ASCCENT AI Security Summit

Register Here: https://events.gtri.gatech.edu/event/asccent-2025

Date/Time:

Wednesday December 3, 2025
8:00 am – 5:00 pm EST
Registration opens at 7:15 am

Virtual & Location:

GTRI Conference Center
Visitor Information Website
250 14th St NW, Atlanta, GA 3033

Session Topics

Session 1: Defense, Dual Use, and National Security

Explore the critical intersection of AI security and AI-enabled cybersecurity approaches that serve both national security and commercial sectors.

Session 2: AI Security in Healthcare

Explore the pressing need for robust data security and cybersecurity in the modern healthcare landscape, spanning sensitive data, software, and hardware considerations.

Session 3: Energy Security & AI Infrastructure

Explore the critical relationship between the energy that fuels AI infrastructure and the security measures essential for protecting our power grids in the age of AI.

Keynote Speakers

ASCCENT

Georgia Tech Research Institute

Schedule

7:15 am – 8:00 am	**Arrival, Networking, & Breakfast**
8:00 am – 9:15 am	**Welcome & Introduction** **Keynote:** Michael Steed, Founder, Paladin Capital Group **Fireside Chat:** Ann Dunkin, Distinguished External Fellow at GT, Former CIO of DOE **Moderator:** Dr. William Robinson, GTRI Deputy Director for Research, Information and Cyber Sciences Directorate
9:15 am – 9:30 am	**Break & Coffee**
9:30 am – 11:30 am	**Defense, Dual Use, & National Security** **Keynote:** Kevin Brown, Defense Tech Entrepreneur **Speakers/Panelists:** Denzil Wessels, Co-Founder, Dymium Daniel Sergile, Palo Alto Networks Dr. Taesoo Kim, Professor GT SCP, SCS Lauryn Williams, Deputy Director, Center for Strategic and International Studies (CSIS) **Moderator:** Stephen Welby, GTRI Deputy Director for Research, leading the Sensors and Intelligent Systems Directorate
11:30 am – 12:30 pm	**Lunch (Catered)**
12:30 pm – 2:40 pm	**Energy Security & AI Infrastructure** **Keynote:** Tom Fanning, Ret. CEO Southern Company **Speakers/Panelists:** Valerie Cofield, Executive Director, Institute for Critical Infrastructure Technology (ICIT) Jacob Benjamin, Global Practice Lead, Dragos Dr. Veronica Adetola, Chief Research Scientist and Team Leader, Pacific Northwest National Labs Dr. Trevor Lewis, Principal Research Scientist, GTRI **Moderator:** Ann Dunkin, Distinguished External Fellow at GT, Former CIO of DOE
2:40 pm – 2:55 pm	**Break & Coffee**
2:55 pm – 4:30 pm	**AI Security in Healthcare** **Keynote:** Dondi West, Assistant General Counsel at GSK **Speakers/Panelists:** Dr. Brendan Saltaformaggio, Associate Professor GT SCP, ECE Stoddard Manikin, CISO, Children's Healthcare of Atlanta Dr. Jon Duke, Director of the Center for Health Analytics and Informatics at GTRI **Moderator:** Eric Scott, CISO, GTRI
4:30 pm – 4:35 pm	**Closing Remarks**

Speaker & Participant Biographies

Michael Steed

Michael Steed is the Founder and Managing Partner and serves as Chairman of the Paladin Cyber Fund, Paladin Cyber Fund II and Paladin III Investment Committees. Mr. Steed provides management oversight of the firm's operations and investments and is responsible for the strategic direction of Paladin's current and future activities. Prior to forming Paladin Capital, Mr. Steed served as Senior Vice President of Investments of a major financial services company based in Washington, DC, and served as President of its SEC registered investment advisory firm. From 1981 to 1985, Mr. Steed served as Special Counsel to the Chairman and as the National Director of the Democratic Party of the United States of America (DNC). Previously, Mr. Steed engaged in the practice of law, both as a prosecutor in the Los Angeles City Attorney's Office and in private practice. Mr. Steed previously served on the Board of Trustees of Loyola Marymount University and is currently an emeritus member of the Board of Visitors for Duke University's Sanford School of Public Policy. He is Treasurer of the John F. Kennedy Library Foundation, a founding member of the Board of the National Democratic Institute (NDI) and a member of the Board of the National Alliance to End Homelessness and a member of the Board of Directors of Harvard University's Belfer Center's Defending Digital Democracy Project. He received his Bachelor of Arts from Loyola Marymount University in Los Angeles and his JD from Loyola Law School.

