TechNet Cyber 2025

What You Missed

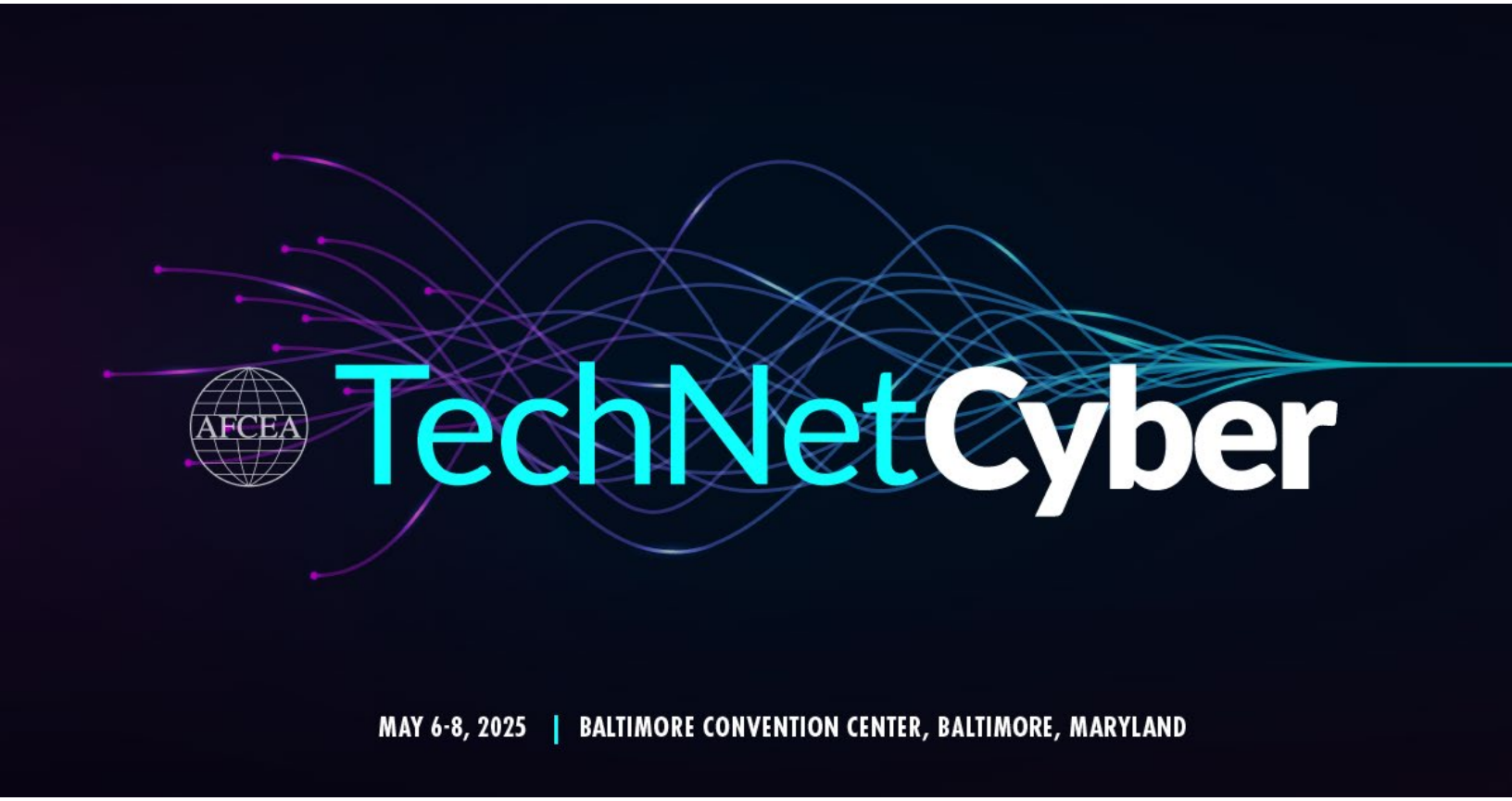

Table of Contents:

Executive Summary

TechNet Cyber 2025 brought together members of government, industry, and academia to discuss pressing challenges facing the DoD. This year's theme was "Empowering the Warfighter: Innovate, Integrate, Dominate."

The DoD is undergoing a rapid digital transformation. Spurred on by it's goal to achieve zero trust by 2027, and in light of new administration priorities, the DoD is aiming to tackle it's challenges quicker than ever before.

