

POWER TO CONNECT



ENTERPRISE WITHIN REACH

DISA

**CUSTOMER & INDUSTRY
FORUM 2011**

PROGRAM GUIDE

**AUGUST 15-18, 2011
BALTIMORE CONVENTION CENTER
BALTIMORE, MARYLAND**



Welcome to the DISA Customer and Industry Forum 2011. This is a great opportunity for all of us — DISA and our mission partners in the Services, Combatant Commands, Agencies, coalition forces — to actively engage in a focused training environment to collaborate, share information, and exploit the opportunity to directly engage with industry on innovative technologies to enable and ensure capabilities in support of our Warfighters and National-Level Leadership.

Our theme, *“Power to Connect: Enterprise Within Reach”* conveys two important concepts that direct our strategic focus.

“Power to Connect” expresses our operational objective to achieve and provide our users global access to the protected, enterprise infrastructure and services from anywhere, anytime, and from any device to leverage information, enabling decisive decision making.

"Enterprise Within Reach" represents the significant progress that collectively we have made toward a defense enterprise information environment. This is an integrated platform, which includes the network, computing environment, services, information assurance, and NetOps capabilities. The enterprise information environment will provide the ability for Warfighters to connect, identify themselves, discover and share information, and collaborate across the full spectrum of military operations. It is the foundation for enterprise-wide capabilities and common services that will enable operational effectiveness and achieve efficiencies.

Our partnerships are absolutely essential and will determine our ultimate success. That's why I encourage you to fully and actively engage in every part of this forum. This is an unique opportunity to hear from exceptional speakers, who are both innovators and thought-provoking leaders, and to attend tracks sessions built around our Lines of Operations and Joint Enablers. Our intent is to stimulate your thinking and your direct and active involvement, the exchange of information, and the generation and sharing of innovative ideas will move us closer to our objective —

*"Power to Connect:
Enterprise Within Reach."*



Carroll F. Pollett
Lieutenant General, USA
Director, DISA

USEFUL INFORMATION

Conference Agenda	4
Speaker Biographies	10
Tracks and Sessions Synopses & Schedules	13
Convention Maps	38
DISA Exhibit	40

REGISTRATION HOURS

Monday, August 15	11 a.m. – 6:30 p.m.	Charles Street Lobby
Tuesday, August 16	6:30 a.m. – 5 p.m.	Charles Street Lobby
Wednesday, August 17	6:30 a.m. – 5 p.m.	Charles Street Lobby
Thursday, August 18	6:30 a.m. – 3 p.m.	Charles Street Lobby

EXHIBIT HOURS

Monday, August 15	4:30 p.m. – 6:30 p.m.	Exhibit Hall A - D
Tuesday, August 16	9:45 a.m. – 5 p.m.	Exhibit Hall A - D
Wednesday, August 17	9:45 a.m. – 7 p.m.	Exhibit Hall A - D
Thursday, August 18	9:45 a.m. – 3 p.m.	Exhibit Hall A - D

USEFUL INFORMATION

Location Information

Baltimore Convention Center
One West Pratt Street
Baltimore, Maryland 21201
Phone: (410) 649-7000

Attire

The uniform for military personnel attending the Customer and Industry Forum is Class B's. Civilian attire for the conference is business casual.

Cyber Cafe

Access to personal email is available in the Cyber Café. The Cyber Café is located in the exhibit hall during exhibit hall hours.

DISA Conference Operations Support Center

The conference operations support center (Ops Center) is located in room 320. Limited office supplies, a copier, printer, and telephone are available for use by conference attendees.

Business Hours:

Monday, August 15	8 a.m. – 4:30 p.m.
Tuesday, August 16	6:30 a.m. – 5 p.m.
Wednesday, August 17	6:30 a.m. – 6 p.m.
Thursday, August 18	6:30 a.m. – 5 p.m.

CONNECTION CENTRAL

Meet and greet DISA's senior leaders and find out what's new at DISA!
Connection Central is located in the DISA Pavilion of the Exhibit Hall.

Tuesday, August 16

11:30 p.m. - 12 p.m.

Tony Montemarano, Component Acquisition Executive
Richard Hale, Chief Information Assurance Executive
Alfred Rivera, Director, Computing Services

1:30 p.m. - 2 p.m.

Gerald Doyle, Director, Enterprise Engineering
Steven Hutchison, Test and Evaluation Executive
Cindy Moran, Director, Network Services

2 p.m. - 2:30 p.m.

Thomas Ainsworth, Chief, Corporate Planning & Mission Integration
Jimaye Sones, Chief Financial Executive/
Comptroller
Jack Penkoske, Director, Manpower, Personnel & Security

2:30 p.m. - 3 p.m.

Mark Orndorff, PEO, Mission Assurance and Network Services
Bruce Bennett, PEO, Communications
Henry Sienkiewicz, Chief Information Officer

3 p.m. - 3:30 p.m.

Larry Huffman, Principal Director, Operations
Alan Lewis, Vice Director, Computing Services
William Brougham, Vice Director, Network Services

Wednesday, August 17

12 p.m. - 12:30 p.m.

Becky Harris, Vice Component Acquisition Executive
Kathleen Miller, Director, Procurement, and Chief, DITCO
Martin Gross, PEO Command and Control Capabilities

12:30 p.m. - 1 p.m.

Paige Atkins, Director, Strategic Planning and Information
Dave Mihelcic, Chief Technology Officer
David Bennett, PEO, GIG Enterprise Services

EXPAND YOUR NETWORKING OPPORTUNITIES!

DISA



Follow **@USDISA** on  to receive agenda and logistics updates.

Share your DISA CUSTOMER & INDUSTRY FORUM experience with other attendees and colleagues back at the office:
Tweet with us using the **#DISA11** hashtag.

You can also like us on  at www.facebook.com/USDISA.

MONDAY August 15

11 a.m. – 6:30 p.m.	Conference Registration	Charles Street Lobby
4:30 p.m – 6:30 p.m	AFCEA Technology Showcase Grand Opening	Exhibit Hall A - D



Technology Showcase Grand Opening Reception Station Sponsors

GENERAL DYNAMICS
Information Technology

URS

DISA and its mission partners must take advantage of technological advances to engineer and evolve the Department's information infrastructure and the capabilities it provides.

TUESDAY August 16

6:30 a.m. – 5 p.m.	Conference Registration	Charles Street Lobby
 AFCEA Technology Showcase	Conference Registration Sponsored by 	
9:45 a.m. – 5 p.m.	AFCEA Technology Showcase	Exhibit Hall A - D
6:30 a.m. – 7:45 a.m.	Continental Breakfast	Pratt Street Lobby
 AFCEA Technology Showcase	Continental Breakfast Sponsored by 	
8 a.m. – 8:15 a.m.	Opening Ceremony	Ballroom E
8:15 a.m. – 9 a.m.	Opening Address LTG Carroll F. Pollett, USA Director Defense Information Systems Agency	Ballroom E
9 a.m. – 9:45 a.m.	Gen Duncan J. McNabb, USAF Commander, U.S. Transportation Command	Ballroom E
9:45 a.m. – 10:15 a.m.	Coffee Break	Exhibit Hall A - D
 AFCEA Technology Showcase	Coffee Break Sponsored by 	
10:15 a.m. – 11 a.m.	John Chambers Chairman and CEO, Cisco	Ballroom E
11 a.m. – 12 p.m.	Exhibit Hall Break	Exhibit Hall A - D
12 p.m. – 1:30 p.m.	Lunch with Keynote Speaker Deputy Secretary of Defense William J. Lynn III	Ballroom E
 AFCEA Technology Showcase	Lunch Sponsored by 	
1:45 p.m. – 2:45 p.m.	Tracks and Sessions	Meeting Rooms 301- 335 & Level 4
2:45 p.m. – 3 p.m.	Break	
3 p.m. – 4 p.m.	Tracks and Sessions	Meeting Rooms 301- 335 & Level 4
4 p.m. – 4:30 p.m.	Beverage Break	Levels 3 & 4 Hallways
 AFCEA Technology Showcase	Beverage Break Sponsored by 	
4:30 p.m. – 5:30 p.m.	Tracks and Sessions	Meeting Rooms 301- 335 & Level 4
5:30 p.m. - 6:30 p.m.	AFCEA "Catch & Release" Network Reception	Pratt Street Lobby
7 p.m. – 9 p.m.	An Evening at the Aquarium Networking Reception	National Aquarium, Baltimore

*Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.

WEDNESDAY August 17

6:30 a.m. – 5 p.m. Conference Registration Charles Street Lobby



Technology Showcase

Conference Registration Sponsored by



9:45 a.m. – 7 p.m. AFCEA Technology Showcase Exhibit Hall A - D

6:30 a.m. – 7:45 a.m. Continental Breakfast Pratt Street Lobby



Technology Showcase

Continental Breakfast Sponsored by **NORTHROP GRUMMAN**

8 a.m. – 8:05 a.m. **Paige Atkins** Ballroom E

Director, Strategic Planning and Information
DISA

8:05 a.m. – 8:50 a.m. **Paul Maritz** Ballroom E

Chief Executive Officer, VMware

8:50 a.m. – 10 a.m. DISA's Strategic Way Ahead Ballroom E

Paige Atkins, Director, Strategic Planning
and Information

Tony Montemarano, Component Acquisition
Executive

David Mihelcic, Chief Technology Officer

Richard Hale, Chief Information Assurance
Executive

10 a.m. – 10:30 a.m. Coffee Break Exhibit Hall A - D



Technology Showcase

Coffee Break Sponsored by **NORTHROP GRUMMAN**

10:30 a.m. – 5 p.m. Tracks and Sessions Meeting Rooms 301 - 335

Forecast to Industry

10:30 a.m. – 10:35 a.m. **LTG Carroll F. Pollett**, USA Ballroom E

Director, DISA

10:30 a.m. – 11 a.m. **Kathleen Miller**

Director, Procurement, and Chief, DITCO
DISA

11 a.m. – 11:30 a.m. Program Executive Officer, Mission
Assurance & Network Operations

11:30 p.m. – 1 p.m. Lunch Exhibit Hall A - D



Technology Showcase

Lunch Sponsored by **HARRIS
CAPROCK**

*Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.

WEDNESDAY August 17

Forecast to Industry (continued)

1 p.m. – 1:15 p.m.	Computing Services Directorate	Ballroom E
1:15 p.m. – 2 p.m.	Network Services	
2 p.m. – 2:15 p.m.	Program Executive Officer Communications	
2:15 p.m. – 2:30 p.m.	Program Executive Officer, GIG Enterprise Services	
2:30 p.m. – 2:45 p.m.	Program Executive Officer, Command and Control Capabilities	
2:45 p.m. – 3 p.m.	Chief Information Officer	
3 p.m. – 3:15 p.m.	Chief Technology Officer	
3:15 p.m. – 3:30 p.m.	Office of Small Business Programs (OSBP)	
3:30 p.m. – 4 p.m.	Beverage Break	Levels 3 & 4 Hallways



Technology Showcase

Beverage Break Sponsored by



4 p.m. – 4:15 p.m.	Fort Meade Regional Partnership	
4:15 p.m. – 4:45 p.m.	Q&A/Closing Remarks	
5 p.m. – 7 p.m.	AFCEA Networking Event	Exhibit Hall A - D

**Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.*

THURSDAY August 18

6:30 a.m. – 3 p.m. Conference Registration Charles Street Lobby



Technology Showcase

Conference Registration Sponsored by



9:45 a.m. – 3 p.m. AFCEA Technology Showcase Exhibit Hall A - D

6:30 a.m. – 7:45 a.m. Continental Breakfast Pratt Street Lobby



Technology Showcase

Continental Breakfast Sponsored by **NORTHROP GRUMMAN**

8 a.m. – 8:05 a.m. **LTG Carroll F. Pollett, USA**, Director, DISA Ballroom E

8:05 a.m. – 8:15 a.m. **Teri Takai**, Chief Information Officer, DoD Ballroom E

8:15 a.m. – 9:45 a.m. CIO Panel [Moderator: Teri Takai] Ballroom E

Lt Gen William Lord, USAF, Chief of Warfighting Integration and Chief Information Officer, USAF

LTG Susan Lawrence, USA, Army Chief Information Officer, G-6

VADM Kendall Card, USN, Deputy Chief of Naval Operations for Information Dominance, Director of Naval Intelligence

BGen Kevin Nally, USMC, Director, C4, Chief Information Officer of the Marine Corps

9:45 a.m. – 10:15 a.m. Coffee Break Exhibit Hall A - D



Technology Showcase

Coffee Break Sponsored by **NORTHROP GRUMMAN**

10:15 a.m. – 10:20 a.m. **Paige Atkins**, Director Strategic Planning and Information, DISA Ballroom E

10:20 a.m. – 11:40 a.m. Industry Panel [Moderator: David Mihelcic, DISA CTO] Ballroom E

Rob Tarkoff, Senior VP and GM, Digital Enterprise Solution, Adobe

Michele Weslander Quaid, Federal Chief Technology Officer, Google

Jeff Bergeron, U.S. Public Sector Chief Technology Officer, Hewlett-Packard Co.

