

NDIA



CYBERSECURITY DIVISION MEETING

October 17, 2023 | Arlington, VA | [NDIA.org](https://www.ndia.org)

Table of Contents

WHO WE ARE	2
EVENT INFORMATION.....	3
WELCOME LETTER	4
AGENDA.....	5
BIOGRAPHIES	7



NDIA

WHO WE ARE

The National Defense Industrial Association is the trusted leader in defense and national security associations. As a 501(c)(3) corporate and individual membership association, NDIA engages thoughtful and innovative leaders to exchange ideas, information, and capabilities that lead to the development of the best policies, practices, products, and technologies to ensure the safety and security of our nation. NDIA's membership embodies the full spectrum of corporate, government, academic, and individual stakeholders who form a vigorous, responsive, and collaborative community in support of defense and national security. For more than 100 years, NDIA and its predecessor organizations have been at the heart of the mission by dedicating their time, expertise, and energy to ensuring our warfighters have the best training, equipment, and support. For more information, visit NDIA.org

GET INVOLVED

Learn more about NDIA's Divisions and how to join one at NDIA.org/Divisions



LEADERSHIP

Trey Hodgkins
Division Chair

Heather Tedder
Division Co-Chair

Cybersecurity Division

WHO WE ARE

The division's primary objective is to contribute to U.S. national security by promoting communication and interaction between the industry, government and military on cybersecurity and cyber defense policy, legislation, requirements and technology

The Cybersecurity Division's charter is to facilitate industry, government, and academia interaction in policy, legislative, legal and technical areas directly related to protecting cyber assets and maintaining access to the cyber domain. Such interaction is intended to promote the development of a secure, resilient and reliable cyber domain for the United States and its allies, and to provide for an exchange of information and views between industry, academia, government and military representatives. The effective cooperation between these groups is essential to establish and maintain U.S. superiority in the cyber domain.

Event Information

ATTIRE

Civilian: Business
Military: Uniform of the Day

SURVEY AND PARTICIPANT LIST

You will receive via email a survey and list of participants (name and organization) after the conference. Please complete the survey to make our event even more successful in the future.

EVENT CONTACT

Jenica Seguine
Meeting Planner
(703) 247-2561
jseguine@NDIA.org

Rhea Ambanta
Division Coordinator
(703) 247-9479
rambanta@NDIA.org

CHATHAM HOUSE RULES

This meeting will be held under Chatham House rule. Attendees are free to use the information from the discussions, but neither the identity nor the affiliation of the speaker(s), nor that of any participant, may be revealed.

HARASSMENT STATEMENT

NDIA is committed to providing a professional environment free from physical, psychological and verbal harassment. NDIA will not tolerate harassment of any kind, including but not limited to harassment based on ethnicity, religion, disability, physical appearance, gender, or sexual orientation. This policy applies to all participants and attendees at NDIA conferences, meetings and events. Harassment includes offensive gestures and verbal comments, deliberate intimidation, stalking, following, inappropriate photography and recording, sustained disruption of talks or other events, inappropriate physical contact, and unwelcome attention. Participants requested to cease harassing behavior are expected to comply immediately, and failure will serve as grounds for revoking access to the NDIA event.

EVENT CODE OF CONDUCT

NDIA's Event Code of Conduct applies to all National Defense Industrial Association (NDIA), National Training & Simulation Association (NTSA), Emerging Technologies Institute (ETI), and Women In Defense (WID) meeting-related events, whether in person at public or private facilities, online, or during virtual events. NDIA, NTSA, ETI, and WID are committed to providing a productive and welcoming environment for all participants. Visit [NDIA.org/CodeOfConduct](https://www.ndia.org/CodeOfConduct) to review the full policy.

