

NTSA CYBER PAVILION

I/ITSEC 2021 • ORLANDO, FLORIDA • BOOTH #2870



SPONSORED BY:



BAE SYSTEMS



CYBER PAVILION

BOOTH 2870

The inaugural NTSA CYBER PAVILION is the meeting place for Cyber, Electromagnetic, and Information Warfare professionals to collaborate on needs and capabilities.

- **LEARN:** Hear from Defense leaders, Government Programs, Industry Partners (i.e., Current and Future Cyber Training Outlook, Electronic Warfare and Cyber Modeling and Simulation Capabilities, and others)
- **COMMUNICATE:** Discuss opportunities (i.e., Electronic Warfare and Cyber at the Tactical Level, integration of capabilities into staffs, EW/Cyber/SIGINT Integration, Understanding Mis & Dis-Information Campaigns, etc.)
- **PROVIDE:** Examples of current capabilities, ongoing work, contacts to pursue aligning solutions to needs
- **KING OF THE HILL EVENT** – Simulcast Tracking Event on Thursday, 2 December, 0830-1000

As the capabilities in these different fields continues to grow in each service, this pavilion will be a platform to help communicate and cooperate on finding solutions to this ever changing environment supporting the U.S. Government and Department of Defense, and other countries and commercial organizations. Senior leaders from many organizations will speak at the pavilion to provide a better understanding of current capabilities, and assist in communicating the needs of their organizations and services they provide — all part of the pavilion objectives.

OUTLOOK – COMMENTS FROM DEFENSE LEADERS

- Facilitated Panel – Service Principal Cyber Advisors
- Service Leaders discuss high level challenges facing the DoD and provide thoughts regarding applications to enhance understanding for these areas

OPPORTUNITIES – DISCUSSION ON NEEDS FROM PROGRAMS/PROJECTS

- Facilitated Panel – DoD PMs/PEOs & Capability Managers
- PMs discuss the needs of their specific programs regarding Cyber, Electromagnetic and Information Warfare topic areas
- Capability Managers discuss current and evolving requirements

OFFERINGS – INDUSTRY AND GOVERNMENT SOLUTIONS

- Facilitated Panel – Cyber Pavilion Sponsors
- Pavilion sponsors discuss corporate approaches to meet customer needs

NOTABLE ATTENDEES – NETWORKING CONTACTS

- Service Principal Cyber Advisors (Army, Navy and Air Force Advisors)
- Service PMs/PEOs
- DoD Capability Managers
- Industry Sponsors of the Cyber Pavilion

OTHER PAVILION ACTIVITIES: Presentations, exchanges with government, industry professionals – Kiosk presentation areas and main event stage setting for panel events and select presentations. Consider the Cyber Pavilion as your place to check in with other cyber professionals. Come join us at the Pavilion, find a booth facilitator to coordinate display of printed material or inquire about availability of Kiosk scheduled time for your presentations.

CYBER PAVILION MAJOR EVENT SCHEDULE

MONDAY, 29 NOVEMBER

(EXHIBITS 1400-1800)

Opportunities and Capabilities

1430 U.S. Army Combat Capabilities Development Command - Soldier Center (DEVCOM SC) Simulation & Training Technology Center (STTC); Army Cyber Institute (ACI), United States Military Academy (USMA)

TUESDAY, 30 NOVEMBER

(EXHIBITS 1200-1830)

Opportunities and Capabilities

1330 Offerings Panel (Cyber Pavilion Sponsors)

1430 Opportunities Panel (DoD PMs/PEOs & Capability Managers)

1530 Information Warfare Panel

WEDNESDAY, 1 DECEMBER

(EXHIBITS 0930-1800)

1000 Outlook Panel (Service Principal Cyber Advisors)

1100 Q&A session: King of the Hill

1330 Demonstration: Synthetic Internet for Training and Exercises (SITE) and Social Media Environment and Internet Replication (SMEIR)