Dan Hushon, Senior Director Chief Technology Officer, EMC Corp.

Tim Brown, Senior VP, Chief Security Architect, Distinguished Engineer, CA Technologies

*Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.

THURSDAY August 18

11:40 a.m. – 12:40 p.m.	Break	Exhibit Hall A - D
12:40 p.m. – 1:15 p.m.	Lunch	Ballroom E



AFCEA Technology Showcase

Lunch Sponsored by



1:15 p.m. – 1:45 p.m.	VADM Michael A. LeFever, USN , Commander Office of the Defense Representative to Pakistan	Ballroom E
1:45 p.m. – 2 p.m.	Closing Remarks	
2 p.m. – 2:30 p.m.	Dessert	Exhibit Hall A - D
2:30 p.m. – 3:30 p.m.	Tracks Sessions	Meeting Rooms 301- 335 & Level 4
3:30 p.m. – 4 p.m.	Beverage Break	Levels 3 &4 Hallways



AFCEA Technology Showcase

Beverage Break Sponsored by



4 p.m. – 5 p.m.	Tracks Sessions	Meeting Rooms 301- 335 & Level 4
-----------------	-----------------	-------------------------------------

TUESDAY



LTG Carroll F. Pollett, USA

Director, DISA and Conference Host

As DISA Director, LTG Carroll F. Pollett leads a global organization of military and civilian personnel who plan, develop, deliver, and operate joint interoperable command and control capabilities and a global enterprise infrastructure in direct support of the President, Secretary of Defense, Joint Chiefs of Staff, Combatant Commanders, Department of Defense components, and other mission partners across the full spectrum of operations. LTG Pollett was commissioned through the Infantry Officer Candidate School. He earned a Bachelor of Science degree from Georgia Southern College and holds master's degrees in Business Administration from Central Michigan University and in National Resource Strategy from National Defense University.



General Duncan J. McNabb, USAF

Commander, U.S. Transportation Command

Gen Duncan J. McNabb is commander, U.S. Transportation Command, Scott Air Force Base, Ill. USTRANSCOM is the single manager for global air, land, and sea transportation for the Department of Defense. Gen McNabb graduated from the U.S. Air Force Academy in 1974. A command pilot, he has amassed more than 5,400 flying hours in transport and rotary wing aircraft. He has held command and staff positions at squadron, group, wing, major command and Department of Defense levels. During operations Desert Shield and Desert Storm, Gen McNabb commanded the 41st Military Airlift Squadron, which earned Military Airlift Command's Airlift Squadron of the Year in 1990.



John T. Chambers

Chairman and CEO, Cisco Systems

John Chambers is Chairman and CEO of Cisco. He has helped grow the company from \$70 million when he joined Cisco in January 1991, to \$1.2 billion when he assumed the role of CEO, to its current run rate of \$40 billion. In 2006, Chambers was named Chairman of the Board, in addition to his CEO role. Chambers has received numerous awards for his leadership during his past 16 years at the helm of Cisco, including Time Magazine's "100 Most Influential People," one of Barron's' "World's Best CEOs," the "Best Boss in America" by 20/20, one of BusinessWeek's "Top 25 Executives Worldwide," "CEO of the Year" by Chief Executive Magazine, the Business Council's "Award for Corporate Leadership," and "Best Investor Relations by a CEO" from Investor Relations Magazine three times.



The Honorable William J. Lynn III

Deputy Secretary of Defense

William J. Lynn III is the 30th deputy secretary of defense. Lynn's career has included extensive public service at various levels within government. He has served as the Under Secretary of Defense (Comptroller) from 1997 until 2001 and for four years prior to that, he was the director of Program Analysis and Evaluation (PA&E) in the Office of the Secretary of Defense. Before entering the Department of Defense in 1993, Lynn served for six years on the staff of Senator Edward Kennedy as liaison to the Senate Armed Services Committee. Prior to 1987, he was a senior fellow at the National Defense University and was on the professional staff of the Institute for Defense Analyses.

WEDNESDAY



Paul Maritz

Chief Executive Officer, VMware, Inc.

Paul Maritz joined VMware in July 2008 as president and chief executive officer. Prior to joining VMware, he was president of the Cloud Infrastructure and Services Division at EMC after the company's February 2008 acquisition of Pi, where he was the founder and CEO. Before founding Pi, he spent 14 years working at Microsoft, where he served as a member of the five-person Executive Committee that managed the overall company. As vice president of the Platform Strategy and Developer Group, among other roles, he oversaw the development and marketing of system software products (including Windows 95, Windows NT, and Windows 2000), development tools (Visual Studio) and database products (SQL Server) and the complete Office and Exchange product lines. Prior to Microsoft, he spent five years working at Intel as a software and tools developer.

THURSDAY



Teri Takai

Chief Information Officer, Department of Defense

Ms. Teri Takai serves as the principal advisor to the Secretary of Defense for Information Management/ Information Technology and Information Assurance as well as non-intelligence Space systems, critical satellite communications, navigation, and timing programs, spectrum, and telecommunications. She provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions. Ms. Takai previously served as chief information officer for the State of California.



Lt Gen William T. Lord, USAF

Chief of Warfighting Integration and Chief Information Officer/A6, U.S. Air Force

Lt Gen William T. Lord is the chief of Warfighting Integration and Chief Information Officer, Office of the Secretary of the Air Force in Washington, D.C. Lt Gen Lord leads five directorates and one field operating agency consisting of more than 350 military, civilian, and contractor personnel supporting a portfolio valued at \$7 billion. He integrates Air Force warfighting and mission support capabilities by networking space, air, and terrestrial assets. Additionally, he shapes doctrine, strategy, and policy for all communications and information activities.



LTG Susan S. Lawrence, USA

Army Chief Information Officer/G-6

As the CIO, LTG Lawrence reports directly to the Secretary of the Army for setting strategic direction and objectives, and supervises all Army C4 (command, control, communications, and computers) and IT functions. As the G-6, she supports the Chief of Staff of the Army by advising on network, communications, and signal operations. This includes advising on the impact of communications security, force structure, equipping, and employment of network, communications, and signal capabilities on Army operations.



VADM Kendall L. Card

Deputy Chief of Naval Operations for Information Dominance/Director of Naval Intelligence

VADM Card is a native of Fort Stockton, Texas. He earned a Bachelor of Science degree in Mechanical Engineering from Vanderbilt University in December 1977 and holds a master's degree in National Security and Strategic Studies from U.S. Naval War College. He is also a graduate of U.S. Naval Test Pilot School. From 1979 to 2006, VADM Card served in various operational tours at sea. He has served as director, Command Control Systems, North American Aerospace Defense Command and U.S. Northern Command; commander, Task Forces 51/58/59/151/158; commander, Expeditionary Strike Group Three; and director of Concepts, Strategies, and Integration for Information Dominance.



BGen Kevin J. Nally, USMC

Director, C4/Chief Information Officer of the Marine Corps

BGen Kevin Nally is the director for Command, Control, Communications, and Computers (C4) for the United States Marine Corps. BGen Kevin Nally was commissioned a second lieutenant in the Marine Corps in May 1981, after graduating from Eastern Kentucky University with a Bachelor of Science in Agronomy and Natural Resources. After completing The Basic School and Communications Officer Course, he was assigned to the 1st Marine Amphibious Brigade where he served as a Communications Platoon Commander for the Marine Service Support Group-37 and later as a Communications Platoon Commander for the Brigade Service Support Group. During this tour, BGen Nally attended SCUBA School, Pearl Harbor where he served in an additional duty capacity as a search and rescue diver.



VADM Michael A. LeFever

Commander, Office of the Defense Representative to Pakistan

VADM Michael A. LeFever is a 1976 graduate of the United States Naval Academy where he received a Bachelor of Science degree in Oceanography. VADM LeFever served as director, Manpower, Personnel, Training, and Education Policy Division (N13); deputy director, Expeditionary Warfare Division (OPNAV N75); and director, Surface Officer Distribution Division, Navy Personnel Command (PERS 41), Millington, Tenn. Additional tours ashore included action officer on the Joint Staff in the Command, Control, and Communications Directorate (J6); executive assistant to the vice director, Joint Staff; branch head for Fleet Readiness; executive assistant to the deputy and chief of staff, U.S. Atlantic Fleet; and senior fellow, Chief of Naval Operations Strategic Studies Group.



Robert Tarkoff

Senior Vice President and General Manager, Digital Enterprise Solutions of Adobe Systems Inc.

As senior vice president and general manager of the Digital Enterprise Solutions business unit, Rob Tarkoff is responsible for Adobe's Customer Experience Management offerings that transform digital experiences for enterprises and government agencies. Tarkoff oversees the Adobe Enterprise Platform, which combines Adobe® LiveCycle® Enterprise Suite (ES) with the Web Content Management, Digital Asset Management, and Social Collaboration solutions gained through Adobe's acquisition of Day Software. He is responsible for Adobe's worldwide solution partnerships, including systems integration partners and strategic ISVs.



Michele Weslander Quaid

Chief Technology Officer (Federal), Google Inc.

Michele Weslander Quaid is the Google Federal Chief Technology Officer and an innovation evangelist. Throughout her career, she has taken on the challenge of creating start ups and transforming existing businesses in both industry and government. Through her successes, she has been recognized and sought after as a leader of change and innovation. Prior to joining Google, her work experience included nearly 20 years in the national security community, to include more than a decade in industry as an image scientist and chief engineer supporting government programs, before being asked to join the U.S. government in 2002 in various transformational roles to include CTO, CIO, and other senior executive positions.



Jeff Bergeron

Chief Technologist, U.S. Public Sector, Enterprise Services, Hewlett-Packard Company

Jeff Bergeron is the HP chief technologist (CT) for the U.S. Public Sector. For more than 16 years, Bergeron has been dedicated to delivering services that enable clients to optimize business applications, streamline processes, and establish an agile operating model that aligns with mission goals and objectives – resulting in a comprehensive IT strategy that is tied to mission outcomes and aligned with their strategic vision. As the CT of Public Sector, he leads a team of chief technologists that are responsible for positioning HP's capabilities and offerings within the U.S. government market sector.



Dan Hushon

Senior Director and Distinguished Engineer, Office of the CTO, EMC Corporation

Dan Hushon runs the Advanced Systems Engineer group with a key focus on Cloud Service Providers and internet scale/Big Data information and analytics. As CTO for EMC's Service Provider program, Hushon is rationalizing the strategic technical and product portfolio in order to architecturally align the IIP product strategies with emerging requirements. He is also responsible for the broader information systems architectures that are exploited by clouds and enterprises to improve the manageability, scalability, serviceability, and substantially improved insights derived from big data.