Ann Dunkin, P.E.

Ann Dunkin is an External Fellow and Distinguished Professor of the Practice at the Georgia Institute of Technology. She is also the CEO of Dunkin Global Advisors, providing strategic business advice to companies of all sizes as well as fractional CIO services. She serves as an independent director on the governing board of Global Interconnection group and the advisory boards for Bowtie Security, Openpolicy and CGAI. During the Biden-Harris Administration, Ann served as Chief Information Officer at the U.S. Department of Energy, where she managed a $5 billion IT portfolio and a $1 billion high-performance computing budget. In this role, she spearheaded

initiatives in cybersecurity, cloud migration, and digital transformation, aligning IT advancements with the DOE's mission to promote energy efficiency and environmental stewardship.

Prior to her tenure at DOE, Ann held several key positions, including CIO of the U.S. Environmental Protection Agency (EPA) during the Obama administration, Chief Strategy and Innovation Officer at Dell Technologies, CIO for the County of Santa Clara, and Chief Technology Officer for the Palo Alto Unified School District. Her early career at Hewlett-Packard encompassed various leadership roles in engineering, research and development, IT, manufacturing engineering, software quality, and operations.

Throughout her career, Ann has demonstrated a commitment to leveraging technology to solve complex problems, enhance organizational performance, and deliver innovative solutions across both the private and public sectors.

Dunkin is a published author, with her most recent book titled Industrial Digital Transformation and a frequent speaker on topics such as emerging technology, including the intersection of energy, AI and quantum, government technology modernization, digital transformation, and organizational development.

Ann's contributions to the field have been recognized with numerous accolades. Ann was recently named to the Forbes CIO Next list 2024. She also received the 2024 Institute of Industrial and Systems Engineering (IISE) Captains of Industry Award and the Institute for Critical Infrastructure Technology's 2024 Pinnacle Award. She has been given a range of previous awards, including a 2024 Fed 100 Award, the 2022 Capital CIO Large Enterprise ORBIE Award, DC's Top 50 Women in Technology for 2015 and 2016, ComputerWorld's Premier 100 Technology Leaders for 2016, StateScoop's Top 50 Women in Technology list for 2017, FedScoop's Golden Gov Executive of the Year in 2016, 2021, 2022, 2023,and 2024 and FedScoop's Best Bosses in Federal IT 2022. She was also named to Washington Exec's Ones to Watch list for 2023.

Ann holds a Master of Science degree and a Bachelor of Industrial Engineering degree, both from the Georgia Institute of Technology. She is a licensed professional engineer in the states of California and Washington and an IISE Fellow. In 2018, she was inducted into Georgia Tech's Academy of Distinguished Engineering Alumni and in 2024 she was named to the inaugural list of "Women at Georgia Tech."

Kevin Brown

Kevin Brown is an accomplished entrepreneur and executive, with 25+ years' experience building, running, and advising companies in Silicon Valley, including depth in AI, cybersecurity, and defense tech. Kevin is co-founder and CEO of Innit, which has generated 41 patents relating to sensors, AI, and nutrition in the Food and Health sectors. Previously, he served in roles including CEO of Kidaro (acquired: MSFT), Vice President at Decru (acquired: NTAP), and VP/GM and founding team at Internet infrastructure pioneer Inktomi (NASDAQ: INKT, acquired: YHOO). Kevin was named a Fellow at UC Berkeley's Haas School of Business and sat on the Dean's Advisory Circle for 10 years, and earned his Bachelor's and MBA degrees at UC Berkeley, where he served as MBA class president.

Tom Fanning

Tom Fanning served as chairman, president and CEO of Southern Company from 2010 - 2023. His innovative thinking and ability to anticipate and adapt to new technologies and evolving regulatory and social landscapes have positioned the company as a leader in delivering clean, safe, reliable and affordable energy to millions of customers through its subsidiaries.

During his career more than 40-years with the company, Fanning held executive roles across a variety of business disciplines, including finance, strategy, international business development and technology. Fanning also served on the board of directors of the Federal Reserve Bank of Atlanta and is a past chairman. He is also a past chairman of the Conference of Chairs of the Federal Reserve Banks and the Edison Electric Institute.