THURSDAY, 2 DECEMBER

(EXHIBITS 0930-1500)

0830 King of the Hill Exercise simulcast

1000 Offerings Panel (Cyber Pavilion Sponsors)

1300 Demonstration: Synthetic Internet for Training and Exercises (SITE) and Social Media Environment and Internet Replication (SMEIR)

WITHIN THE CYBER PAVILION: Kiosk Presentations During Daily Exhibit Hall Hours

Four Kiosks with rotating presentations from Sponsors, Government Participants, and Industry Partners (Schedule available in the Cyber Pavilion)

PRINCIPAL CYBER ADVISOR BIOGRAPHIES

DEPARTMENT OF THE ARMY

MR. TERRY MITCHELL, SES

Mr. Terry Mitchell assumed the position as the Principal Cyber Advisor to the Secretary of the Army and the Army Chief of Staff on September 15, 2020. Mr. Mitchell is responsible for advising both the SA and CSA on all cyber matters and implementing the Department of Defense Cyber Strategy within the Army. As the PCA, he represents the Secretary at cyber-related senior DoD level forums to include the Cyber and Digital Modernization Monthly Meetings, the Deputy Management Action Group, etc. to inform and advocate for cyberspace activities. He is also responsible for implementing the Department of Defense Cyber Strategy within the Army by coordinating and overseeing the execution of the Army's policies and programs relevant to Cyber, including certification of the Army's Budget for Cyber activities.

Prior to his appointment as the Principal Cyber Advisor, Mr. Mitchell was assigned as the Director of the Army G-2 Plans and Integration Directorate since January 1, 2015. He lead the development of policy and plans and set conditions to meet or exceed anticipated Army Intelligence manning, equipping, training, resourcing, and readiness requirements. He oversaw the functional management of the signals intel-

ligence, geospatial intelligence, open source intelligence, and measurement and signatures intelligence disciplines. He led Army Intelligence initiatives to identify, exploit, and field new intelligence capabilities from across the military, agencies, academia, and industry, to enable their assessment, acquisition, and integration into the Force. The directorate integrates Army Intelligence, Surveillance and Reconnaissance technology across the Army and DoD. He directed the activities of an intelligence-focused science and technology community of interest that brings together members of the Intelligence Community, Military Services, academia, and industry to develop initiatives to assess the military utility and integration of emerging/leading-edge technologies. He oversaw the collaboration and synchronization between the G-2 staff and Army Futures Command.

Before this time with the G-2, Mr. Mitchell served as the Assistant Deputy Under Secretary of Defense for Command and Control in the Office of the Deputy Under Secretary of Defense (Advanced Systems & Concepts), where he formulated and executed policy, programs and initiatives to promote rapid transition of technologies and enabling operational concepts from applied engineering to field and sustained military capabilities to support joint missions. Programs directed by this office in-

clude Advanced Concept Technology Demonstrations, Joint Capability Technology Demonstrations, Technology Transition Initiative, Joint Warfare (Experimentation) Program and programs to enhance the Defense industrial base.

Mr. Mitchell retired from the Army in 2001 after an active duty career spanning twenty- seven years. His operational military assignments included duties in multiple Army Military Intelligence Battalions and intelligence centers in the European and Central Command theaters. He also served at the US Army Intelligence Center and School, designing programs of instruction for multidiscipline/multi-echelon intelligence systems. He also completed an assignment in the Office of the Secretary of Defense, Operational Test and Evaluation Office, where he was awarded the DoD Military Tester of the Year award for his test strategy and conduct of the Year 2000 (Y2K) Operational Evaluations.

DEPARTMENT OF THE NAVY

MR. CHRIS CLEARY, SES

Christopher Cleary was named the Department of the Navy Chief Principal Cyber Advisor (PCA) in November 2020. In this role, he is responsible for advising the Secretary of the Navy, Chief of Naval Operations, and Commandant of the Marine Corps and implementing the Department of Defense Cyber Strategy within the Department of the Navy (DON). Prior to being appointed as the PCA he was the DON Chief Information Security Officer (CISO) and Director of the DON CIO Cybersecurity Directorate.