Tim Brown

Senior Vice President, Chief Security Architect, and Distinguished Engineer, CA Technologies

Tim Brown has overall technical direction and oversight responsibilities for the CA security products. With more than 20 years of information security expertise, Brown has been involved in many areas of security, including identity and access management, security compliance, threat research, vulnerability management, encryption, and managed security services. He has worked with many companies and government agencies to implement sound and practical security policies and solutions. He is an avid inventor with more than 20 filed patents, is on the board of the Open Identity Exchange, and has provided expert testimony at a U.S. Congressional hearing.

About the Tracks and Sessions

Our tracks and sessions are the heart of our conference — the way we set the stage to dialogue about the important challenges we face as a combat support agency. This dialogue drives the necessary preparation to maintain and advance the Power to Connect. This year, our tracks are aligned and based on the DISA Campaign Plan, a document that functions as our comprehensive, integrated strategic plan that will guide us in accomplishing the agency's mission and vision. Our three lines of operation — Enterprise Infrastructure, Command and Control and Information Sharing, and Operate and Assure — serve as the overarching foundation for realizing our goals. They are the framework in which the tracks and sessions are organized. Additionally, we have tracks that fall under five of our nine Joint Enablers — elements that support the Lines of Operation. As always, our tracks and sessions are content-rich, collaborative learning experiences.

Enterprise Infrastructure	14
C2/Information Sharing	22
Operate and Assure	26
Contracting	29
Engineering	30
Information, Knowledge Management & Process Improvement	34
Spectrum	35
Testing	36

Enterprise Infrastructure Track Schedule

Tuesday

1:45 p.m. – 2:45 p.m.	National Senior Leadership Decision Support Service	Room 301
	SIPR DMZ [FOUO]*	Room 308
	Web Content Filtering (WCF) [FOUO]*	Room 309
	DISA Web Audit Management [FOUO]*	Room 314/315
	Enterprise Services: Today and Beyond	Room 317
	Global NetOps Requirements and Capabilities	Room 324
	IT Consolidation	Room 327
	Optical Evolution 10G/100G	Room 328/329
	IT Efficiencies and Enterprise IT Acquisition Consolidation:	
	What's Ahead from DoD ESI	Room 330
	Defense Message System (DMS) Part 1 [FOUO]*	Room 331/332
	Computing Services Strategy	Ballroom I
	Secure Configuration Management (SCM)	Ballroom II
	3 p.m. – 4 p.m.	Centaur Community Data Center (CDC) [FOUO]*
Domain Name System Security [FOUO]*		Room 309
Enterprise Services Governance		Room 317
JEN/JIE		Room 327
Voice Mobility		Room 328/329
Defense Message System (DMS) Part 2		Room 331/332
Secure Configuration Management/Continuous Monitoring Demo		Ballroom II
Common User Services	Ballroom I	
4:30 p.m. – 5:30 p.m.	DESA [FOUO]*	Room 307
	Attack, Detection/Diagnosis and Response (A2DR) [FOUO]*	Room 308
	Enterprise User: Go Anywhere, Log In, and Be Productive	Room 317
	Public Key Infrastructure (PKI) [FOUO]*	Room 328/329
	IP Convergence Overview [FOUO]*	Room 331/332
	Enterprise Email	Ballroom I
	Host-Based Security Solution (HBSS)	Ballroom II

Wednesday

10:30 a.m. – 11:30 a.m.	Enterprise Services Today and Beyond	Room 317
	Enterprise Voice Services	Room 328/329
	IT Efficiencies and Enterprise IT Acquisition Consolidation:	
	What's Ahead from DoD ESI	Room 331/332
	SharePoint	Ballroom I

*Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).

Enterprise Infrastructure

Wednesday (continued)

1 p.m. – 2 p.m.	Enterprise Collaboration Strategy Update/IdAM Management	Room 324
	Enterprise Infrastructure Reference Implementation	Room 325
	Network Customer Service Update	Room 328/329
	Subscription Management and Rate Setting	Room 331/332
	RACE	Ballroom I
2:30 p.m. – 3:30 p.m.	Getting Ahead in the Clouds	Room 307
	IP Convergence Architecture	Room 309
	Enterprise Messaging/SKIWeb	Room 324
	JEN/JIE	Room 321-323
	Integrated Waveform	Room 327
	Platform as a Service	Ballroom I
4 p.m. – 5 p.m.	Getting Ahead in the Clouds	Room 307
	IT Consolidation	Room 321-323
	DISN Transport Network Evolution and Enablers	Room 324
	Communications in Disasters	Room 331/332
	Gateways	Room 328/329
	Virtualization/Storage Strategy	Ballroom I

Thursday

2:30 p.m. – 3:30 p.m.	Phase 2 Pilot and Enterprise Capabilities [FOUO]*	Room 307
	NIPRNet Hardening [FOUO]*	Room 308
	Assured Shared Framework	Room 318
	DISA NetOps [FOUO]*	Room 321-323
	Communications in Disasters	Room 331/332
4 p.m. – 5 p.m.	Global NetOps Information Sharing Environment	Room 307
	Cross Domain Enterprise Services (CDES) [FOUO]*	Room 308
	National Senior Leadership Decision Support Service [FOUO]*	Room 314/315
	MADSS	Room 318
	Joint IP Modem (JIPM)	Room 327
All Track Sessions	Defense Red Switch Network (DRSN) Demonstration Room	Room 310

**Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

We will enable users to connect, identify themselves, access services, find and share information, and collaborate as needed for the mission at hand.

Assured Shared Framework (ASF) (Advanced Concepts Office)

This session will cover the technical underpinning that provides the protected Enclave for the Vice Chairman of the Joint Chiefs of Staff (VCJCS). The ever-changing demand of the Department of Defense (DoD) mission requires agile reaction to an ever-increasing new threat. The current process of bringing internet technologies to the .mil environment is neither timely nor efficient. DoD requires a middleware platform that provides the ability to rapidly integrate secure commercial technologies to the military domain. The Assured Shared Framework (ASF) provides the middleware solution to rapidly integrate commercial off-the-shelf (COTS) products. ASF is an enabling technology for exposing third-party capabilities as web services. It controls interfaces of new un-trusted third-party capabilities (web services and/or applications). ASF in itself is not an end-product for the warfighter; it only provides arbitrated access to the Enterprise Infrastructure technical underpinnings.

Attack, Detection/Diagnosis and Response (A2DR) [FOUO]*

This session will provide background and the future development strategy for the Attack Detection/Diagnosis and Response (A2DR) program. It will also discuss the Community Data Center (CDC), a unified analysis center for users, supporting a GIG (Global Information Grid)-scale capability for both event-based and retrospective analysis. The Data Analysis Long Term Storage (DALTS) and other A2DR program and initiatives that use the CDC will also be discussed. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Centaur Community Data Center (CDC) [FOUO]*

The Community Data Center (CDC) is comprised of sensor data, specialized processes, and computer network defense tools including Fight Club. Because the CDC operates in a separate environment from command and control (C2) networks, network defense analysts can analyze data in its native environment and develop appropriate responses to threats with no impact upon operational networks. Sensor data is moved from various strategic locations throughout the Global Information Grid (GIG) to large cluster storage databases at PE Warner Robins Air Force Base for further Computer Network Defense (CND) analysis. Approximately 120GB of data is collected daily. Users are National Security Agency (NSA), combatant commands (COCOMs), and military services. Further, it is used for malware/attack vector investigations. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Common User Services

This session will present the current status and roadmap of Computing Services' deployments of cloud computing. Also covered will be the future direction of multiple enterprise offerings, to include the Rapid Access Computing Environment (RACE), Global Content Delivery Services (GCDS), System Network Availability Performance Service (SyNAPS), and SharePoint as a service. Highlights will be given to the streamlining of the accreditation process specifically the Path-to-Production, end-to-end monitoring, and RACE on the SIPRNet (classified network).

Communications in Disasters

Providing absolutely dependable service delivery to warfighters at the tactical edge requires that all communications systems in use are fully integrated and interoperable. DISA is committed to ensuring that warfighters get the assured service delivery at the tactical edge. As complex and challenging as wartime scenarios can be, disasters normally present a greater communications challenge. In addition to the increased number of participating entities (e.g. local law enforcement, other agencies, etc.), disasters are commonly completely unpredictable and combine a wide range of event types with varying extent of damage to existing infrastructure and assets. DISA recognizes that, in most cases, disaster-relief communications is a superset of wartime communications requirements. Therefore, by focusing on interoperability and integration of disaster-relief communications systems, we are necessarily also solving the communications challenges for the warfighter at the tactical edge, as well as enhancing U.S. national security.

Computing Services Strategy

This session will present the Computing Services strategy, including updates on Computing Services' accomplishments, process improvement efforts, and future technologies that provide for an efficient and optimal organization.

Cross Domain Enterprise Services (CDES) [FOUO]*

The Cross Domain Enterprise Service (CDES) provides a fee-for-service alternative to organizations investing significant resources in the fielding, sustainment, and defense of their own individual cross domain solutions. CDES offers a range of secure cross domain information-sharing solutions spanning NIPRNet (unclassified network), SIPRNet (classified network), and select coalition networks. These capabilities include a full spectrum of data types supporting a variety of functions. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Defense Message System (DMS) Parts 1 & 2 [Part 1 FOUO]*

The Defense Message System (DMS) is a core Enterprise Infrastructure information exchange service, operating on NIPRNET (unclassified network) and SIPRNET (classified network) in both the strategic and tactical environments, as well as providing enterprise-level cross domain services between NIPRNET and SIPRNET. This session will address the current and future sustainment status of the DMS. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Defense Red Switch Network (DRSN) Demonstration Room

The DRSN DEMO room will have displays and demonstrations of the latest DRSN switches, consoles, peripheral equipment, voice over secure Internet protocol (VoSIP), and the Secure Mobile Environment-Portable Electronic Device (SME-PED). Representatives from DISA's Network Services Directorate Voice Services Division and Raytheon will be available to demonstrate the following equipment and capabilities: Enhanced Switch Reporting System, Voice over Secure Internet Protocol (VoSIP), TXP Phone VoIP and Basic Rate ISDN, traditional Red Switch, Enhanced Communications Console (ECC), Chairman's Mobile Communications (mobile secure communications package), IP Long Local, New switch database, SME-PED, and user interface capability for DSS-2A switch.

DISA NetOps [FOUO]*

The current state of the DISA NetOps environment includes a mix of self-contained NetOps tools deployed to autonomously operate and manage individual enterprise services for the warfighter. These tools, while valuable to the individual service organizations they support, are not enterprise-focused across the agency and do not encourage cost efficiency, rapid detection, diagnosis, and resolution of end-to-end problems, or rapid delivery of services. The current state of the environment is inefficient (in cost, resource consumption, and time) and does not effectively meet the challenge of providing the right actionable information to the right people, in a timely and secure manner, for effective decision making. Come hear about the evolution of DISA's unified technical approach to operating and assuring the DISA-managed elements of the Defense Information Environment and what's up next for the agency.

**Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

DISA Web Audit Management [FOUO]*

This session will provide background and future developments on tools developed or that are in development under the DISA Web Audit Management Program, which focuses on providing new analytical methods to detect insider threat behavior using existing and near-term planned Community Data Center (CDC) resources to the maximum extent practical. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

DISN Transport Network Evolution and Enablers

To support this new generation of Defense Information System Network (DISN) Internet Protocol (IP) Transport services, our deployed optical transport layer technologies need to adapt to provide higher capacity, extended reach, enhanced flexibility, and greater transparency. Elimination of Legacy asynchronous transfer mode (ATM) and time division multiplexing (TDM) technologies are the hallmark of near-term DISN Transport Architectures. This talk focuses on the architecture needed to eliminate older DISN Transport technologies and implement new 100G Dense Wavelength Division Multiplexing (DWDM), Multi-Degree Reconfigurable Optical Add/Drop Multiplexer (ROADM), and Switched IP/Ethernet technologies. We will also explore new fiber technologies required to support this evolution over the next decade.