Under Fanning's leadership, Southern Company constructed two state-of-the-art nuclear units in Georgia, the first new nuclear units to be built in the United States in more than 30 years. During his tenure, the company also added more than 4,000 megawatts of renewable energy and explored beyond-the-meter customer solutions.

Dondi West

Dondi serves as Assistant General Counsel at GSK where he advises senior tech, digital and security leaders on matters related to Cybersecurity. As security counsel, Dondi plays a pivotal role helping to lead the company's digital transformation, which includes leveraging digital technologies like artificial intelligence (AI), machine learning (ML), and deep learning to unite science, technology and talent to get ahead of disease together.

He previously worked as a security attorney at TikTok and Microsoft. Before becoming in-house counsel, he was a Senior Cyber Intelligence Analyst at PwC and spent time supporting U.S. Cyber Command, NSA, and ODNI as a defense contractor. Dondi also served as an Information Warfare Officer in the U.S. Navy, and holds a B.S. in Mathematics, a M.S. in Applied Information Technology, and a Juris Doctor. He is a Certified Information Systems Security Professional (CISSP).

Dr. Veronica Adetola

Veronica Adetola, Ph.D. is a Chief Research Scientist and Team Leader at Pacific Northwest National Laboratory (PNNL), where she leads multidisciplinary research to optimize grid-edge resources and strengthen the reliable and resilient operation of power and energy infrastructures. Her research spans model-based and AI/ML-based control, optimization, and system–control co-design for diverse applications.

From 2021 to 2025, she served as a Thrust Lead for PNNL's Resilience Through Data-Driven, Intelligently Designed Control (RD2C) initiative, where she helped develop resilient-by-design frameworks and multi-layer mitigation strategies spanning device, network, and control application layers. She also serves as Chief Scientist for the Energy System Co-Design with Multiple Objectives and Power Electronics (E-COMP) initiative, addressing emerging grid stresses driven by evolving generation portfolios and rapid load growth associated with AI and high-performance computing infrastructures.

Prior to joining PNNL, she spent nearly a decade conducting industry research at United Technologies Research Center (now Raytheon Technologies Research Center). Dr. Adetola holds 10

issued U.S. patents and serves as Associate Editor for IEEE Transactions on Control Systems Technology.

Dr. Jacob Benjamin

Jacob Benjamin is the global practice lead of consulting services, at the industrial cyber security company Dragos, Inc. In this role, Dr. Benjamin oversees the delivery and execution of consulting services provided by Dragos for ICS/OT/SCADA networks worldwide.

Prior to joining Dragos, Dr. Benjamin was a nuclear cybersecurity researcher at Idaho National Laboratory and a nuclear cybersecurity specialist for Duke Energy. Over the last fifteen years, Jacob has performed a variety of cyber-related tasks at many domestic and international critical infrastructures. He has substantial experience developing cybersecurity programs for nuclear power plants as well as performing cybersecurity risk assessments for critical digital assets, systems, and networks within industrial environments. Dr. Benjamin has provided his expertise for the U.S. Department of Energy, the National Nuclear Security Administration (NNSA), and the International Atomic Energy Agency (IAEA).

Dr. Benjamin remains active in the industrial control system security community as an author on a several research publications and a speaker at various industry conferences. He continues to act as a part-time lecturer and subject matter expert for cybersecurity and critical infrastructure workshops affiliated with Idaho National Laboratory, Utica University, and the Citadel Military College of South Carolina.

Valerie Cofield

Ms. Cofield is the Executive Director for Institute for Critical Infrastructure Technology (ICIT). ICIT's mission is to modernize, secure, and make resilient critical infrastructure that provides for people's foundational needs. ICIT is a resource for organizations and communities that understand that people need to be at the center of critical infrastructure research and decision making, ensuring that modernization and security investments in critical infrastructure have a lasting, positive impact on society.

Prior to joining ICIT, Ms. Cofield served as the Chief Strategy Officer of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). In that role she was the principal policy and strategic adviser to CISA leadership and senior management, integrating strategy across all the organization's mission areas and ensuring policy, strategy, and operational consistency throughout the agency.

Prior to CISA, Ms. Cofield served in the FBI for 22 years in a variety of roles. She was Deputy Assistant Director (DAD) for the Cyber Capabilities Branch within the Federal Bureau of Investigation's (FBI) Cyber Division where she led coordination and deployment of the division's technical tools and capabilities, and oversaw cyber-related training, recruiting, hiring, and budgeting for the division. She also served in a senior executive role as chief of staff of the Science and Technology Branch and as a DAD of the Digital Transformation Office (DTO), where she engaged with interagency partners and other key stakeholders on policy issues related to current and emerging technologies and their impact on law enforcement.

