine - Forsyte IT Solutions
3:50 PM to 4:00 PM	Closing Remarks Waleed Farag - Indiana University of PA

ABOUT CYBERSECURITY DAT AT IUP

Each year since 2008, the IUP Institute for Cybersecurity in conjunction with IT Support, has hosted Cybersecurity Day during the month of October to celebrate National Cybersecurity Awareness Month.

Nationally recognized security experts from government, academia, and industry are invited to present technical, or employment-focused topics to students, faculty, staff, and the community. Topics in previous years include incident response, cyber crime, cyber forensics, machine learning, privacy, current cybersecurity challenges, and many more.

Cybersecurity Day at IUP is always free and open to the public, and all are invited to attend.

For complete details on previous Cybersecurity Day activities, visit bit.ly/IUP-CSDAY

Please contact Dr. Waleed Farag, Director, Institute for Cybersecurity, at farag@iup.edu with questions.

2026 CYBERSECURITY DAY SPONSORS

The 19th Annual Cybersecurity Day is proudly sponsored by PC4A and the IUP Institute for Cybersecurity



THE 19TH ANNUAL CYBERSECURITY DAY AT IUP

OCTOBER 13, 2026

HUB OHIO ROOM
IUP MAIN CAMPUS



PRESENTATION DETAILS & SPEAKER BIOS

Title: Microsoft-native Security Operations, Modern Attack Patterns, and Practical Career Pathways into SOC Work



Presented by: Mike Frank - Security Engineer, Fosite IT Solutions

Speaker Bio: Mike Frank is a Security Engineer at Forsyte IT Solutions, where he has spent nearly two years supporting approximately 30 clients across security configuration, compliance management, and cybersecurity best practices. Mike also engages with Forsyte's SOC across Tier 1, Tier 2, and Tier 3 responsibilities, supporting alert investigation, response, and client security operations. He holds a B.S. in Cybersecurity Management and Analytics from Virginia Tech.



Presented by: Nick Christine - Senior Account Executive, Forsyte IT Solutions

Speaker Bio: Nick Christine is a Senior Account Executive at Forsyte IT Solutions, supporting education and public-sector organizations across the Northeast. He brings more than 15 years of experience in enterprise account management, customer engagement, and consultative technology sales. Nick helps organizations connect Microsoft security, identity, data protection, and managed services to practical outcomes such as risk reduction, stronger operational resilience, and greater value from existing Microsoft investments.

Presentation Summary: This session is designed to help attendees understand how modern education environments are being attacked, how Microsoft-native security operations can reduce risk, and what practical steps students can take to prepare for security operations careers. The content is grounded in Forsyte's Guardian 365 experience supporting K–12, higher education, and public-sector institutions, with emphasis on identity driven attacks, alert optimization, 24x7 SOC coverage, and hands-on career readiness.

Title: Skills-Based Hiring



Presented by: Matt Isnor - Director, DoW Cyber Workforce Development

Speaker Bio: With over 20 years of experience within the cyberspace and intelligence communities, Isnor brings a meticulous approach to tackling complex challenges. He currently serves as the chief of Cyber Workforce Development at the Department of War Chief Information Office. In this role, he leads the standardization of the cyberspace workforce through the DoW Cyberspace Workforce Framework, ensuring critical skills align with mission tasks.

Presentation Summary: The Department of War is facing a critical frontline vulnerability: an estimated 20,000 unfilled cybersecurity positions. Traditional, degree dependent hiring pipelines are simply too slow and consistently fail to identify the right talent. In this session, we will take you inside the DoW's radical shift toward a skills-based hiring philosophy—a mandate directly aligned with White House Executive Orders 13932 and 14170. We are moving beyond the résumé to prioritize verifiable technical capabilities over paper credentials, opening the door for high-caliber, non-traditional talent to defend the nation's critical networks.

Title: The Navy Innovation Ecosystem



Presented by: Joey Mathews - Superintendent of the IT Division, US Naval Research Laboratory

Speaker Bio: Joey Mathews is the superintendent of the Information Technology Division at the US Naval Research Laboratory. He leads a broadly-based program of research and development spanning artificial intelligence and autonomy, networking and communications, information operations, high-assurance systems and cyber warfare, knowledge management and decision support, and computational science.