The DoD is moving to adopt new security controls through it's Software Fast Track (SWFT) to radically transform Authorities to Operate (ATO) and deploy software fast. To do this, the DoD is working to adopt AI-enabled cybersecurity tools at scale and is taking new action such as sunsetting the Approved Product List (APL).

With the DoD's zero trust journey well underway, officials shared their progress on the initiative. Agencies like DISA and the Navy have made great strides at beating the 2027 deadline and deploying operational zero trust capabilities today. Other officials shared challenges they've run into on the road to zero trust—highlighting issues such as aging infrastructure and the need for a large culture shift.

Across every agency though, the message was clear. This year is a year of action and bringing capabilities that once existed on a whiteboard into operational reality.

Please reach out to the Market Research Team at Research@carahsoft.com if you have any questions or would like more information.

Artificial Intelligence

- **AI is Transforming Warfare:** The cyber professionals on the panel **Keeping Pace with the Adversary and the Warfighter: Data-Centric Operations** were asked "Which technology will shape the future of warfare the most?" The majority responded with Artificial Intelligence, while some included Unmanned Systems and Virtual Reality in their responses. **[Panel: Keeping Pace with the Adversary and the Warfighter: Data-Centric Operations]**

Cloud

- **DoD Cloud Challenges:** Jerry Newell, Senior Technical Advisor for the Hybrid Computing Line of Business at the Defense Information Systems Agency (DISA) listed some of the cloud-related challenges that the DoD faces. Newell stated that biggest challenges are Slow and Costly IT Procurement, Lack of Cost Transparency, Security and Compliance Risks, Complex Multi-Cloud Environments, and Operational Inefficiencies. **[Distributed Hybrid Multi Cloud]**
- **Distributed Hybrid Cloud Model:** The Distributed Hybrid Cloud Model (DHCM) is seeking to solve some of the challenges listed above, and has already gone through an Other Transaction Authority (OTA). Some of it's features include a Single Management Portal, an On-Prem Cloud Environment, Commercial Cloud Assets, Containers, Traditional Virtualized Assets, Dedicated Hosts, and Networking. **[Distributed Hybrid Multi Cloud]**

Cyber

- **What's Next for Zero Trust in Navy:** David Voelker, Zero Trust Architecture Lead for the Department of the Navy discussed what they're working on next with their zero trust effort Flank Speed. The Navy needs autonomous penetration testing, need to identify which of their 152 zero trust capabilities are applicable to their baseline, and how to help their over 2,000 programs identify, buy, and deploy these capabilities by the end of FY27. **[Panel: DoD Zero Trust Success Stories]**
- **Rise of "Purple Teaming":** Randy Resnick, Chief of Zero Trust and DoD Deputy CIO for Cybersecurity described the new types of testing the DoD needed to conduct to progress their zero trust goals. Many traditional programs run "attack-fix" models, or red-teaming then blue-teaming, that often take 9-months or more to get to that "fix" activity. For zero trust, DoD brought in "purple teams" that could resolve fixes immediately as red teams were active. **[Panel: DoD Zero Trust Success Stories]**

"When in doubt, collect the telemetry, you never know what new or novel adversary techniques you may find."