In 2019, Ms. Cofield was selected as the FBI's senior detail to the Cyberspace Solarium Commission. This Congressional Commission was authorized through the FY2019 National Defense Authorization Act (NDAA). Its mission was to develop a national strategy for preventing cyberattacks of significant consequences. While on the Commission, Ms. Cofield was a Senior Director and Task Force Lead. The Commission completed its report in March of 2020 with over 80 recommendations, 25 of which have been enacted into law.

Dr. Jon Duke, MD, MS

Dr. Jon Duke is Director of the Center for Health Analytics and Informatics at the Georgia Tech Research Institute and Principal Research Scientist in the Georgia Tech College of Computing. Dr. Duke has led over $45 million in funded research for industry, government, and foundation partners. His research focuses on artificial intelligence and interoperability tools for analyzing complex health data, with applications spanning clinical care, research, safety, cost transparency, and public health. Dr. Duke was a founding member of the OHDSI consortium, an open-source health analytics collaborative now in over 20 countries. He served on the Board of Directors of Liaison Technologies and has advised over a dozen startups from the Georgia Tech ecosystem.

Dr. Duke graduated from Harvard Medical School and completed his internal medicine residency at the Brigham and Women's Hospital in Boston. He completed fellowship training in Medical Informatics and holds a master's degree in Human-Computer Interaction from Indiana University.

In addition to over 50 peer-reviewed publications, Dr. Duke's work has been featured in the lay media ranging from the New York Times to Consumer Reports.

Dr. Taesoo Kim

Taesoo Kim is Professor in the School of Computer Science, College of Computing at the Georgia Institute of Technology, which he joined in 2014 after completing his Ph.D. at the Massachusetts Institute of Technology. Kim is interested in building computing systems where underlying principles justify why it should be secure. Those principles include the design of the system, analysis of its implementation, and clear separation of trusted components. Kim seeks to develop tools that automatically identify which parts of an operating system have been affected, allowing a system administrator to recover from cyberattacks without excessive, manual effort.

Since arriving at Georgia Tech, Kim has secured numerous research grants from the Office of Naval Research, the National Science Foundation, and Defense Advanced Research Projects Agency (DARPA), among others. He continues to earn numerous honors such as the 2015 Internet Defense Prize from USENIX and Facebook, he competed as a finalist in the inaugural DARPA Cyber Grand Challenge with Team Disekt, and he led Team Atlanta to win the DARPA AI Cyber Grand Challenge (AIxCC).

Kim holds two bachelor's degrees -- in Computer Science and in Electrical Engineering -- from the Korea Advanced Institute of Science & Technology (KAIST) and graduated summa cum laude. He earned a Master's in Electrical Engineering and Computer Science from MIT under Nickolai Zeldovitch before continuing under the same advisor in its Ph.D. program. Kim is affiliated with the Institute for Information Security & Privacy at Georgia Tech and contributed to its predecessor -- the Georgia Tech Information Security Center.

Dr. Trevor Lewis

Dr. Trevor Lewis is a Principal Research Scientist and Offensive Cybersecurity Engineer for the Georgia Tech Research Institute (GTRI). Dr. Lewis' primary areas of research and consulting for the US Department of War, US Department of Energy (DoE), and Critical Infrastructure entities include penetration testing, red teaming, cyber threat emulation, Defensive Cyber Operations (DCO), high-security architecture design, and threat hunting, among many others. At GTRI, Dr. Lewis routinely leads research projects that implement real-world operational cybersecurity capabilities for industry, government, and DoD customers that have real mission impacts, including electric power/ICS/SCADA environments.

Stoddard Manikin

Stoddard Manikin has over 25 years of experience in information technology, cyber security and privacy. He specializes in advising complex organizations on security topics including resiliency, regulatory compliance, integrating information security with enterprise risk management, and identity and access management.

Mr. Manikin is currently Vice President and Chief Information Security Officer for Children's Healthcare of Atlanta, one of the largest pediatric clinical care health systems in the United States.

Prior to joining Children's, Mr. Manikin led multiple consulting practices including FishNet Security's (formerly Logic Trends) southeast region identity and access management practice, where he was responsible for pre-sales and service delivery oversight. Mr. Manikin joined Logic Trends from Ernst & Young, where he led the southeast area security services team as a Senior Manager.