ANTITRUST STATEMENT

The NDIA has a policy of strict compliance with federal and state antitrust laws. The antitrust laws prohibit competitors from engaging in actions that could result in an unreasonable restraint of trade. Consequently, NDIA members must avoid discussing certain topics when they are together at formal association membership, board, committee, and other meetings and in informal contacts with other industry members: prices, fees, rates, profit margins, or other terms or conditions of sale (including allowances, credit terms, and warranties); allocation of markets or customers or division of territories; or refusals to deal with or boycotts of suppliers, customers or other third parties, or topics that may lead participants not to deal with a particular supplier, customer or third party.

Welcome to The Cybersecurity Division Meeting

On behalf of the Cybersecurity Division at the National Defense Industrial Association, welcome to the fall meeting in observance of Cybersecurity Awareness Month. Each October, government agencies and private sector organizations work to raise the level of awareness of cyber risks and NDIA is pleased to join that effort in 2023. Each year marks ever increasing threats and challenges from cyber-actors and 2023 is no different from previous years.

This convening of the Cyber Division is the first in some time and marks an effort to create a series of forums for NDIA members to discuss and address cyber risks. As we move into 2024, our plan is to convene an increasing cadence of meetings to keep up with the pace of cyber threats and the responses to address them. We hope that you find this a great opportunity to meet and engage with policy and decision makers and gather with like-minded NDIA members to discuss cyber-related issues.

Cybersecurity policy, administration initiatives, regulations and legislation affect all Americans, and companies represented in the NDIA membership are uniquely impacted as members of the defense industrial base. To more effectively address those cyber activities and position NDIA to respond and react, we have created four Committees to organize our work. They are: Legal and Policy; Cybersecurity Supply Chain; Software Assurance; and Cybersecurity Standards. Each of these distinct focus areas is seeking NDIA members to engage and participate in the work of the Committees. If you or other colleagues focused on these topics are not already on the Division and Committee contact lists, please let us know. We would appreciate and encourage your engagement.

Thank you for joining the Cybersecurity Division as we re-engage on this important issue.

Trey Hodgkins
Cybersecurity Division Chair



Join the Conversation

[@NDIAToday](#) [@NDIAMembership](#) [NDIA.org/LinkedIn](#) [@NDIAToday](#) [@NDIAToday](#)

NDIA | CAREER CENTER

Connecting Talent with Great Opportunities

This latest member benefit of the National Defense Industrial Association offers qualified defense and national security professionals and employers an intuitive platform to identify the next best opportunity or candidate. With single-sign-on, quick and advanced searches, job alerts, career resources, pre-screen questionnaires, success tracking, and more, the NDIA Career Center is the defense industry's premier resource for career growth and advancement.

Log in and complete your profile today at [Jobs.NDIA.org](#)

Agenda

Tuesday, October 17

8:00 am – 3:30 pm

Registration

GEORGE

8:00 – 9:00 am

Networking Breakfast

GEORGE

9:00 – 9:30 am

Welcome Remarks

GEORGE

Trey Hodgkins

Chair, NDIA Cyber Security Division

Brig Gen Guy Walsh, USAF (Ret)

Executive Vice President, NDIA

Concurrent Sessions: Committee Breakouts

9:30 am – 12:00 pm

Cyber Legal Policy Committee

MARTHA

Susan Warshaw Ebner

NDIA Cyber Legal Policy Committee Co-Chair

Rolando Sanchez

NDIA Cyber Legal Policy Committee Co-Chair

Welcome and Introduction (9:30 – 9:40 am)

Introductions (9:40 – 10:15 am)

Networking Break (10:15 - 10:30 am)

NDIA Legislative Affairs (10:30 – 11:00 am)

Michael Seeds

Senior Director, Strategy & Policy, NDIA

Survey of Past Committee Activities

(11:00 – 11:15 am)

Survey of Pending Legislation and Rules

(11:15 – 11:35 am)

Session Wrap-up (11:35 am – 12:00 pm)

Cyber Supply Chain Committee

GEORGE

Donald Davidson

NDIA Cyber Supply Chain Committee Co-Chair

Bruce Jenkins

NDIA Cyber Supply Chain Committee Co-Chair,

Welcome and Introduction (9:30 – 9:45 am)

Introductions (9:45 – 10:15 am)