Ian Leatherman, *Zero Trust Strategy Lead*, Microsoft US Federal

- **Takeaways from Flank Speed:** Ian Leatherman, Zero Trust Strategy Lead for Microsoft US Federal had a few major takeaways from Microsoft's work on Flank Speed. The first is that every person in the organization has to be involved in security, it is not just a technology solution. The second is how critical visibility is. Mr. Leatherman stated, "When in doubt, collect the telemetry, you never know what new or novel adversary techniques you may find." **[Panel: DoD Zero Trust Success Stories]**
- **Deploying Zero Trust at Scale:** The Zero Trust Portfolio Office set their DoD-wide zero trust adoption target as the end of FY27, however, Flank Speed is already operational. David Voelker, Zero Trust Architecture Lead at the Department of the Navy noted that the Flank Speed configuration could be lifted and shifted to other customers in the DoD and could likely deploy it in about 24 hours. Mr. Voelker also says he might considered an automated way to do this lift and shift. Ian Leatherman, Zero Trust Strategy Lead for Microsoft US Federal said that the DoD already has the technology to do this, but the last mile for a deployment like that would be a culture challenge. Mr. Leatherman asked "How many commanders know how many endpoints, applications, and users are on their network at any given time?" **[Panel: DoD Zero Trust Success Stories]**
- **Successes and Challenges at the National Guard Bureau:** The National Guard Bureau has made a lot of progress on zero trust. The Bureau had to develop its own Zero Trust Plan separate from Army and Air Force due to some of the different responsibilities the Guard is tasked with. The National Guard has also run into unique challenges as they must interact with State, Local, and Tribal authorities at a different level than the services do. The National Guard Bureau is looking to upgrade its tactical communications in the homeland. **[Panel: Keeping Pace with the Adversary and the Warfighter: Data-Centric Operations]**
- **Every Marine a Cyber Warrior:** COL Dennis W. Katolin, AC/S G-3 at the United States Marine Corps Forces Cyberspace Command stated that his number one priority is getting every Marine proficient in cyber and data. He believes that the Marines are treating cyberspace like they used to treat the aviation combat element with many saying "we know how to use it, but you folks do it". COL Katolin believes there needs to be a shift away from this mindset. **[Panel: Keeping Pace with the Adversary and the Warfighter: Data-Centric Operations]**

- **Command & Control Being Challenged:** CAPT Joseph E. Meuse, Deputy Commander of the Coast Guard Cyber Command said that one of his biggest takeaways from recent cyberattacks is how quickly the Coast Guard's command and control structure could be challenged. The Coast Guard in particular is very used to operating in a kinetic environment with set geographic responsibilities, however, the adversary doesn't respect those random geographic boundaries they've set. **[Panel: Keeping Pace with the Adversary and the Warfighter: Data-Centric Operations]**

- **Cyber as a Critical Function:** Jane Rathbun, Chief Information Officer for the Department of the Navy stated that every capability they build or deploy has two customers: the first is the warfighter and the second is the cyber operator who has to secure that capability. Industry should keep this in mind when designing products and pitching them to the DoD. **[Panel: Service CIO Update]**

- **Software Fast Track Steps:** Katie Arrington, Acting Department of Defense Chief Information Officer discussed the Software Fast Track (SWFT) set to launch on June 1st, 2025. The initiative will replace the traditional Authority to Operate (ATO) structure and add requirements for contractors including: a third-party Software Bill of Materials (SBOM), a third-party risk assessment, populate the Enterprise Mission Assurance Support Service (eMASS) with artifacts, and after that contractors will get a Provisional ATO. Ms. Arrington stated "We're going to blow up the [Risk Management Framework] RMF" and have industry tell DoD what is and isn't working. Paper compliance isn't enough anymore, Ms. Arrington is looking for "continuous monitoring, red teaming, and people to continually evaluate their capability." **[Keynote]**

Software Fast Track (SWFT): The Software Fast Track (SWFT) is changing the way the DoD manages risks and conducts it's Authority to Operate (ATO). Contractors can get involved with the latest software acquisition and risk management changes by participating in the three recently released RFIs. These RFIs include RFI – Software Fast Track (SWFT) Tools, RFI – Software Fast Track (SWFT) External Assessment Methodologies, and RFI – Software Fast Track (SWFT) Automation & Artificial Intelligence (AI). These RFIs close May 20th. **[DoD Software Modernization Senior Steering Group]**

- **Approved Products List to be Sunset:** Katie Arrington stated that the DoD will be sunsetting the Approved Products List (APL) and that they're no longer sponsoring additions to the list. The SWFT initiative will take over the role and establish a "trust, but verify" procedure for it. Ms. Arrington said "I'm more worried about red teaming than I am about an Approved Products List." **[Keynote]**

- **Cyber as a Core Function:** Wanda Jones-Heath, Ph.D., Principal Cyber Advisor at the Department of the Air Force discussed the best way to accelerate the integration of cyber capabilities across the department. If cyber is considered a core function rather than a support function the DoD has to think about where they invest money to better enable that function. This includes areas like software factories that help produce tools and the cyber ranges to test them. Ms. Jones-Heath ask for industry was to build capabilities at speed. **[Panel: Cyber Readiness 2025 and Beyond: Innovating, Integrating, and Empowering the Warfighter]**