DoD Enterprise Security Architecture (DESA) [FOUO]*

The DoD Enterprise Security Architecture (DESA) is intended to reduce the complexity and cost of network defense while improving the Department's security posture and improving support for mobile, embedded, and other users. Efficiency will be improved by reducing duplication of operations, establishing joint protections and responsibilities across Communities of Interest (COIs), leveraging other information technology consolidation and enterprise-level capabilities, and flattening the network. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Domain Name System (DNS) Security [FOUO]*

Hear about how Domain Name System (DNS) Hardening is expanding the current capabilities of DISA's DNS infrastructure to include a layered approach to DNS Security. Discussion will include efforts for .mil Proxy services, Enterprise Recursive Services, DNS Security Extensions, and Users Experience Monitoring. The changes that these initiatives bring play a vital part in the overall defense of DoD DNS services that attendees should hear about and understand. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Enterprise Collaboration Strategy Update

This session will serve as an overview of collaborations capabilities, priorities, technical/programmatic strategy, and technical transition. The session will also cover way ahead efforts for the near future.

Enterprise Cross Domain Strategy and Architecture [FOUO]*

This presentation will update the current state of enterprise cross domain strategy and architecture and the related community activities driving it forward. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Enterprise Email

This session will define Enterprise Email as a service, discuss its service offerings and touch on capabilities made available to current customers. Enterprise Email is a globally-accessible managed service offering that provides both desktop-based Outlook email and Outlook Web Access (OWA) email. This system uses the Enterprise User account data provided by the Identity Synchronization Service (IdSS) and the Enterprise Application and Services Forest (EASF). The Army is currently migrating all of their members to this service.

Enterprise Messaging

This session is an introduction and overview of Enterprise Messaging in 2012, the benefits of Messaging, and what to expect in the near future.

Enterprise Services Governance

This session is an overview of the Department of Defense Chief Information Officer (DoD CIO) Vision and Enterprise Strategy Roadmap. Topics will include governance structure, data service initiatives, and funding approach activities planned for 2011 and 2012.

Enterprise Services: Today and Beyond

This session will serve as an overview and description of current and upcoming Enterprise Services. What's planned for 2011 and 2012 and deployable Enterprise Services will be discussed. The full scope of the Program Executive Office (PEO) services and capabilities as well as general overview will also be covered.

Enterprise Voice Services

Enterprise Voice can provide a full range of voice-related capabilities to more than 4 million Department of Defense (DoD) users from central locations that fully leverage the Defense Information System Network (DISN) and Internet protocol (IP) technologies. This approach avoids the duplication of costs for voice services, operations and maintenance, network operations, sustainment, and information assurance at nearly 2,000 locations worldwide with a lower total cost of ownership.

Gateways

DISA is implementing the Department of Defense (DoD) Teleport System. The system will integrate, manage, and control a variety of communications interfaces between the Defense Information System Network (DISN) terrestrial and tactical satellite communications (SATCOM) assets at a single point of presence. The Teleport System is a telecommunications collection and distribution point that provides deployed warfighters with multiband, multimedia, and worldwide reach-back capabilities to the DISN that far exceed current capabilities. Teleport is an extension of the Standardized Tactical Entry Point (STEP) program, which currently provides reach-back for deployed warfighters via the Defense Satellite Communications System (DSCS) X-band satellites.

Getting Ahead in the Clouds

This session is designed to communicate the DISA vision for cloud computing, show what is driving the Department of Defense (DoD) to embrace the cloud paradigm, and show where we are headed into the future. The session will explore the DoD cloud community perspective, look at the reasons DISA needs to be engaged in delivering cloud services, and discuss what actions need to be taken to get there.

Global NetOps Information Sharing Environment (GNISE)

The Department of Defense (DoD) NetOps environment includes a large array of disparate non-standardized NetOps infrastructures that prohibits accurate situational awareness (SA), mission planning and execution, and effective decision making. Significant deficiencies exist in achieving the DoD NetOps strategic vision due to the lack of an integrated, standardized, and unified NetOps infrastructure and enterprise environment to enable effective cyberspace operations. Come hear what DISA is doing to establish a unified and agile DoD NetOps and cyber SA capability to enable command and control (C2) and SA across all DoD organizations, systems, services, and resources and understanding of their interrelationships for mission impact analysis, planning, and execution.

Global NetOps Requirements and Capabilities

Come, listen, and give your input about the enterprise-level capabilities DISA has provided the Department of Defense (DoD) in support of the NetOps mission; and to achieve shared situational awareness. Current operations are driving requirements for advanced analytics, greater information sharing and collaboration, and increased machine-to-machine interfaces to achieve information superiority and shorten decision cycles. Hear how DISA is partnering with the community to capture, understand, and rapidly deliver on complex DoD-wide NetOps requirements.

Host-Based Security Solution (HBSS) [FOUO]*

The Host-Based Security Portfolio includes DISA tools that are designed to protect end points. Learn more about the current state of these tools [HBSS, AV/AS, wireless security, and bootable media] and future initiatives and activities, such as training, information sharing, new releases, and more. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Identity and Access Management: Consistent Access to Capability

This is an introduction to Identity and Access Management's (IdAM's) strategic vision, portfolio, access control, and account provisioning. These characteristics, when added together, make it easy, agile, and inexpensive to share information within the Department of Defense (DoD), and safe to share with coalition partners.

Integrated Waveform (IW)

Learn about this revolutionary new capability for ultra high frequency satellite communications (UHF SATCOM), consisting of a software upgrade to existing UHF SATCOM radios that will allow for up to three times more accesses in addition to a marked improvement in voice quality. UHF SATCOM is essential for deployed warfighters due to its ability to offer communications in all weather and under dense cover. Current UHF SATCOM constellation is heavily oversubscribed, and that situation is expected to worsen as the constellation continues to age. The Integrated Waveform Demand Assigned Multiple Access (DAMA) upgrade will increase capacity efficiencies, offering additional networks, as well as an increase in voice quality and dynamic assignment of bandwidth.

Internet Protocol (IP) Convergence Architecture

This briefing will provide an overview of the Defense Information System Network (DISN) Real-Time Services/Unified Capabilities architecture, to include a brief overview of the Information Assurance Architecture.

Internet Protocol (IP) Convergence Overview [FOUO]*

This briefing will provide an overview of Defense Information System Network (DISN)-converged capabilities, which will lead the migration to everything over Internet protocol (EoIP) end-to-end with interoperable, assured, and secure-approved products for the Department of Defense (DoD). **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

IT Consolidation

In August 2010, the secretary of defense directed the consolidation of information technology (IT) infrastructure to achieve savings in acquisition, sustainment, and manpower costs and to improve the Department's ability to execute its missions while defending its networks against growing cyber threats. In response, the Information Technology Enterprise Strategy and Roadmap (ITESR) identified opportunities to consolidate DoD IT infrastructure through 26 initiatives in five functional areas: network services, computing services, application and data services, end-user services, and IT business processes. Each initiative contributes to one or more of the IT Enterprise goals - increase mission effectiveness, improve cyber security, and deliver efficiencies. This presentation will describe the Near Term Implementation Plan, which focuses on eight near-term initiatives, the working group's current efforts, and the way ahead to meeting the DoD CIO's required deliverable.

IT Efficiencies and Enterprise IT Acquisition Consolidation: What's Ahead from DoD ESI

"Hear the latest on how the DoD ESI and the federal-wide SmartBUY Program are establishing enterprise agreements for IT hardware, software, and related services. This session will also introduce efforts within the DoD to promote and measure IT infrastructure management success. More than just asset inventories, ITAM must institute business practices that join financial, contractual and inventory functions to support IT life cycle management, and facilitate strategic decision making.

Joint Enterprise Network/Joint Information Environment (JEN/JIE)

This presentation will provide the target audience with a background and overarching overview of the Joint Enterprise Network (JEN) implementation of the Joint Information Environment (JIE). Further, the presentation will provide a current status of the JEN implementation in the European theater.

Joint Internet Protocol Modem (JIPM)

The Joint Internet Protocol Modem (JIPM) is the Department of Defense (DoD) IP modem standard, leveraging commercial technology and open-standards to provide a common platform IP modem that ensures efficient use of bandwidth and secure transmission of warfighter IP traffic via DoD-led and DoD-owned transponded satellite communications (SATCOM) systems. The JIPM standard allows multiple modem vendors to build interoperable variants - enabling military services and combatant commands (COCOMs) to consolidate operations and resources at the DoD gateways, thus reducing costs for maintenance/sustainment and improving SATCOM bandwidth utilization.

Mission Assurance Decision Support System (MADSS) (Advanced Concepts Office)

During even the most carefully planned military operation, external events can create problems for organizations that depend on information technology (IT) to help execute their missions. The Mission Assurance Decision Support System (MADSS) brings together the knowledge base and business processes of network operations and critical infrastructure protection to provide the commanders and decision makers a near real-time assessment of these situations to answer their most pressing questions: What capabilities have I lost? What capabilities remain? What are my alternatives? How does this change the way we execute? MADSS aims to provide warfighters and DISA the ability to not only answer these questions, but also manage and mitigate the risks imposed by the vulnerabilities in the Global Information Grid (GIG) and its supporting commercial infrastructure.

National Senior Leadership Decision Support Service (NSLDSS) (Advanced Concepts Office)

The Joint Staff has embarked upon a transformation effort that will alter the way business is conducted within the Joint Staff and the combatant commands. Different operating models (e.g., persistent collaboration, social networking) and the technologies of the 21st century must be embraced to maintain a global awareness, respond with light speed, and secure a competitive edge through leveraging intellectual capital wherever it is. The National Senior Leadership Decision Support Service (SLDSS) joint capability technology demonstration (JCTD) provides web-based, thin client capabilities that will enhance National Military Command Center (NMCC) operational effectiveness by dramatically improving the senior leaders' ability to more efficiently gain situational awareness, collaborate, develop, and assess courses of action and collaboratively determine execution. DISA is tasked to provide the engineering support and Net-Centric Enterprise Services (NCES) for these emerging technologies to increase operational effectiveness for an expanded mission set.

NIPRNet Hardening [FOUO]*

NIPRNet Hardening Strategy includes key capabilities such as Demilitarized Zones/Domain Name System/Email and Web Filtering. Perimeter defense is the application of multiple solutions aimed at protection of the NIPRNet (unclassified network) and its assets from outside threats. This presentation will highlight the initiatives DISA has taken to make it more difficult for the adversary at the NIPRNet boundary. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Optical Evolution 10G/100G

Learn how the optical evolution will incorporate three phases: (1) Legacy, (2) Transition, and (3) Internet Protocol (IP)-centric network. The evolution will require that the currently employed 10G wavelength technology evolves to 100G wavelength technology. An IP-centric network that will support real-time services with guaranteed end-to-end delivery of services will require a network with the ability to maximize the use of on-demand delivery of bandwidth.

Platform as a Service (PaaS)

This session will discuss Platform as a Service (PaaS) as a transformational approach to delivering information technology (IT)-hosting capabilities under a commercial-style cloud services model. The service will provide secure standardized development, test, and production environments with a streamlined path to production process that speeds the development, delivery, and sustainment of new mission capabilities.

Phase 2 Pilot and Enterprise Capabilities [FOUO]*

This session will highlight the Privilege Management capabilities being developed and deployed to facilitate federated and secure information sharing. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Public Key Infrastructure (PKI) [FOUO]*

This session will serve as an overview of the current Department of Defense Public Key Infrastructure (DoD PKI) program and PKI policies. The latest information on Increments 1 and 2, PKI hardware tokens, PKI certificates for devices, and architecture enhancements will also be discussed. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Rapid Access Computing Environment (RACE)

This session will define Rapid Access Computing Environment (RACE) capabilities to include the customers ability to order and pay for Windows and Linux Operating systems for NIPRNet/SIPRNet development environments via a self-service portal. The customer can develop, test, and follow the streamlined RACE path-to-production process. RACE offers computing resources that are integrated with the Forge.mil services to provide the customer access to open-source software and collaboration services that support agile development and testing in a Department of Defense (DoD) environment.