Presentation Summary: In 1915, American inventor Thomas Edison opined, “The Government should maintain a great research laboratory to develop guns, new explosives, and all the technique of military and naval progression without any vast expense.” This statement led to the creation of the Naval Research Laboratory in 1923. In this talk, I will discuss factors that motivate naval science and technology investments, cybersecurity considerations for Navy platforms, and opportunities for students to engage with the Navy’s innovation ecosystem.

Title: Cybersecurity Careers Start Here: HUBZone, CMMC, and the Talent Pipeline



Presented by: Christina Hunt - CEO, Cinteot

Speaker Bio: Christina Hunt is the CEO of Cinteot, a cybersecurity and IT firm based in Chambersburg, Pennsylvania, serving federal and defense clients as a woman-owned small business. She is focused on developing local cybersecurity talent through Cinteot’s internship and mentorship programs.

Presentation Summary: As CMMC requirements roll out across the defense industrial base, small businesses like Cinteot are facing a growing need for qualified cybersecurity talent—and that means real opportunity for students entering the field. Cinteot, a woman-owned small business based in a HUBZone designated area, supports clients while investing in the community through hands-on student internships in cybersecurity operations, compliance, and mentorship. In this talk, Hunt will share how being HUBZone-based shapes Cinteot’s mission and how the company’s internship program has become a real pathway to full-time careers.

Title: Nobody Cares About Cybersecurity Until Everything Stops



Presented by: Joe Harford - Founder and President, Reclamere

Speaker Bio: Joe Harford is the founder and president of Reclamere, where he has spent 25 years helping organizations navigate cybersecurity, business risk, and the occasional “everything is on fire” moment. He holds a PhD in workforce education and brings a rare mix of technical perspective, business experience, and practical humor.

Presentation Summary: Drawing on 25 years of real-world experience, Harford will share practical lessons about cyber risk, AI, career development, and the decisions that separate good cybersecurity professionals from trusted business leaders. Students will leave with a clearer understanding of what employers value, how the profession is changing, and why communication, judgment, and business awareness may matter just as much as technical skill.

Title: AI, Digital Competencies, and Societal Resilience: The Human Factor in Cybersecurity



Presented by: Joseph Squillace - Associate Teaching Professor of Cybersecurity, Penn State

Speaker Bio: Joseph M. Squillace is an associate teaching professor of cybersecurity in Penn State’s College of Information Sciences and Technology. He began his career in communications security as a US Air Force Tactical Air Control Party operator, managing cryptographic keys and secure radio links, and later worked in industry as a systems engineer and chief technology officer. As a 2025 Fulbright Scholar at Széchenyi István University in Hungary, he taught graduate courses on cyber law, national strategy, and social resilience.



Presented by: Roland Kelemen - Program Director and Associate Professor, Széchenyi István University

Speaker Bio: Program director and associate professor, head of the Department of Law of Modern Technologies and Cybersecurity, Deák Ferenc Faculty of Law and Political Sciences, Széchenyi István University. His research on cyberspace earned him a Fulbright Scholarship in the United States for the 2021–22 academic year. He is the head of the Cyberfare State Research Lab, a research group funded under the NKFIH Starting Program.

Presentation Summary: The rapid development of artificial intelligence not only creates new opportunities for cybersecurity but also amplifies existing human vulnerabilities. Drawing on Europol’s IOCTA 2026 and the FBI’s IC3 2025 data, it examines how generative AI scales social engineering, deepfakes, and online fraud by exploiting gaps in digital literacy. The objective should be to develop competent digital citizens who not only use emerging technologies but are also capable of recognizing, assessing, and managing their risks.

Title: Department of War Cyber Service Academy



Presented by: Alice Smitley - Cyber Service Academy Program Manager, Department of War Chief Information Officer’s Workforce Innovation Directorate

Speaker Bio: Alice Smitley is the Cyber Service Academy program manager within the Department of War’s Chief Information Officer’s Workforce Innovation Directorate. In this role, she leads the strategic development of the DoW’s cyber talent pipeline, designs long-range program plans, and manages the transition of CSA operations back to the DoW CIO. She also coordinates scholar placement across the DoW, identifies future cyber skills, and fosters critical partnerships with academic institutions.

Presentation Summary: The next world conflict won’t just be fought on land, at sea, or in the air. It is happening right now in the bits and bytes of our critical infrastructure. The Department of War Cyber Service Academy is the nation’s premier engine for digital defense. We have a singular, critical mission: recruit the absolute brightest cyber minds, retain our elite operators, and supercharge national security curricula to stay ahead of global adversaries. We don’t just educate we mobilize.