- **Cyber as an Acquisition Pillar:** Anne M. Schumann, Principal Cyber Advisor at the Department of the Navy recommended that cyber be a pillar alongside Cost Schedule Performance in traditional acquisitions. She believes that because it isn't built in, there isn't as much attention paid to it, and often times it can be considered a "trade-off". **[Panel: Cyber Readiness 2025 and Beyond: Innovating, Integrating, and Empowering the Warfighter]**

> *"A lot of our advancements in cybersecurity have been geared at the IT space and that's great but we need to rapidly apply our lessons learned to our operation technology—both to our critical infrastructure and our weapons platforms."*
>
> **Anne M. Schumann,** *Principal Cyber Advisor*, Department of the Navy

- **Challenges with Securing Operation Technology:** Anne Schumann also discussed how the Navy is looking to secure operational technology. Ms. Schumann said, "A lot of our advancements in cybersecurity have been geared at the IT space and that's great but we need to rapidly apply our lessons learned to our operation technology—both to our critical infrastructure and our weapons platforms." She said that one of the things missing they have on the IT side that they're missing from the operational side is a common framework. The Navy has published their MOSAICS framework to try to address some of these challenges and is looking for a mechanism to allow industry to provide their input on it. **[Panel: Cyber Readiness 2025 and Beyond: Innovating, Integrating, and Empowering the Warfighter]**

- **Securing Critical Infrastructure:** Chief Warrant Officer 5 Matthias J. Ingle, Sr., Senior Technical Advisor at the Office of the Principal Cyber Advisor in the Department of the Army talked about some of the restructuring the Army is undergoing to better achieve its cybersecurity mission. In December of last year the Army senior leaders restructured the governance process for cybersecurity related to operational technology and critical infrastructure. The Army National Guard is now tasked with working closely with utility companies to build trust and provide support in the event of future cyberattacks. **[Panel: Cyber Readiness 2025 and Beyond: Innovating, Integrating, and Empowering the Warfighter]**

- **Challenges to Zero Trust Deployment:** Anne Schumann said one of the greatest challenges to fully deploying zero trust by 2027 is the aging infrastructure that wasn't developed with zero trust security controls in mind. Adding those controls or removing those systems is slow and expensive. Even more difficult is applying those controls to older weapon systems in sustainment that cannot be "ripped and replaced" like other systems. **[Panel: Cyber Readiness 2025 and Beyond: Innovating, Integrating, and Empowering the Warfighter]**

> *"What I wish for is a sensored network and battlefield that is automated and reports to those defenders when someone is knocking at the door."*
>
> **LTG Jeth B. Rey,** *Deputy Chief of Staff*, G-6, United States Army

- **Sensors on the Network:** LTG Jeth B. Rey, Deputy Chief of Staff at G-6 for the United States Army discussed what his desired end-state for the network is. LG Rey said, "What I wish for is a sensored network and battlefield that is automated and reports to those defenders when someone is knocking at the door." He used the example of an airplane cockpit that can tell the pilot when the cargo bay door is open or if the cabin is losing oxygen. The pilot has all of that information fed to them so that they can make a decision fast. LTG Rey wants cyber defenders to be able to be proactive rather than reactive and a heavily sensored network enables that. **[Fireside Chat: Command at the Speed of Relevance: From Data, Networks, and C2 to Decision in the Digital Battlespace]**
- **Components of the Unified Network:** LTG Jeth Rey also described the structure of their Unified Network 2.0 and the key components it is comprised of. The first component is Robust Transport—which Rey believes the Army has achieved over the past three and a half years. The second component is Cloud-Enabled—which the Army is continuing to evolve on. The final component is Zero Trust—which the Army is still working on. LTG Rey said that he wants an identity that can move from the tactical edge to the enterprise that provides access to data and has attribute-bases security controls. **[Fireside Chat: Command at the Speed of Relevance: From Data, Networks, and C2 to Decision in the Digital Battlespace]**
- **How Army is Moving Forward on the Unified Network:** LTG Jeth Rey said that the unified network has an operational, strategic, and tactical piece. On the operational side, the Army is acquiring software-defined and cloud-enabled solutions. On the strategic side, the Army is converging networks across the board. On the tactical side, the Army is pursuing lighter, more lethal capabilities. **[Fireside Chat: Command at the Speed of Relevance: From Data, Networks, and C2 to Decision in the Digital Battlespace]**