Secure Configuration Management (SCM)

The Secure Configuration Management (SCM) session will educate the session participants on the integration and optimization of enterprise information assurance (IA) applications and tools that use standardized data specifications and services in order to provide an automated and continuous process for security and configuration management.

Secure Configuration Management/Continuous Monitoring Demo

The Secure Configuration Management (SCM) demonstration is a technical demonstration of available SCM capabilities using deployed enterprise tools to include: operational reporting, automated Security Technical Implementation Guide (STIG) assessments using the host-based security solution (HBSS), Windows system software inventory discovery, and continuous and automated reporting to a central repository.

SharePoint

This session will define Enterprise SharePoint Service (ESPS) and discuss its many offerings and capabilities for users. ESPS is a globally-accessible managed service offering based on the Microsoft SharePoint 2010 platform. Subscriptions are available on either the standard or enterprise versions of the platform, both of which use the enterprise user account data provided by the Identity Synchronization Service (IdSS).

SIPR DMZ [FOUO]*

This briefing will cover the modifications to the Releasable Demilitarized Zone's (REL DMZ) architecture and function based on the Improved Connectivity Initiative. It will additionally address modifications to the SIPRNet Federal DMZ to accommodate additional connectivity for non-DoD federal and contractor partners in support of DISAs Computer Network Defense Service Provider (CNSDP) mission. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

SKIWeb

This session is an introduction and 2011 transition overview of SKIWeb's capabilities. SKIWeb is an event reporting and blogging capability available to all SIPRNet (classified network) users.

Storage Strategy

The Storage Strategy session will discuss storage engineering and provide customers with an overview of enterprise technical refresh and new technology directions designed to improve services and provide added capabilities.

Subscription Management and Rate Setting

This session is a basic primer on how the subscription process works and how shares and prices are calculated. There will also be a brief discussion of the history and actions since the start of the enhanced planning process on Defense Information System Network (DISN) rates management.

Virtualization

Virtualization and cloud computing have been hot topics in today's information technology (IT) world. This session will provide some insight into why this technology is not only something that provides significant ease of operation, but it is also absolutely necessary to make full use of the hardware being manufactured today. The presentation will also cover the state of virtualization within Computing Services today.

Voice Mobility

This session provides information on the unified voice/data/email access for mobile devices, and supports the DISA Enterprise service concepts. Other topics include integration into unified capabilities requirements (UCR) architecture for classified and unclassified voice to extend capabilities to wireless handsets. Secure voice initiatives will also be covered.

Web Content Filtering (WCF) [FOUO]*

The Web Content Filtering (WCF) Solution is a mandated capability that protects NIPRNet (unclassified network) client web traffic from malware (e.g., viruses, worms embedded in web traffic) intended to infiltrate the Department of Defense (DoD) Enterprise. The WCF system establishes a defensive perimeter for protecting NIPRNet web traffic and ensures that all web traffic that traverses the Internet/NIPRNet boundary is inspected by an enterprise-wide capability. Most importantly, the WCF provides U.S. Cyber Command (USCYBERCOM) the capability for rapid, universal, verifiable policy enforcement at the Internet/NIPRNet boundary. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

C2 and Information Sharing

C2 and Information Sharing Track Schedule

Tuesday

1:45 p.m. – 2:45 p.m.	C2 Way Ahead: JC2 Objective Architecture	Room 307
3 p.m. – 4 p.m.	C2 Way Ahead: Delivering Modernized C2	Room 307
4:30 p.m. – 5:30 p.m.	GCCS-J: Developing Software in an Agile Environment	Room 318

Wednesday

10:30 a.m. – 11:30 a.m.	Joint Planning and Execution Services (JPES) Framework	Room 318
1 p.m. – 2 p.m.	GCCS-J Program Update	Room 309
	JPES - Integrated Gaming System (IGS) Brief & Demo	Room 318
2:30 p.m. – 3:30 p.m.	JPES – Joint Force Projection (JFP) Brief & Demo	Room 318
4 p.m. – 5 p.m.	JPES – Rapid TPFDD Builder (RTB) Brief & Demo	Room 318

Thursday

2:30 p.m. – 3:30 p.m.	MNIS: Leveraging Change for Coalition Information Sharing	Room 317
4 p.m. – 5 p.m.	Unclassified Information Sharing	Room 317

C2 and Information Sharing

C2 Way Ahead: Delivering Modernized C2

The Department of Defense (DoD) is moving from large centrally-provided stovepipe systems and programs to more rapid delivery of relatively-small capabilities delivered by communities of material developers contributing to portfolios of net-centric, loosely-coupled services all leveraging a common infrastructure. This presentation will address how DISA is supporting the joint command and control (C2) community to evolve the Joint C2 Portfolio.

C2 Way Ahead: Joint Command and Control (JC2) Objective Architecture

The Joint Command and Control (JC2) Objective Architecture (OA) describes the architectural concepts for development of joint C2 capabilities to include the physical, software, information assurance, data, and applicable standards. The JC2 OA provides a technical framework to enable joint C2 capabilities to independently develop interoperable joint C2 services, systems, and data structures and exploit the Department of Defense (DoD) Information Enterprise capabilities. It provides the implementation principles and constraints necessary to enable capability investment and modernization planning to achieve the DoD Information Enterprise Architecture (IEA) goals.

Global Command and Control System – Joint (GCCS-J) Program Update

Global Command and Control System-Joint (GCCS-J) is the Department of Defense (DoD) Joint Command and Control (C2) system of record and an essential component for successful implementation of the operational concepts of dominant maneuver, precision engagement, and full-dimension protection. GCCS-J provides the foundation for migration of service-unique C2 systems into a joint, interoperable environment. GCCS-J provides a fused picture of the battlespace within a modern command, control, communications, and computer system that is capable of meeting joint warfighter needs. GCCS-J incorporates the core planning and assessment tools required by combatant commanders and their subordinate Joint Task Force commanders while meeting the readiness support requirements of the military services. To achieve this, GCCS-J provides situational awareness, imagery exploitation, indications and warning, collaborative planning, course-of-action development, intelligence mission support, and real-time combat execution capabilities needed to accelerate operational tempo and conduct successful military operations in the modern warfare environment.

Global Combat Support System - Joint (GCSS-J): Developing Software in an Agile Environment

The Global Combat Support System - Joint (GCSS-J) is an information technology (IT) application that continues to implement the tenets of a service-oriented architecture to deliver visibility of combat support (CS) capability to the joint logistician (i.e., essential capabilities, functions, activities, and tasks necessary to sustain all elements of operating forces in theater at all levels), facilitating information interoperability across and between CS and C2 functions. In conjunction with other Global Information Grid (GIG) elements including Global Command and Control System-Joint (GCCS-J), Defense Information Systems Network (DISN), Defense Message System (DMS), Computing Services, and combatant command/military services/agency information architectures, GCSS-J will provide the IT capabilities required to move and sustain joint forces throughout the spectrum of military operations.

Joint Planning and Execution Services (JPES) Framework

Joint Planning and Execution Services (JPES) Framework (JFW) is an important infrastructure component within the JPES portfolio of capabilities and has applicability to the greater Adaptive Planning and Execution (APEX) community. JFW is designed to provide common services, such as a Joint Permissions Manager, which is a hybrid of role-based access control to satisfy legacy user access policies and attribute-based access control, which allows applications to begin to control user access based on user attributes. Additionally, the JFW provides a Data Virtualization Layer that enables JPES to fully implement a net-centric construct and move command and control (C2) joint planning capabilities into a service-oriented architecture environment through the modernization of legacy databases by isolating the applications from hard-coded interfaces to the databases. JFW also provides an in-memory data cache solution to allow enhanced application performance. This session will provide an overview of the JFW, what exists today, and what the plans are for future enhancements.

JPES - Integrated Gaming System (IGS) Brief & Demo

The Integrated Gaming System (IGS) is a theater-level planning, wargaming, and analysis tool. Through the capabilities of IGS, users can develop an Order of Battle, plan a force-on-force course of action, then exercise its effectiveness, and run multiple scenarios to show the force flow. The IGS will allow users to achieve the combatant commander's intent by identifying force requirements by using the Rapid Adjudication Service, and the tool's Force Ratio Analysis. This briefing and demonstration will show the user what capabilities exist in the tool today and emerging technologies.

JPES - Joint Force Projection (JFP) Brief & Demo

The Joint Forces Projection (JFP) system quickly retrieves essential force projection information used to support decisions made by members of the Joint Planning and Execution Community (JPEC). The specific emphasis is placed on those processes that support identifying, requesting, sourcing, validating, scheduling, movement tracking, and closing of force capabilities requested by the supported commander. JFP provides visibility into the execution of a plan by aggregating data from the following authoritative

C2 and Information Sharing

planning and execution capabilities: Joint Operation Planning and Execution System (JOPES), Global Status of Resources and Training System (GSORTS), Global Transportation Network/Integrated Data Environmental Global Transportation Network Convergence (GTN/IGC), Joint Capabilities Requirements Manager (JCRM), and Automated Message Handling System (AMHS). This briefing and demonstration will show the user what capabilities are resident in the tool today.

JPES - Rapid TPFDD Builder (RTB) Brief and Demo

The Rapid Time-Phased Force Deployment Data (TPFDD) Builder (RTB) is a web-enabled collaborative capability that operates within a service-oriented architecture. RTB simultaneously supports both contingency and crisis action planners to produce high-caliber strategic movement plans to include the TPFDD. RTB facilitates the ability for planners to meet the Secretary of Defense's mandated accelerated pace of critical military planning. This net-centric capability provides data exchanges between current and legacy authoritative data sources and will be interoperable with emerging adaptive planning and execution technologies. This briefing and demonstration will show the community RTB's existing capabilities as well as plans for the future.

Multinational Information Sharing (MNIS): Leveraging Change for Coalition Information Sharing

The presentation includes an overview of the MNIS portfolio and a discussion of recent changes. The discussion will address how MNIS is leveraging partnerships within DISA to deliver the "Power to Connect" for U.S. and coalition warfighters, and changes to sponsor and stakeholder relationships, e.g. Joint Forces Command (JFCOM), and Joint Staff as a result of Secretary Robert Gates' direction to achieve government efficiencies.

Unclassified Information Sharing (UIS)

Unclassified information sharing with the extended enterprise to include non-government and private organizations in a non-.mil environment is required by combatant commanders to coordinate response efforts during Humanitarian Assistance/Disaster Relief and Stability Operations. Several capabilities are in place and there is a desire to field an enterprise solution with a common look and feel across combatant commands (COCOMs). This block will provide a status update of this effort.

C2 and Information Sharing

We will leverage enterprise solutions to enhance C2 and combat support capabilities thereby increasing operational effectiveness.





Operate and Assure Track Schedule

Tuesday

1:45 p.m. – 2:45 p.m.	DIACAP	Room 316
3 p.m. – 4 p.m.	CCRI Phase II Changes [FOUO]* Node Site Coordinator	Room 314/315 Room 324
4:30 p.m. – 5:30 p.m.	Strategic NetOps: Situational Awareness [FOUO]* CNDSP Program and Tier 2 Update [FOUO]* DISA Quality Management Program	Room 309 Room 314/315 Room 324

Wednesday

10:30 a.m. – 11:30 a.m.	Automating STIGs COMSATCOM Update	Room 314/315 Room 327
1 p.m. – 2 p.m.	SATCOM GIG Integration	Room 314/315
2:30 p.m. – 3:30 p.m.	Automating STIGs	Room 314/315

Thursday

2:30 p.m. – 3:30 p.m.	Incident Response: Missions, Trends, and Tools [FOUO]* Strategic NetOps: Situational Awareness [FOUO]* DISN NetOps Service Assurance	Room 314/315 Room 327 Room 328/329
4 p.m. – 5 p.m.	DISA Quality Management Program Mission Transformation to Sustain the Power to Connect (Enterprise Connection Approval)	Room 325 Room 328/329

**Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Automating Security Technical Implementation Guides (STIGs)

The briefing will provide information on the progress Field Security Operations (FSO) has made towards automating security technical implementation guides (STIGs).

