Defense Strategies Institute professional educational forum:

4th Annual Cyber Operations for National Defense Symposium

~ Advancing Cyber Capabilities in Support of Multi-Domain Battle ~

August 2-3, 2017

Mary M. Gates Learning Center | Alexandria, VA

August 2, 2017	
8:00 – 8:45	*Registration and Light Breakfast Reception Open*
8:45 – 9:00	**Moderator Opening Remarks** **Maj Gen Jim Keffer, USAF (Ret)** Director of Cyber, Lockheed Martin Government Affairs
9:00 – 9:40	**Integrating Navy's Fleet Commands to Assimilate Cyber Operations Afloat and Ashore** -Operating and defending Navy networks in ship-shore communication systems -Providing uninterrupted command and control capability across the rest of the Navy -Defending Navy networks and global telecommunication systems **CAPT Andrew Stewart, USN (Confirmed)** Assistant Chief of Staff for Operations, N3 Director, Maritime Operations Center US Fleet Cyber Command/US Tenth Fleet
9:40 – 10:20	**Keynote Remarks:** **The Formation of a Unified Combatant Command** -Elevating US Cyber Command into a full-fledged unified combatant command -The creation of a UCC as the most effective solution to further cyber operations **Maj Gen Burke "Ed" Wilson, USAF (Confirmed)** Deputy Principal Cyber Advisor to the Secretary of Defense Senior Military Advisor for Cyber, Office of the Under Secretary of Defense for Policy, OSD
10:20 – 10:45	*Networking Break*
10:45 – 11:25	**Delivering US Army Cyber Capabilities in Support of Multi-Domain Battle** -Defending networks, data, and weapons systems -Delivering effects against our adversaries in and through cyberspace -Designing, building, deploying and integrating capabilities for the future fight, spanning cyberspace, electronic warfare, and information operations **BG Joseph McGee, USA (Confirmed)** Deputy Commander for Operations US Army Cyber Command
11:25 – 12:05	**Policy, Strategy, and Initiatives at DoD CIO to Enhance Departmental Cybersecurity** -Advancing cyber basics and improving cyber defenses -Coordinating cybersecurity standards, policies, and procedures across federal agencies, coalition partners, and industry -Ensuring the successful mission execution in the face of cyber warfare by a capable adversary **Essye Miller (Confirmed)** Deputy CIO for Cybersecurity DoD
12:05 – 12:45	**US Army's Strategy for Network Modernization to Enhance Cybersecurity** -Future network initiatives and capabilities for the US Army -Challenges and effects of creating one standard architecture -Funding perspective towards Army modernization deadlines **MG Garrett Yee, USA (Invited)** Director Cybersecurity Directorate HQDA CIO/G6

12:45 – 1:45	*Networking Lunch*
1:45 – 2:25	**Supporting National Security and the Warfighter through Effective Oversight of the Defense Industry** -Collecting, analyzing, and providing threat information to industry and government partners -Securing the nation's technological base -Providing information technology services that support the industrial security mission of DoD and its partner agencies **Richard Naylor (Confirmed)** Senior Cyber Advisor & Deputy Director Counterintelligence, Cyber Operations Defense Security Service
2:25 – 3:05	**Air Force Cyber's Warfighter Perspective** -Integrating cyber threats, electronic warfare, enemy surveillance and kinetic threats -Understanding how to best integrate and learn the capabilities and limitations to become ready to use integrated resources for maximum effect against our adversaries **Col Robert Cole, USAF (Confirmed)** Director Air Force Cyber Command Forward (AFCYBER)
3:05-3:25	**Networking Break**
3:25-4:05	**Implementing the U.S. International Strategy for Cyberspace** -US diplomatic efforts to advance an open, interoperable, secure, and reliable internet and information infrastructure -Promoting norms of responsible state behavior and cyber stability, advancing cybersecurity and fighting cybercrime -Reducing threats worldwide by combatting operational threats and large-scale cyber intrusions **Christopher Painter (Confirmed)** Coordinator for Cyber Issues US Department of State
4:05 – 4:45	**Building a Threat-Based Cyber Team** -Case study and incident response detailing the change in focus and philosophy of defensive cyber operations -Maturing and evolving to meet cyber adversary challenges -Defining threats, identifying gaps in cyber operations, and creating threat visibility **Anthony Talamantes (Confirmed)** Manager, Defensive Cyber Operations Johns Hopkins University Applied Physics Laboratory
August 3, 2017	
8:15 – 8:45	*Registration and Light Breakfast Reception Open*
8:45 – 9:00	**Moderator Opening Remarks** **Maj Gen Jim Keffer, USAF (Ret)** Director of Cyber, Lockheed Martin Government Affairs