Doing Business

> *"Do you really need to have a unique capability or are there SaaS solutions out there? That way you can really focus on those unique unicorns."*
>
> **William R. (Bill) Dunlap, Jr.,** *Acting Deputy Chief Information Officer for Information Enterprise,* Office of the DoD Chief Information Officer

- **Key Drivers for Acquisition Reform:** The DoD is working on streamlining it's procurement and Sean Brady, Senior Lead for Software Acquisition Enablers at the Office of the Undersecretary of Defense (Acquisition and Sustainment) explained that there are two key drivers to this transformation. The first is mission, software allows the DoD to adapt it's systems to rapidly changing threats. The second is access to commercial innovation, which allows the DoD access to products than go from idea to deployment in weeks and months rather than years. William R. (Bill) Dunlap, Jr., Acting Deputy Chief Information Officer for Information Enterprise at the Office of the DoD Chief Information Officer added his perspective on DoD's focus on custom solutions asking the question, "Do you really need to have a unique capability or are there SaaS solutions out there? That way you can really focus on those unique unicorns." **[DoD Software Modernization Senior Steering Group]**
- **Four Efforts Driving Digital Transformation:** Thomas W. Simms, Principal Deputy Executive Director for Systems Engineering and Architecture at the Office of the Under Secretary of Defense for Research and Engineering described the four major digital transformation efforts within the DoD. The first is the Modular Open Systems Approach (MOSA) that is driving design to become more modular and is a congressional requirement. The second is the DoD's Digital Engineering Instruction requiring programs to use digital engineering in their design process. The third is APIs that help make the DoD more data-centric and is driven by the DoD's API guidebook. The fourth is the DoD's System Engineering Guidebook which is currently undergoing an update to incorporate guidance from the Secretary of Defense's latest memos. **[DoD Software Modernization Senior Steering Group]**
- **Smaller Services as a Testbed:** Venice Goodwine, the outgoing Chief Information Officer for the Department of the Air Force explained how the smaller services like the Space Force and Marine Corps are small and nimble, making them a perfect testbed for enterprise capabilities. While this can be a good thing, there is the risk of creating a lot of shadow IT within the organizations because of it. **[Panel: Service CIO Update]**

- **How Industry Should Pitch to DoD:** Venice Goodwin also offered some advice to industry on how to navigate some of the changes happening within DoD. She recommended industry practice some "extreme teaming" and pitch how their capability can be deployed across all services. In the past, industry has gone to each service individually, but now the DoD is prioritizing capabilities that can benefit everyone across the department. Solutions should be useful in every domain across land, sea, air, space, etc. RDML Russell E. (Rusty) Dash, Assistant Commandant for C4 & IT and Chief Information Officer for the U.S. Coast Guard added "This administration is absolutely focused on outcomes and results," noting that there is added pressure to deploy capabilities fast rather than just talk about them. **[Panel: Service CIO Update]**
- **Increased Importance of Interoperability:** RDML Dash also discussed the growing importance of interoperability between military and law enforcement functions, particularly between the Coast Guard and Navy. Last month the Navy deployed two destroyers to the border as part of security operations, and the Coast Guard has been working hard to ensure interoperability and communication between the military and law enforcement arms conducting operations there. **[Panel: Service CIO Update]**
- **Lowest Price Technically Acceptable:** Katie Arrington, Acting Department of Defense Chief Information Officer alluded to the fact the DoD will likely try to avoid Lowest Price Technically Acceptable (LPTA) terms stating, "If you're worried about Lowest Rate Technically Acceptable that is a four letter word we're not in love with." **[Keynote]**

Appendix: TechNet Cyber 2025 Sessions Attended

Tuesday, May 6th

Conference Opening and Keynote Address

- LTG Susan S. Lawrence, USA (Ret.), President and Chief Executive Officer, AFCEA International
- Mr. Christopher Barnhurst, Deputy Director, Defense Information Systems Agency (DISA)
- BG Heather Blackwell, Deputy Commander, Joint Force Headquarters Department of Defense Information Network (JFHQ-DODIN)

Panel: DoD Zero Trust Success Stories

- Randy Resnick, Chief of Zero Trust, DoD Deputy CIO for Cybersecurity, Office of the DoD
- Ian Leatherman, Zero Trust Strategy Lead, Microsoft US Federal
- David Voelker, Zero Trust Architecture Lead, Department of the Navy
- Herb Kelsey, Lead for Dell Project Fort Zero and Dell Federal Chief Technology Officer, Dell Technologies
- Christopher (Chris) Pymm, DISA Zero Trust Portfolio Lead, Thunderdome Program Manager, Defense Information Systems Agency