Command Cyber Readiness Inspection (CCRI) Phase II Changes [FOUO]*

Command Cyber Readiness Inspections (CCRIs) replaced Enhanced Compliance Validations (ECVs) in October 2009 as the mechanism by which commanders would be held accountable for their respective network and enclave security posture. Phase I of the CCRI program implemented a rigorous new grading criteria, which provided greater objectivity and analytical measurements of a site's security posture by reviewing technology areas, vulnerability scan results, compliance with U.S. Cyber Command (previously Joint Task Force-Global Network Operations) -issued Computer Network Defense (CND) Directives, and non-technical aspects of an information assurance (IA) program (culture, conduct, and capability). Phase II of the CCRI program began May 2011 and implements changes to the CCRI grading methodology derived from lessons learned from Phase I, and also begins process changes to shift the CCRI methodology from strictly a compliance-based inspection toward an operational readiness inspection. This session will review the Phase II changes. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Computer Network Defense Service Provider (CNDSP) Program & Tier 2 Update [FOUO]*

DISA is the Certifier for the General Service (GENSER) CNDSP program. This briefing will provide the latest updates to the Computer Network Defense Service Provider (CNDSP) Program, to include changes in the evaluator's scoring metrics (ESM). **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

COMSATCOM Update

The Commercial Satellite Communications (COMSATCOM) Update will consist of a panel briefing with a question-and-answer session following the briefings. The briefing will consist of four presentations, given by four panelists. Topics are (1) COMSATCOM Introduction and Overview, (2) an Enhanced Mobile Satellite Services Update (3) COMSATCOM Services, and (4) a Future Commercial Satellite Acquisition (FCSA) Update/Lessons Learned and Provisioning. The entire session will be one hour.

Defense Information System Network (DISN) NetOps Service Assurance

Information-sharing zone, Operational Support Systems (OSS) Central, and key service assurance systems will be described. The briefing will specify the applications, the purpose of each, the type of information provided, and their relevance to DISA customers. Specific systems in scope are the Information Sharing System, OSS Central, Service Quality Management (SQM), Integrated Network Management System (INMS) and Global Trouble Management Systems (GTMS).

DISA Quality Management Program

The DISA QA session will discuss both DISA circular rewrites as well as trends and analysis. The circulars discussion will provide an overview of current rewrites of status reporting (DISAC 310-55-1), Defense Information System Network (DISN) tech control facilities (DISAC 310-70-1), and a workmanship circular that will establish Department of Defense (DoD) installation standards for DISA sites and equipment. Trends and analysis will cover how DISA collects information, makes recommendations, and then publishes the information for customers and decision makers to ascertain the status of the Global Information Grid (GIG) and DISN services.

DoD Information Assurance Certification and Accreditation Process (DIACAP) [FOUO]*

This session will serve as an overview of the DISA certification accreditation process. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Incident Response: Missions, Trends, and Tools [FOUO]*

This discussion will cover current trends identified by the Incident Response team and checklist, tools, and recommendations for site security managers and system administrators to use. This brief will include examples of how organizations use field security operations (FSO)-developed Host-Based Security System (HBSS) Policy Auditor Benchmarks and First Responder Guide to identify compromised/infected systems that were previously undetectable. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Mission Transformation To Sustain the Power to Connect (Enterprise Connection Approval)

The Enterprise Connection Division provides mission services that are all aligned with the 2011-2012 DISA Campaign Plan's Lines of Operation. Congruent to the triad structure titled "Enabling Information Dominance" that is featured at the beginning of the

Operate and Assure



Campaign Plan, the Connection Approval Office (CAP), Ports, Protocols and Service Management (PPSM) and the Defense Information Assurance Security Accreditation Working Group (DSAWG) are all collaborating points of the triad structure that continuously provide full-scope support as the Lines of Operation to ensure that customers are always provided "the power to connect" both efficiently and securely while maintaining the health of the Global Information Grid's (GIG) security posture.

Node Site Coordinator

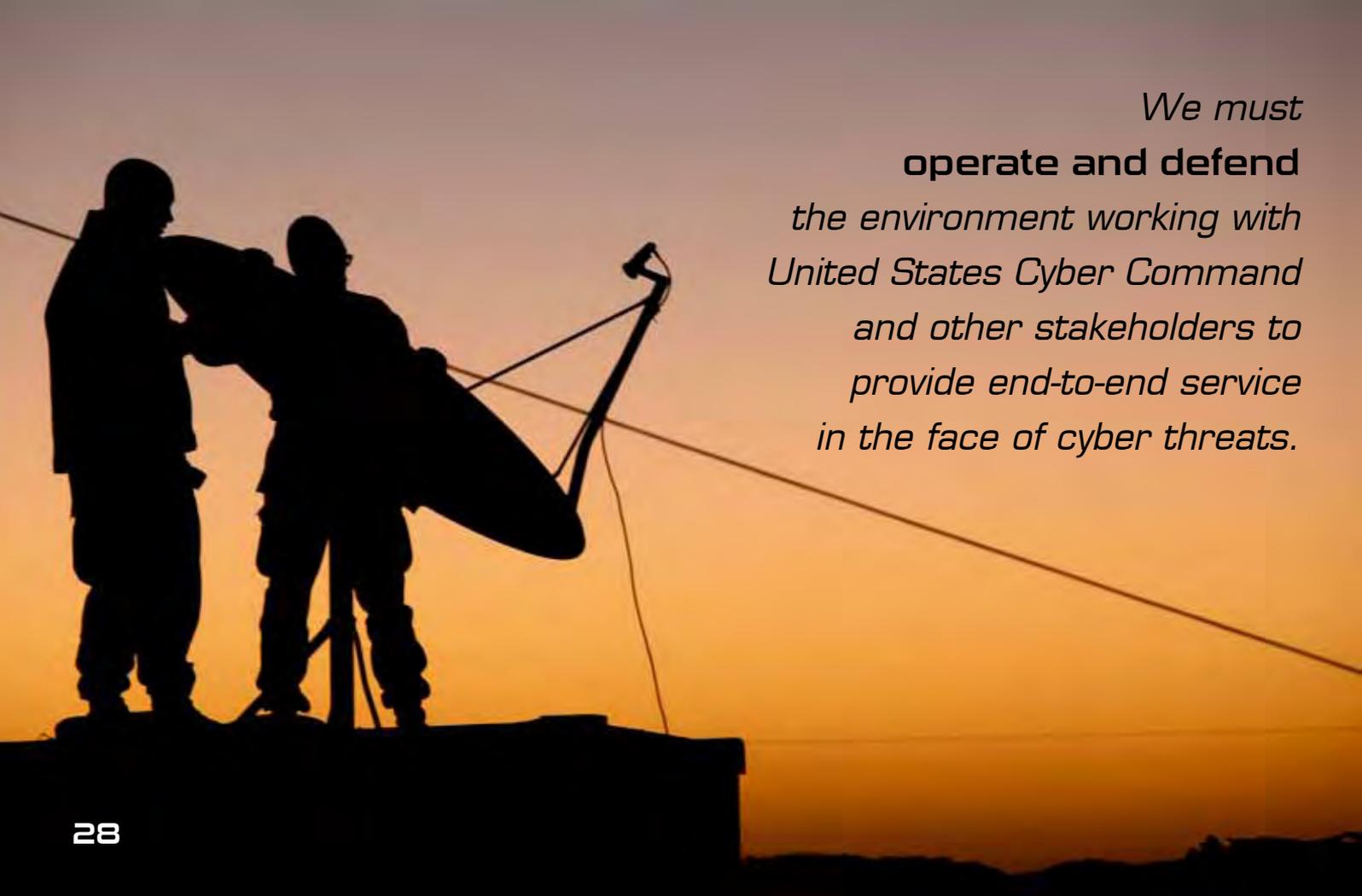
This session will cover the duties and responsibilities of a Defense Information System Network (DISN) node site coordinator. This brief will include functions performed, references, and training as well as an overview of the DISN Node Site Coordinators' Conference hosted annually by DISA CONUS to provide direct collaboration between DISN node site coordinators and DISN operations managers.

SATCOM GIG Integration

The Global Information Grid (GIG) infrastructure is increasingly complex and diverse. To achieve the joint vision for net-centric operations, the GIG must be capable of responding in near-real time to strategic, tactical, and environmental conditions that are very dynamic. This session will cover the GIG converging to the use of Internet protocol (IP) as the main networking protocol in both terrestrial and satellite communications (SATCOM) network and the need to standardize integration of network management interfaces and tools.

Strategic NetOps: Situational Awareness [FOUO]*

As the DISA Command Center (DCC) has matured, a major challenge is solidifying the operational and reporting roles of the DCC to provided strategic NetOps situational awareness. What are the functional requirements for current ops as well as network assurance? This session will address these concerns. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*



*We must
operate and defend
the environment working with
United States Cyber Command
and other stakeholders to
provide end-to-end service
in the face of cyber threats.*

CONTRACTING Track Schedule

Tuesday

3 p.m. – 4 p.m.	Best Procurement Practices and Helpful Information	Room 316
	A DISA Strategic Alignment: Complement, Connect, and Commit	Room 325
4:30 p.m. – 5:30 p.m.	Topical Telecommunication Issues	Room 325

Wednesday

2:30 p.m. – 3:30 p.m.	The Fork in the Road: Priming or Subcontracting ... You Decide	Room 316
-----------------------	--	----------

Thursday

2:30 p.m. – 3:30 p.m.	DoD Source Selection Procedures Changes; Mythbusting; etc.	Room 316
-----------------------	--	----------

A DISA Strategic Alignment: Complement, Connect, and Commit

This is a session for small businesses only. The Office Of Small Business Programs will host a discussion on effective strategic alignment within DISA.

Best Procurement Practices and Helpful Information

This track will include the following topics: Evaluation Criteria for Federal Acquisition Regulation (FAR) Parts 8 & 16 Requirements; How to Make Requirements More Competitive; How to Improve Justifications and Approvals (J&As); Procurement Package Information; Procurement Action Lead Times (PALTS); and ENCORE II.

DoD Source Selection Procedures Changes; Mythbusting; Competition; Efficiency Initiatives; Section 813 Contracting Integrity Panel

This track will include recent changes to source selection procedures of the Department of Defense (DoD); improving communication with industry during the acquisition process ("mythbusting"); competition changes; the Department's Efficiency Initiatives; and Section 813 Contracting Integrity Panel.

The Fork in the Road: Priming or Subcontracting ... You Decide

The DISA Office of Small Business Programs will host a panel session comprised of large and small businesses, providing tips, tools, and techniques for successful priming and/or subcontracting.

Topical Telecommunication Issues

This track will include an overview of the Department of Defense Chief Information Officer (DoD CIO) Vision and Enterprise Strategy Roadmap. Governance structure, data service initiatives, and funding approach activities planned for 2011 and 2012 will also be discussed.

Engineering Track Schedule

Tuesday

1:45 p.m. – 2:45 p.m.	GIG Modeling and Simulation Analysis	Room 325
3 p.m. – 4 p.m.	Community Case Studies (Lessons Learned)	Room 301
	Forge 101 – An Introduction to Forge.mil	Room 321-323
4:30 p.m. – 5:30 p.m.	Continuous Delivery: Maximize Velocity and Value	Room 321-323
	Demystifying Agile Software Development	Room 327
	Interoperability Enhancement Process Information (IEP)/	
	Status Brief [FOUO]*	Room 326
	Joint Capability Technology Demonstrations (JCTDs)	Room 330

Wednesday

10:30 a.m. – 11:30 a.m.	Forge.mil: On-ramp to the DoD Cloud	Room 308
	DISA's Transition to Model-based Systems Engineering using SysML (30 min)	Room 325
	Joint Capability Technology Demonstrations (JCTDs)	Room 307
1 p.m. – 2 p.m.	Forge.mil: On-ramp to the DoD Cloud	Room 307
	Forge 101 – An Introduction to Forge.mil	Room 308
	Community Case Studies (Lessons Learned)	Room 321-323
	Developing GIG Services for the Tactical Edge: Problems, Tech Approaches, Techniques and Design Patterns	Room 326
2:30 p.m. – 3:30 p.m.	Demystifying Agile Software Development	Room 308
	End-to-End Performance Modeling, Simulation, & Analysis	Room 325
	Developing GIG Services for the Tactical Edge (continued)	Room 326
	Continuous Delivery: Maximize Velocity and Value	Room 328/329
4 p.m. – 5 p.m.	Developing GIG Services for the Tactical Edge (continued)	Room 326

**Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Community Case Studies (Lessons Learned)

With a user base of more than 10,000 users and more than 500 projects, Forge.mil lessons learned and success stories are as varied as the types of projects, programs, and organizations using the Forge.mil family of services. During this track session, attendees can participate in a lively discussion with the Forge.mil leadership and current customers on how Forge.mil is transforming software development. Hear from current Forge.mil customers who will share their experiences and successes and discuss the benefits of using Forge.mil and how it has improved their own software development activities. Discover collaborative best practices and find out how the Forge.mil Community site is improving collaboration within and across project teams and communities of interest.