Before returning to his roots in the Navy, Chris worked in the commercial sector as Vice President of Business Development and Strategy for Leidos' Cyber & SIGINT Solutions Operation, based in Columbia, Maryland. Chris's other commercial experience includes Director of Business Development, Tenable; Client Partner, Verizon Enterprise Solutions; Director of Cyber Intelligence, L3 Communications; President, Vir-Sec Government Services; and Senior Manager of Intelligence Programs, Sparta.

Chris is a retired Naval Reserve Officer who served 16 of 24 years on active duty in a variety of leadership roles supporting several commands including, US CYBER COMMAND, National Security Agency (NSA), Office of Naval Intelligence (ONI), National Reconnaissance Office (NRO), Joint Special Operations Command (JSOC), Assault Craft Unit TWO, and USS Simpson (FFG-56). Prior to receiving his commission, Chris spent four years as an F/A-18 Hornet avionics technician serving with The Desert Gladiators (VFA-106). Chris has deployed four times, twice supporting combat operations in Iraq.

He is a Certified Information Systems Security Professional (CISSP) and Program Management Professional (PMP). He has been a lecturer at the United States Naval Academy, Federal Aviation Administration, Naval Postgraduate School, The New School of Design, Montreat College, DEFCON Security Conference, and the National Defense University.

Chris graduated from the United States Naval Academy in

1996 and he obtained a Master of Arts in National Security and Strategic Studies from the Naval War College in 2012.

DEPARTMENT OF THE AIR FORCE

MS. WANDA T. JONES-HEATH, SES

Wanda T. Jones-Heath, a member of the Senior Executive Service, is the Principal Cyber Advisor for the Department of the Air Force, comprised of the U.S. Air Force and U.S. Space Force. As the Principal Cyber Advisor for the DAF, her duties include synchronizing, coordinating and overseeing the implementation of the DAF Cyber Strategy and advising the Secretary of the Air Force on all cyber programs. She is responsible for overseeing cyberspace recruitment; resourcing and training of cyber mission forces, as well as assessing their readiness; overseeing acquisition; advocate for cyber investments; cybersecurity supply chain risk management; security of information systems and weapon systems.

Prior to current position, Ms. Jones-Heath served as the Chief Information Security Officer and advised the Chief Information Officer on cybersecurity policy, cybersecurity programs, and cyber force development. She leads a Directorate comprised of military, civilian, and contractor personnel responsible for developing cybersecurity policy and strategy for over 5,000 Air Force information technology systems. She oversees risk management and cybersecurity accountability for information systems, weapon systems, and operational technology supporting military cyberspace operations. Her portfolio includes policy governing the defense industrial base, supply chain risk management, and cybersecurity capabilities. She has oversight for the Freedom of Information Act, Privacy Act laws, and cryptographic modernization supporting cyber operations.

Since entering civil service, Ms. Jones-Heath has held technical and leadership positions performing cyber operations and cybersecurity duties in communications units from the squadron to the wing level and she has served in headquarters units at the major command, agency, and Air Staff level. Her experience includes extensive joint and interagency work along with cross functional assignments with duties such as testing, assessments, lessons learned management, strategy development and other functions in organizations both within and outside of the communications field.

Ms. Jones-Heath graduated from the University of South Carolina in 1990 with a degree in Computer Science. She began her Civil Service career as a Palace Acquire Intern, Information Systems Specialist, in various functional areas. She moved to Headquarters Air Combat Command, Langley Air Force Base, Virginia, in 1993. There, she held positions responsible for policy and guidance for security and network systems. Prior to arriving at the Headquarters Air Force staff, Ms. Jones-Heath was the Program Manager for Mobility with the Defense Information Systems Agency. Ms. Jones-Heath led the effort to establish a Department of Defense Mobile capability to include infrastructure.