Committee Break (10:15 - 10:30 am)

History of SCRM, NIST SP 800-161 & Commercial Standards

(10:30 – 11:30 am)

Jon Boyens

Deputy Chief, Computer Security Division, National Institute of Standards and Technology (NIST)

Joyce Corell

Senior Technology Advisor, Office of the Director of National Intelligence (ODNI)

Open Discussion and Session Wrap-up

(11:30 am – 12:00 pm)

12:00 – 1:00 pm

Networking Lunch

GEORGE

1:00 – 1:15 pm

Afternoon Kickoff and Committee Introductions

GEORGE

Trey Hodgkins
NDIA Cybersecurity Division Chair

Heather Tedder
NDIA Cybersecurity Division Vice Chair

Donald Davidson
NDIA Cyber Supply Chain Committee Co-Chair

Bruce Jenkins
NDIA Cyber Supply Chain Committee Co-Chair

Susan Warshaw Ebner
NDIA Cyber Legal Policy Committee Co-Chair

Rolando Sanchez
NDIA Cyber Legal Policy Committee Co-Chair

Ian Schmertzler
NDIA Cyber Standards Committee Co-Chair

Sandra Throneberry
NDIA Cyber Standards Committee Co-Chair

Caitlin Dohrman
NDIA Software Assurance Committee Co-Chair

Emile Monette
NDIA Software Assurance Committee Co-Chair

1:15– 2:00 pm

DHS CUI Rule: Do You Need an ATO?

GEORGE

Sarah Todd
Executive Director, Acquisition Policy & Legislation, Office of the Chief Procurement Officer (OCPO),
U.S Department of Homeland Security (DHS)

2:00 – 2:45 pm

FBI Presentation

GEORGE

Evan Schlessinger
Supervisory Special Agent, Federal Bureau of Investigation (FBI)

Jeffrey Horton
Intelligence Analyst, Cyber Crime Strategic Intelligence Unit, Federal Bureau of Investigation (FBI)

2:45 - 3:00 pm

Networking Break

GEORGE

ETI EMERGING TECHNOLOGIES INSTITUTE | **NDIA**

EMERGING TECH HORIZONS

NDIA'S TECHNOLOGY PODCAST

[Listen Now](#)

Sponsored By: **Raytheon**
An RTX Business

3:00 – 3:45 pm

SBOM + HBOM = DBOM: Bills of Material

GEORGE

Chris Oatway

Associate General Counsel, Verizon

Rosa Underwood

IT Specialist - IT Security Subcategory, Information Technology Category (ITC), Federal Acquisition Service (FAS), U.S. General Services Administration (GSA)

Veronica Daigle

Executive Director, Readiness & Cybersecurity, The Boeing Company

3:45 pm

Closing Remarks

GEORGE

Trey Hodgkins

NDIA Cybersecurity Division Chair

Biographies



Sarah Todd

Executive Director, Acquisition Policy and Legislation
Office of the Chief Procurement Officer (OCPO)

Sarah Todd is the Executive Director of Acquisition, Policy, and Legislation

(APL) within the DHS Office of the Chief Procurement Officer. In this role, she is responsible for maintaining DHS procurement authorities, the Homeland Security Acquisition Regulations and the Homeland Security Acquisition Manual, as well as DHS-wide implementation of new Executive Orders, statutes, regulations, DHS-level policy, and Administration and Secretary-level priorities affecting acquisition.

Among other work, Todd has supported the Department's launch of the DHS Vendor Cyber Hygiene Assessment Framework and also serves as the DHS Senior Accountable Official for the Implementation of the Make PPE in America Act.

A member of the Senior Executive Service, Todd joined APL after having served nine years with U.S. Immigration and Customs Enforcement (ICE). At ICE she held several key leadership positions including Deputy Head of the Contracting Activity, overseeing a workforce of 180+ acquisition professionals obligating \$3.8 billion in spend

annually. Sarah also has a wealth of private sector experience as a small business owner of a private aviation firm.