Continuous Delivery: Maximize Velocity and Value

The goal of Continuous Delivery is continual development and frequent delivery of “production ready” software to an organization and its customers. Through the use of automated deployment and configuration management techniques, Continuous Delivery helps reduce the complexity and risks typically encountered during the testing and release phases (commonly referred to as ‘the last mile’). This innovative approach consistently yields higher-quality software delivered in a more frequent and rapid fashion. As a result, customers are able to take advantage of the technology updates and innovations as they become available, and quickly react to changing mission needs. During the Continuous Delivery track, the presenters will outline key technologies and techniques used by the Forge.mil project team to achieve its maximum delivery velocity and “satisfy the customer through early and continuous delivery of valuable software” (Agile Manifesto).

Demystifying Agile Software Development

Agile development has been in the mainstream for nearly a decade and has become the methodology of choice at some of the largest and most dynamic private-sector companies in the world. Despite this widespread adoption, agile best practices have gained very little traction in the public sector and the Department of Defense (DoD) in particular. One of the most commonly-held objections is that agile methods lack the process rigor, top-down control and traceability required within DoD. This session will review how DISA implemented the agile methodology to develop the Forge.mil suite of products. The intent of this track is to share how the Forge.mil team leveraged agile best practices to speed delivery and achieve higher quality while maintaining the process rigor required by DoD. The talk begins with a brief overview of the agile process, then deep-dives into how the Forge.mil team tailored agile best practices, leveraged automation and adopted open-source tools to satisfy the delivery requirements of various stakeholders including the operations and information assurance communities and program management teams.

Developing GIG Services for the Tactical Edge: Problems, Technical Approaches, Techniques, and Design Patterns

This session consists of a sequence of presentations aimed at providing an overview of the issues and challenges pertaining to developing Global Information Grid (GIG) services for the tactical edge, and exploring a number of viable and pragmatic approaches to resolving the “Tactical Edge Service” problems. The GIG tactical environment is characterized by disconnected operation, intermittent connectivity, and low bandwidth (DIL) as well as ad hoc mobile networks and other constraints, which require innovative approaches to service development. These presentations will examine a number of technical edge frameworks (TEF) developed by the GIG community to support service development, and also develop a robust technical framework in which a number of technical approaches including Service Adaptation, Tactical Service Design Patterns, and Tactical Network Improvement are described. Each approach entails a few specific techniques that will be illustrated with examples. Additionally, the information assurance (IA) and NetOps capabilities needed to support those approaches will be discussed as well. The objective of this session is to present the latest technical work developed by DISA Enterprise-Wide Systems Engineering (EWSE) in terms of the technical framework and approaches to solving the “Tactical Edge Service” problems.

DISA's Transition to Model-Based Systems Engineering using SysML

This session provides an overview of the Enterprise Engineering (EE) Directorate's initiative to develop DISA capabilities using a model-based systems engineering (MBSE) process and systems modeling language (SysML) versus the traditional document-driven systems engineering process. This presentation will describe EE's effort to develop tailored MBSE processes to create standard requirements, architecture, and design diagrams using SysML for DISA's programs and projects, training the workforce, and piloting MBSE/SysML for GIG Convergence Master Plan (GCMP) version 2.0. The objective of this session is to educate the audience on the benefits of using MBSE and SysML for developing DISA capabilities versus the traditional document-based systems engineering approach.

End-to-End Performance Modeling, Simulation, and Analysis

The Global Information Grid (GIG) is adopting many new information technologies such as synchronous and asynchronous collaboration; virtualized desktop and server computing infrastructure; dynamic service provisioning; as well as the second generation of web design to support social networking and sharing of user-generated content. With these new technologies emerging at a rapid pace, it is often difficult to predict or troubleshoot performance-related issues either before or after service deployment. This briefing will discuss DISA's capability in conducting end-to-end performance simulation, modeling, and analysis, as well as the benefits achieved from both end-user and service provider points of view.

GIG Modeling and Simulation Analysis

This presentation will provide updates on recent activities in communications modeling, simulation, and analysis (MSSA), especially Joint Communication Simulation System (JCSS) modeling support to Global Information Grid (GIG) Enterprise-Wide Systems Engineering (EWSE) activities. JCSS provides communications planners and system analysts with the capability to analyze existing and proposed network architectures and predictively evaluate the performance of new devices and applications. By simulating communications effects of existing or planned networks that support warfighter operations, JCSS helps to quantify risks and identify command, control, communications, and computers (C4) deficiencies prior to execution or change implementation. Thus, results from JCSS simulations and analyses could provide support for prudent acquisition decisions. Another important role of JCSS is that it acts as a repository for communications models developed by services and agencies throughout the Department of Defense (DoD). By allowing these databases, models, and templates to be used and shared by others, modeling studies conducted using JCSS result in a higher fidelity and more consistent product throughout DoD. DISA/the Modeling and Simulation Division of the Enterprise Engineering Directorate employs JCSS to provide modeling and simulation support for DISA programs. Meanwhile, other military services and agencies apply it as appropriate to their modeling of communications projects and programs.

Forge 101 - An Introduction to Forge.mil

DISA's Forge.mil is a family of services designed to improve the ability of the Department of Defense (DoD) to rapidly deliver dependable software, services, and systems in support of net-centric operations and warfare. Forge.mil uses an application lifecycle management (ALM) platform as well as a collaborative content and knowledge management system along with open source collaborative principles and the DoD private, secure cloud computing infrastructure to reduce costs and speed innovation. Learn how to participate in this growing community of developers, program managers, testers, certifiers, system administrators, end users and warfighters to connect with other Forge.mil users, find and join existing projects and community groups, create your own project, build your own community, and discover and download software for use and re-use. Understand the benefits of Forge.mil and how to make the most of the current capabilities to improve your own team's development and delivery of software, services, and systems.

Forge.mil: On-ramp to the DoD Cloud

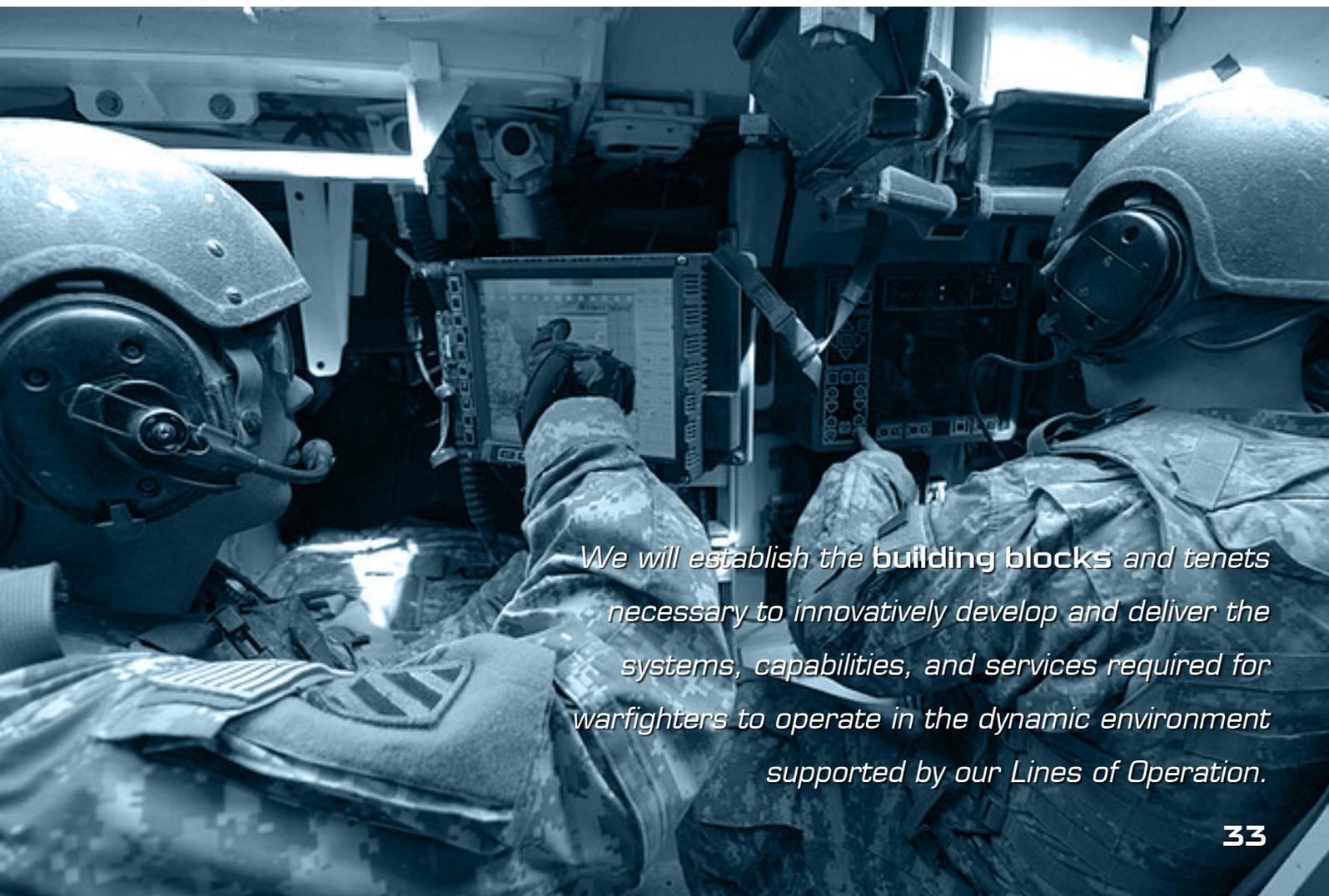
Since its inception in 2009, Forge.mil, the groundbreaking Department of Defense (DoD) collaborative software development platform, has improved the ability of projects and programs to rapidly deliver dependable software. Learn how Forge.mil supports other DoD initiatives to include Agile Software Development, Cloud Computing and the DoD Storefront. This session will provide an overview of existing Forge.mil capabilities such as the Forge.mil Community; SoftwareForge; ProjectForge; information on available external integrations to include continuous integration with Hudson and the DoD private, secure cloud computing infrastructure; and a look at what is on the Forge.mil Product Roadmap to include emerging Forge.mil testing services and automation techniques to support continuous delivery of software.

Interoperability Enhancement Process (IEP) Information/Status Brief [FOUO]*

This presentation is targeted at service component program managers who require implementation of tactical data links (i.e. Link 16, VMF) and will provide the status on the IEP effort led by DISA and the Joint Staff regarding improving interoperability of tactical data links from a lifecycle perspective. IEP consists of Joint Interoperable Systems Management and Requirements Transformation (iSMART) and Joint Capabilities and Limitations (JC&L). This presentation is intended to provide an overview of this Joint effort as it has evolved over the last three years. **Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

Joint Capability Technology Demonstrations (JCTDs) (Advanced Concepts Office)

These short term, sprint-based programs are one of the enablers being leveraged to rapidly achieve a service-oriented, web-based, enterprise infrastructure for the Department of Defense (DoD) as envisioned by the Vice Chairman of the Joint Chiefs of Staff (VCJCS).