9:00 – 9:40	**Strengthening the Government's National Security Efforts by Combatting Cyber Threats** -Supervising the investigation and prosecution of cases affecting national security, foreign relations, and export of military strategic commodities and technology -Investigating, disrupting, and deterring malicious cyber activities -Building on the creation of the National Security Cyber Specialist network, with its goal to get ahead of the threat and continue to enhance its focus on cyber threats to national security **Sean Newell (Confirmed)** Deputy Chief, Cyber National Security Division U.S. Department of Justice
9:40 – 10:20	***Keynote Remarks:*** **Air Force Cyberspace Strategy and Policy** -Assisting and providing operational requirements that guide development and management of Air Force cyberspace forces -Allocating operationally ready cyberspace forces and capabilities -The changing nature of warfare allowing Air Force to be proactive with cyber at the squadron level **Maj Gen Patrick Higby, USAF (Confirmed)** Director, Cyberspace Strategy and Policy Office Information Officer, Office of the Secretary of the Air Force
10:20 – 10:50	*Networking Break*
10:50 – 11:30	**The Impact of Cloud Services in Improving CIA's Cybersecurity Posture** -The significance of cloud to efficiently implement systems and secure workloads -Cloud's ability to improve the speed at which the agency is able to carry out cybersecurity audits on IT systems -The success of the mutually beneficial vendor-customer relationship with Amazon Web Services **Sherrill Nicely (Confirmed)** Chief Information Security Officer CIA
11:30 – 12:10	**DHS' Innovative Approaches to Drive Change in Cybersecurity Risk Management** -Establishing metrics with measurable impact on improving cybersecurity for Federal Civilian Executive Branch departments and agencies -Gathering cybersecurity requirements and developing operational policies for federal government -Leveraging best practices and lessons learned in support of Federal Civilian Executive Branch departments' and agencies' cyber hygiene **Mark Kneidinger (Confirmed)** Director, Federal Network Resilience Office of Cybersecurity and Communications DHS
12:10 – 1:10	***Panel Discussion:*** **Addressing the National Cybersecurity Workforce Shortage** *This panel will bring together Government and educational leaders to discuss the pressing issue of cybersecurity education and training, and how to effectively deal with the ever-changing field as it has become a national priority. Panelists joining us for this discussion will provide delegates with updates on the efforts and challenges in filling a workforce that aims to protect government infrastructure and critical systems. Members of the panel will deliberate the issues preventing federal agencies from attracting cyber talent, expanding cybersecurity through education and training and lastly, how to effectively identify and retain such talent.*

	Moderator: **Dr. Frank Kesterman,** Professor of Cybersecurity and Homeland Security, Manager Cybersecurity Employer and Industry Relations, University of Maryland University College **(Confirmed)** **Panelists:** **Dr. Victor Piotrowski**, Lead Program Director, CyberCorps, National Science Foundation **(Confirmed)** **Harry Wingo**, Professor, Cyber Security Department, College of Information and Cyberspace, National Defense University **(Confirmed)** **Lisa Dorr**, Director of IT Workforce Planning & Development, US Department of Health and Human Services **(Confirmed)**
1:10 – 1:45	*Networking Lunch*
1:45 – 2:20	**Maintaining a Strong and Resilient Economy by Protecting Against Cyberattacks** -Providing a competitive and secure global trade environment through strong cyber networks and systems -Focusing on the significance of public-private partnership due to varying natures of a cyberattack -Improving cyber response capabilities by increasing information sharing **Matthew Eggers (Confirmed)** Executive Director, Cybersecurity Policy National Security and Emergency Preparedness Dept. U.S. Chamber of Commerce
2:20 – 3:00	**Current Cyber Challenges Affecting Government Networks** -Providing proactive, predictive, and adaptive cyber security services for the senators, committees, and subcommittees -Allowing users to understand threat data to understand vulnerabilities to better secure the network -Leveraging organizations' risk management framework to better employ cybersecurity **Linus Barloon (Confirmed)** Director of Cybersecurity Office of the Sergeant at Arms US Senate
3:00– 3:40	**Why is Cybersecurity so Difficult and What Can we do About It?** -Lincoln Lab's co-design approach in order to meet security and functionality requirements -Development of system solutions for challenging critical missions including collecting, processing, and exchanging sensitive information in compliance with DoD cyber security requirements -The use of embedded computing to enhance DoD systems **Dr. Michael Vai (Confirmed)** Senior Technical Staff Secure Resilient Systems and Technology Group MIT Lincoln Laboratory
3:40	**End of Symposium**