Todd holds a Master of Science in Government Contracts from The George Washington University and a bachelor's degree in business administration from The University of Texas at Tyler. She was the editor in Chief of the 2014 Journal of Contract Management and a co-author of an article published in the February 2022 Edition of *Contract Management* magazine, *Working Smarter Not Harder*; streamlining source selection in federal procurement.



Chris Oatway

Managing Associate General Counsel
Verizon

Chris Oatway is responsible for cybersecurity and supply chain policy, as

well as consumer protection issues relating to robocalls and text messaging, at Verizon. Prior to Verizon, he was an antitrust litigator

at Covington & Burling in Washington, DC, and his early career he included stints at major law firms in Brussels and Mexico City. Before attending law school he worked as an economic consultant, providing antitrust analysis to risk arbitrage hedge funds.

Oatway received his law degree, magna cum laude, from Georgetown, where he also earned a Master of Science in Foreign Service. He studied undergraduate economics at the University of Massachusetts.



Rosa Underwood

IT Specialist, IT Security Subcategory Information Technology Category Federal Acquisition Services
U.S. General Services Administration

Rosa Underwood is an IT Specialist in the IT Security Subcategory

within Information Technology Category (ITC), Federal Acquisition Service (FAS), supporting the transition to a more modernized and resilient infrastructure. She also contributes to GSA initiatives for the adoption and integration of cybersecurity into the acquisitions process to help strengthen the resiliency of the Supply Chain Government-wide.

Underwood has an extensive background in IT and telecommunications with many years of profound experience from various roles in the private sector. Before joining GSA, she was a contractor supporting

the implementation of the Continuous Diagnostics and Mitigation (CDM) program at the Dept. of Commerce. In her role as a Senior Systems Engineer at Juniper Networks. She focused on idealistic solutions for compliance with Federal and international standards for hardware and software, including cryptographic module validation programs, across routing, security, and switching platforms. Much of her expertise comes from her tenure at Verizon Communications where she spent over 10 years of her career in Verizon Labs as a Subject Matter Expert (SME). Using her technical knowledge, Underwood crafted innovative solutions that led to 22 patents granted by the US Patent and Trademark Office. The depth of her experience includes

roles in governance, risk, and compliance (GRC); project management; network operations; customer service; hardware and software testing; and systems integration.

Underwood's professional experience is complemented by degrees in Internetworking Technology, Telecommunications Engineering, and Optoelectronics Engineering. She holds several professional certifications in cybersecurity, project management, and cloud technology. She was named a winner of MeriTalk's 2023 Cyber Defenders Awards which recognizes individuals in government and industry who drive innovation, advance the nation's cybersecurity, and who have made significant contributions across cyber programs in Federal IT.



Veronica Daigle

Executive Director, Readiness & Cybersecurity
The Boeing Company

Veronica Daigle is the Executive Director of Readiness & Cybersecurity

at The Boeing Company. Prior to joining Boeing in 2020, Daigle was the Senate-confirmed Assistant Secretary of Defense for Readiness in the Department of Defense (DoD), where she served as the principal staff advisor to the Secretary of Defense and the Under Secretary of Defense for Personnel and Readiness on all matters related to military readiness. In that position, Daigle managed three deputy assistant secretaries of defense, with a combined staff of over 50 military and civilian personnel.

Daigle entered the Federal Government in 2008 as a Presidential Management Fellow at the White House's Office of Management and Budget (OMB), and subsequently served as an operations research analyst

in DoD's office of Cost Assessment and Program Evaluation (CAPE). From 2008 to 2013, Daigle assessed a wide-ranging portfolio of issues, including the operational requirements and costs for Army ground operations, the potential effect of continued Overseas Contingency Operations funding on readiness programs, and the sufficiency of resources to support mental health services for Service Members. In 2013, Daigle was selected to become a career member of the Senior Executive Service and served as the Director of CAPE's Force and Infrastructure Analysis Division. She joined the Office of the Under Secretary of Defense for Personnel and Readiness in 2017 as the Principal Deputy Assistant Secretary of Defense for Readiness, and was confirmed by the Senate to be the Assistant Secretary of Defense for Readiness in the summer of 2019.