DoD Software Modernization Senior Steering Group

- Robert W. (Rob) Vietmeyer, Chief Software Officer for the Deputy Chief Information Officer for Information Enterprise (DCIO(IE)), Office of the DoD Chief Information Officer
- Sean Brady, Senior Lead for Software Acquisition Enablers, Office of the Undersecretary of Defense (Acquisition and Sustainment)
- Thomas W. Simms, Principal Deputy Executive Director, Systems Engineering and Architecture, Office of the Under Secretary of Defense for Research and Engineering
- William R. (Bill) Dunlap, Jr., Acting Deputy Chief Information Officer for Information Enterprise, Office of the DoD Chief Information Officer

Panel: Keeping Pace with the Adversary and the Warfighter: Data-Centric Operations

- LtGen Matthew G. Glavy, USMC (Ret.), Former Deputy Commandant for Information, Headquarters, U.S. Marine Corps
- COL Heath A. Giesecke, USA, Director, Enterprise Cloud Management Agency, U.S. Army
- Kenneth C. McNeill, Chief Information Officer and Director, C4 Systems Directorate, National Guard Bureau
- Col John W. Picklesimer, USAF, Commander, 67 Cyber Wing, Sixteenth Air Force
- Major General (Air Vice-Marshal) Armin Fleischmann, Commander CID Support Forces and DCOS Capabilities, CID Command, Bonn

- Col Dennis W. Katolin, USMC, AC/S G-3, United States Marine Corps Forces Cyberspace Command
- CAPT Joseph E. Meuse, USCG, Deputy Commander, Coast Guard Cyber Command

Wednesday, May 7th

Keynote

- Ashley Manning, Principal Deputy Assistant Secretary of Defense for Cyber Policy, U.S. Department of Defense

Panel: Service CIO Update

- MG Garrett Yee, USA (Ret.), Vice President, DoD Customer Relations, General Dynamics Information Technology
- Venice Goodwine, Chief Information Officer, Department of the Air Force
- BG Urbi Lewis, USA, Director for Cybersecurity/CISO, HQDA, Office of the CIO
- RDML Russell E. (Rusty) Dash, USCG, Assistant Commandant for C4 & IT and Chief Information Officer, U.S. Coast Guard
- SES II Jeffery A. Hurley, Director (Acting) Information Command, Control, Communications and Computers (IC4), Deputy Commandant, Information-HQMC
- Jane Rathbun, Chief Information Officer, Department of the Navy

Keynote

- Katherine (Katie) Arrington, Performing the Duties of the Department of Defense Chief Information Officer, Department of Defense

Panel: Cyber Readiness 2025 and Beyond: Innovating, Integrating, and Empowering the Warfighter

- BG Terrence A. Adams, Deputy Principal Cyber Advisor to the Secretary of Defense and Senior Military Advisor for Cyber Policy
- Wanda Jones-Heath, Ph.D., Principal Cyber Advisor, Department of the Air Force
- CW5 Matthias J. Ingle, Sr., USA, Senior Technical Advisor, Office of the Principal Cyber Advisor, Department of the Army
- Anne M. Schumann, Principal Cyber Advisor, Department of the Navy

Thursday, May 8th

Fireside Chat: Command at the Speed of Relevance: From Data, Networks, and C2 to Decision in the Digital Battlespace

- LTG Susan S. Lawrence, USA (Ret.), President and Chief Executive Officer, AFCEA International
- LTG Jeth B. Rey, USA, Deputy Chief of Staff, G-6, United States Army
- LTG David T. (Todd) Isaacson, USA, Director for Command, Control, Communications and Computers (C4)/Cyber, Chief Information Officer, J-6, Joint Chiefs of Staff

Distributed Hybrid Multi Cloud

- Zachary Funt, Technical Advisor, Hybrid Computing Line of Business, Defense Information Systems Agency
- Jeremie Lane, Technical Advisor, Hybrid Computing Line of Business, Defense Information Systems Agency
- Forrest Holifield, Senior Technical Advisor, Hosting and Compute, Defense Information System Agency
- Jerry Newell, Senior Technical Advisor, Hybrid Computing Line of Business, Defense Information Systems Agency