Dr. William Robinson

William H. Robinson, Ph.D., is the GTRI Deputy Director for Research, leading the Information and Cyber Sciences Directorate (ICSD). As ICSD Director, Robinson leads the Information and Communications Laboratory (ICL) and the Cybersecurity, Information Protection, and Hardware Evaluation Research (CIPHER) Laboratory, and manages research portfolios that span GTRI. In addition, Robinson is a tenured Professor of Electrical and Computer Engineering at Georgia Tech.

Before joining GTRI, Robinson served as Professor of Electrical Engineering with tenure and the Vice Provost for Academic Advancement at Vanderbilt University. There, he led the Security and Fault Tolerance Research Group, whose mission was to design, model, verify, and implement robust computing systems that positively benefit stakeholders with consumer, defense, industrial, and medical applications. He was selected for a National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award and the Defense Advanced Research Projects Agency (DARPA) Computer Science Study Panel.

Robinson has an expansive portfolio of research, publications, scholarly work, presentations, and awards. While at Vanderbilt University, he was involved in research for sponsors including DARPA, the Defense Threat Reduction Agency (DTRA), and NSF. Robinson's research related to national security includes: (1) radiation-hardened electronics for satellite and missile systems, (2) hardware trust and assurance for integrated circuits and third-party intellectual property, (3) cyber security with intrusion detection systems, and (4) resilience for unmanned aerial systems and mobile ad hoc networks. In 2015 and in 2016, he served as the General Chair for the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), which convenes a robust community of researchers from academia, government, and industry. He served as the Technical Program Chair for the 2024 IEEE Nuclear and Space Radiation Effects Conference (NSREC), an international forum on radiation effects in materials, electronic devices, circuits, and systems.

Robinson holds a B.S. in Electrical Engineering from the Florida Agricultural and Mechanical University (FAMU) as well as a M.S. in Electrical Engineering and Ph.D. in Electrical and Computer Engineering from Georgia Tech.

Eric Scott

Eric R. Scott is the inaugural and Chief Information Security Officer (CISO) and Director of the Information and Cybersecurity Department (ICD) at GTRI. Eric has the overall responsibility to provide vision and leadership for the cybersecurity & compliance programs of unclassified systems, data, and networks at GTRI. This includes but not limited to information security operations, cyber risk & intelligence, data loss & fraud protection, privacy, data governance, regulatory compliance, policy management and audits & assessment. Eric serves on the GTRI IT leadership team, and is responsible for overseeing all aspects of unclassified cybersecurity at GTRI.

Eric came up through the technical ranks starting as junior helpdesk analyst and progressing through systems and networks before shifting exclusively to cybersecurity 20 years ago. Eric not only has a solid background in cybersecurity, but also specifically leading cybersecurity within research and development (R&D) organizations as well. Before joining GTRI, Eric led the enterprise cybersecurity efforts at the National Cancer Institute (NCI) and before that at the Defense Advance Projects Agency (DARPA). Furthermore, Eric served as the MAJCOM Chief Information Security Officer (CISO) for the Air National Guard (ANG) overseeing the cybersecurity all of the ANG intelligence, surveillance, and reconnaissance (ISR) systems and assets.

Throughout his career, Eric also supported cyber efforts for the United States Navy (USN), the Defense Intelligence Agency (DIA), and the Department of Energy (DOE). Eric is combat veteran, retiring after 20 years of honorable service in the United States Marine Corps (USMC) Reserves where he worked in information technology, cybersecurity, and information operations.

Eric holds an Associate of Applied Technology (AAT) degree from Athens Technical College, an Associate of Arts (AA) degree from Pensacola State College, a Bachelor of Science in Business Administration (BSBA) degree from Shippensburg University and a Master of Science (MS) degree from George Mason University. Eric is also a certified Project Management Professional (PMP), and a Certified Information Systems Security Professional (CISSP).

Dr. Brendan Saltaformaggio

Dr. Brendan Saltaformaggio is an Associate Professor in the School of Cybersecurity and Privacy and the School of Electrical and Computer Engineering at the Georgia Institute of Technology. He also hold a courtesy appointment in the School of Computer Science. Brendan leads the Cyber Forensics Innovation Laboratory (CyFI Lab), made up of a team of researchers who work together to further the investigation of advanced cyber crimes and the analysis and prevention of next-generation malware attacks. The lab's work ranges from research in cyber forensics and computer system security to key applications in the vetting of untrusted/malicious software and the protection of critical cyber-infrastructure. Underpinning this research is the development of fundamental techniques for binary software analysis and instrumentation, modeling and collection of cyber-forensic evidence, and integrated multi-layer system defenses.