Prior to her federal service, Daigle worked nearly ten years in the financial sector where she developed industry-wide benchmarks to measure the risk-adjusted performance of securities lending activities. She collaborated closely with senior executives at 20 global banking institutions to prepare customized benchmark analyses and marketing strategies, and supported over 150 state Treasurers, public pension fund executives, and mutual fund administrators in assessing the performance of their securities lending programs.

Daigle earned a Bachelor of Arts in Philosophy from Fordham University and a Master's Degree in Political Science/ International Affairs from George Mason University. She is a recipient of the Department of Defense Medal for Distinguished Public Service and the Office of the Secretary of Defense Medal for Exceptional Civilian Service.

Small Business Innovation Summit

NDIA

Register Today!

Join us at the NDIA Small Business Innovation Summit to learn how you, as a small business innovator, can support supply at the tactical edge and positively impact national security interests.

Are you a small business looking to take your defense technology to the next level? Are you new to government contracting? Are you looking for tips on how to engage in the SBIR/STTR program or navigate the rich federal innovation ecosystem? This conference is for you.

The government is actively looking for solutions in the areas of human performance, robotics, communications, cybersecurity, and trusted supply chain. Register today and learn first-hand how you can apply your technologies, ideas, and innovations to address national security needs.

December 5 – 7, 2023 | Lincoln, MA | [NDIA.org/SBSummit23](https://www.ndia.org/SBSummit23)

34TH ANNUAL SO/LIC SYMPOSIUM

NDIA

Register Today!

SOF Priorities for Strategic Competition

Special Operations Forces remain a national advantage in this decisive decade, but strategic competition is rapidly shifting the geopolitical, technological, economic, and environmental challenges facing SOF. Irregular warfare remains key to meeting these challenges, but a changing environment shifts the relative emphasis between IW missions. Today, SOF must lead the charge in rapidly scaling new capabilities relevant to strategic competition just as it quickly scaled CT/COIN capabilities to meet the needs of the Global War on Terror. The drive to find these new capabilities, take care of the force and families, and meet the challenges of new missions comes from the shared priorities at the core of every SOF formation: people, win, transform. Join the nation's top SOF leaders and experts as we unite to tackle these threats together.

October 30 – 31, 2023 | Washington, DC | [NDIA.org/SOLIC](https://www.ndia.org/SOLIC)



Leading the Way in Engagement, Networking, and National Defense

Plan Ahead for Success | 2023 – 2024 Featured Meetings, Conferences, and Events



34th Annual NDIA SO/LIC Symposium

October 30 – 31, 2023 | Washington, DC



38th Annual National Logistics Forum

February 6 – 7, 2024 | Oklahoma City, OK



2024 Human Systems Conference

March 21 – 22, 2024 | Arlington, VA



2023 Aircraft Survivability Symposium

October 31 – November 2, 2023* | Monterey, CA



2024 Tactical Wheeled Vehicles Conference

February 26 – 28, 2024 | Charlotte, NC



2024 Ronald Reagan Missile Defense Conference

April 16 – 17, 2024 | Washington, DC



2023 Expeditionary Warfare Seminar

November 1*, 2024 | Arlington, VA



2024 Pacific Operational Science & Technology (POST) Conference

March 4 – 7*, 2024 | Honolulu, HI



MODSIM World 2024

May 20 – 22, 2024 | Norfolk, VA



I/ITSEC 2023

November 27 – December 1, 2023 | Orlando, FL



2024 Munitions Executive Summit

March 19 – 11, 2024 | Parsippany-Troy Hills, NJ



Training & Simulation Industry Symposium (TSIS) 2024

June 12 – 13, 2024 | Orlando, FL

*All Classified | **Partially Classified

Visit [NDIA.org/Events](https://www.ndia.org/Events) for more information on all of our meetings, conferences, and events.