Stephen Welby

Stephen Welby is the GTRI Deputy Director for Research, leading the Sensors and Intelligent Systems Directorate (SISD). Stephen manages operations across three research areas: the Advanced Concepts Laboratory (ACL), the Aerospace, Transportation and Advanced Systems Laboratory (ATAS), the Sensors and Electromagnetic Applications Laboratory (SEAL), and the Cybersecurity, Information Protection, and the Hardware Evaluation Research (CIPHER) Laboratory.

Stephen has more than three decades of government, non-profit, and industrial experience in technology and product development, including senior leadership positions at the Defense Advanced Research Projects Agency (DARPA).

Stephen most recently served as Special Assistant to the President for Science and Technology Policy and as Deputy Director for National Security in the White House Office of Science and Technology Policy (OSTP). Stephen led an OSTP team focused on strengthening the nation’s long-term global competitiveness and reducing risk through the assessment, development, deployment,

and governance of current and emerging technologies. He oversaw efforts to develop long-term national science and technology (S&T) strategies, shape new investments in foundational technologies, modernize national security systems, ensure supply chain security, cultivate an agile innovation base, enhance export and investment controls, manage emergent risks and build the world's best STEM workforce. His focus areas included Biotechnology and Biosecurity, Artificial Intelligence, Semiconductors, Space Systems, Quantum Information Science, Nuclear Matters, and Economic Security.

Prior to joining the White House, Stephen was the Executive Director and Chief Operating Officer of the Institute of Electrical and Electronics Engineers (IEEE), the world's largest not-for-profit organization of technology professionals.

In 2015, Stephen was confirmed by the U.S. Senate as the Assistant Secretary of Defense for Research and Engineering. In this role, he served as the Chief Technology Officer for the U.S. Department of Defense, leading one of the largest and most complex research, development, and engineering organizations in the world. Stephen previously was the Deputy Assistant Secretary of Defense for Systems Engineering, and was responsible for establishing and executing engineering policy and oversight across the Department.

Stephen holds a bachelor of science degree in chemical engineering from The Cooper Union for the Advancement of Science and Art, a master's degree in business administration from the Texas A&M University, and master's degrees in computer science and applied mathematics from The Johns Hopkins University.

Denzil Wessels

Denzil is a veteran technologist with a career built on securing mission-critical environments. He has spent years operationalizing and building Zero Trust strategies for the global market, spanning Cloud Security, VPN, SASE, ZTNA, Network Access Control (NAC), and Mobile Defense.

His pedigree includes building and scaling technology for the world's most recognizable security infrastructure companies, including Zscaler, Juniper (HPE), F5, and Aruba Networks (HPE), Oort (Cisco).

Currently, Denzil is driving innovation at Dymium, solving the complex data access challenges inherent in modern AI and Enterprise deployments. He focuses

on enabling zero-trust data consumption without compromising security or sovereignty—a critical requirement for the future of enabling AI safely and securely.

Lauryn Williams

Lauryn Williams is the deputy director and senior fellow in the Strategic Technologies Program at the Center for Strategic and International Studies. Until January 2025, she was chief of staff to the assistant secretary of defense for industrial base policy within the Office of the Under Secretary of Defense for Acquisition and Sustainment, where she spearheaded the release of the National Defense Industrial Strategy Implementation Plan. From 2022 to 2024, Lauryn was director for strategy in the White House Office of the National Cyber Director and led the strategic initiative on space system cybersecurity, which leveraged extensive government agency, industry, and international collaboration. This work resulted in the first-ever minimum cybersecurity requirements for federal space systems. Prior to the White House, Lauryn served as a policy advisor in the Pentagon space policy office and led efforts to leverage commercial space and develop norms of responsible behavior. She has also served in the Department of Energy's National Nuclear Security Administration, where she led international export control projects, and worked at the Carnegie Endowment for International Peace. Lauryn received her master's degree in public and international affairs from Princeton University and her bachelor's degree in political science, with honors in international security studies, from Stanford University.

With Support From

PALADIN CAPITAL GROUP

Organizing Partners

PALADIN GLOBAL INSTITUTE

Georgia Tech Strategic Energy Institute