We will establish the building blocks and tenets necessary to innovatively develop and deliver the systems, capabilities, and services required for warfighters to operate in the dynamic environment supported by our Lines of Operation.



Information, Knowledge Management & Process Improvement Track Schedule

Tuesday

4:30 p.m. – 5:30 p.m.	How Upcoming Process Changes Will Impact DISA Customers	Room 316
-----------------------	---	----------

Wednesday

10:30 a.m. – 11:30 a.m.	ITSMO Overview	Room 309
	Knowledge Management in a SharePoint Environment	Room 316

**Government attendees and contractors with a need to know ONLY. Additional badging required (active military ID for military, CAC for government attendees or government contractors).*

DISA IT Service Management Office (ITSMO) Overview

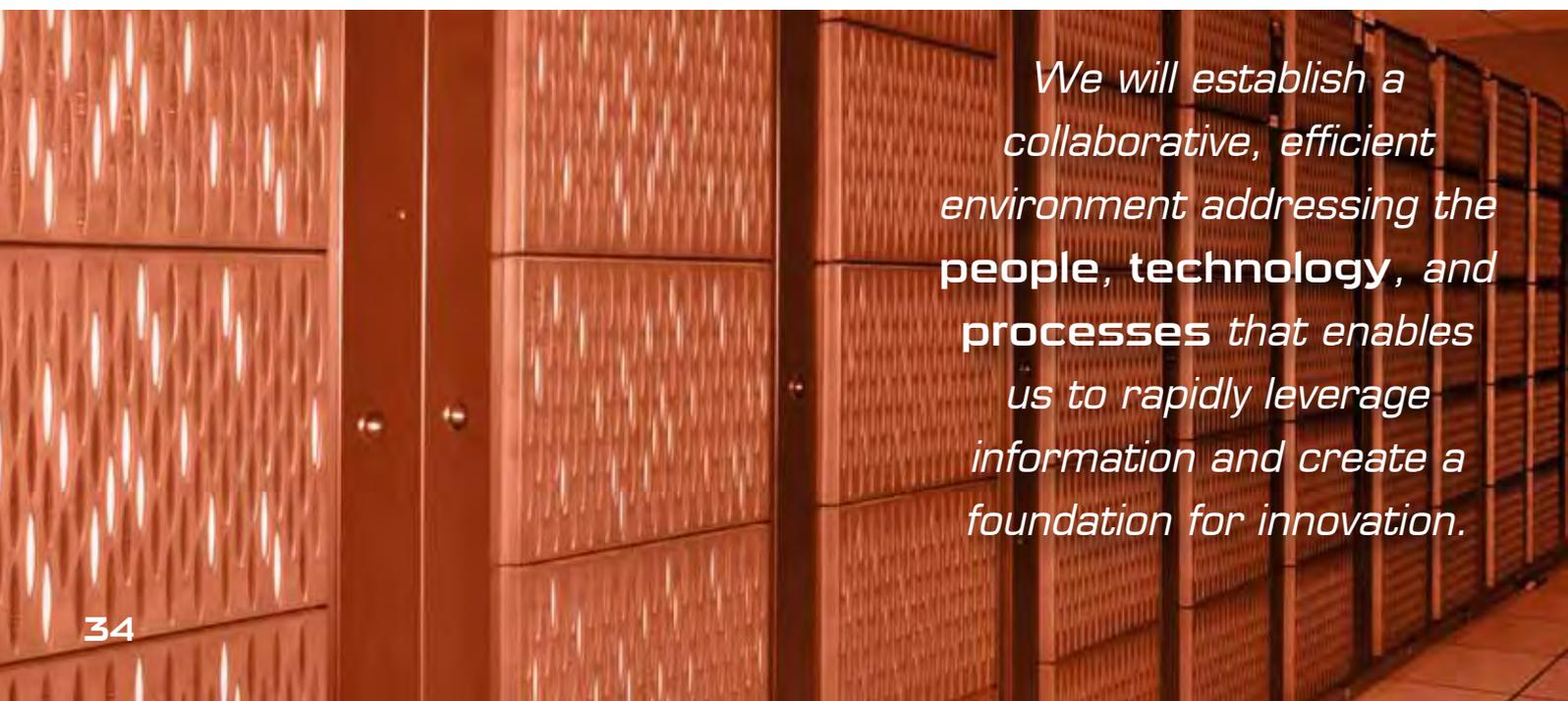
The origin and mission of the Information Technology Service Management Office (ITSMO) will be presented in this session. The session will include DISA's approach to process improvement, including governance, key project milestones, deliverables, and timelines. It will also include process improvements to date, our unique challenges, and objectives through fiscal year 2014.

How Upcoming Process Changes Will Impact DISA Customers

This session will discuss how process improvement initiatives currently in progress will impact customers. It will discuss how governance decisions and actions will be communicated, how improved configuration management processes will improve handling of incidents, how consolidation of a service catalog will provide a one-stop shopping point, and how knowledge management initiatives improve consistency of corporate communications to customers and many others.

Knowledge Management in a SharePoint Environment

This session will serve as an overview of the DISA vShare program and how DISA is using the enterprise SharePoint as a DISA service offering to manage knowledge in the agency.



We will establish a collaborative, efficient environment addressing the people, technology, and processes that enables us to rapidly leverage information and create a foundation for innovation.

Spectrum Track Schedule

Tuesday

1:45 p.m. – 2:45 p.m.	Spectrum Access: The Means to Connect	Room 326
3 p.m. – 4 p.m.	Spectrum Access: GEMSIS, The Tools to Connect	Room 326

Thursday

2:30 p.m. – 3:30 p.m.	Spectrum Access: The Means to Connect	Room 326
4 p.m. – 5 p.m.	Spectrum Access: GEMSIS, The Tools to Connect	Room 326

Spectrum Access: GEMSIS, The Tools to Connect

This track will explain how the Global Electromagnetic Spectrum Information System (GEMSIS) is improving spectrum access by providing capabilities that support the management and deconfliction of the electromagnetic spectrum and enable effective spectrum use for the warfighter worldwide. The GEMSIS program supports the overall DISA vision of enabling information dominance through effective spectrum operations. This presentation will address how GEMSIS present and future capabilities will support that vision. It will provide details on GEMSIS Increments 1 and 2 and will provide its approach for integrating those capabilities into a common desktop for the user. By providing the next generation suite of spectrum management tools, GEMSIS is a key component in providing and assuring spectrum access.

Spectrum Access: The Means to Connect

The world is going wireless! Everything from smart phones, to tablet PCs, to secure mobile environment portable electronic devices (SME PEDs) - is using wireless technologies to make our lives easier. Wireless technology is not only affecting our daily lives, but is also affecting the way the Department of Defense (DoD) conducts its missions. Military operations are becoming increasingly information-centric, which requires seamless, ubiquitous access to the Global Information Grid (GIG) - in most instances through wireless technology. But wireless technology requires access to the electromagnetic spectrum, which is a fragile and limited resource. This track session will talk about the electromagnetic spectrum - what it is, how important it is to the DoD warfighting capabilities, how it is managed, the challenges to spectrum access, and how the Defense Spectrum Organization (DSO) is supporting DoD to ensure its spectrum access. This session will also include a presentation on the Global Electromagnetic Spectrum Information System (GEMSIS), which is the DoD program of record that will provide the capabilities necessary to address the spectrum management challenges of today and the future.

*We will enable
information dominance through
effective spectrum operations.*



Testing Track Schedule

(See synopses on opposite page for subtopics)

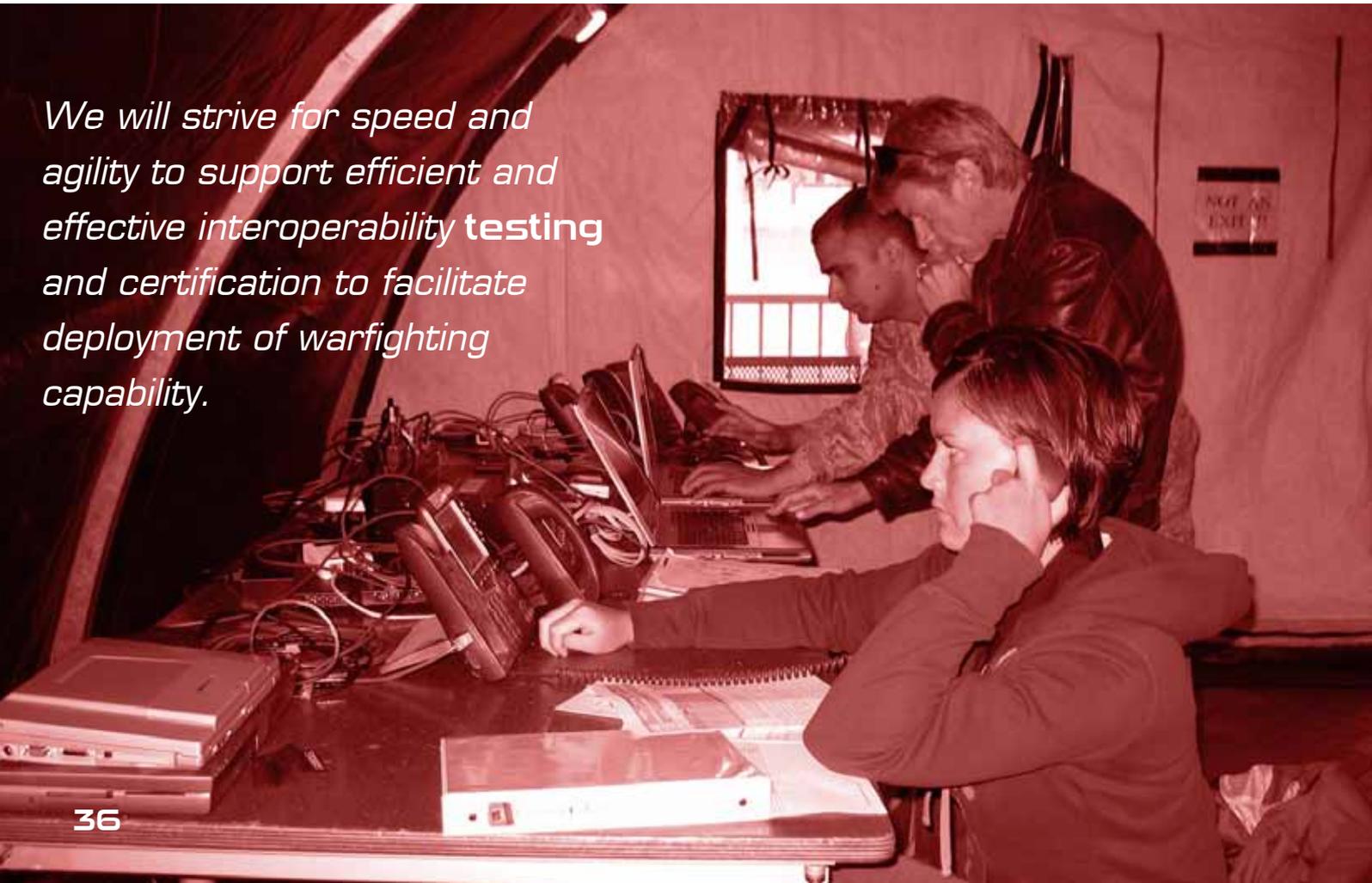
Tuesday

1:45 p.m. – 2:45 p.m.	Agile Testing (Part 1)	Ballroom III
3 p.m. – 4 p.m.	Agile Testing (Part 2)	Ballroom III
4:30 p.m. – 5:30 p.m.	The Evolution of the T&E Infrastructure	Ballroom III

Wednesday

10:30 a.m. – 11:30 a.m.	Test and Certification Today (Part 1)	Ballroom III
1 p.m. – 2 p.m.	Test and Certification Today (Part 2)	Ballroom III
2:30 p.m. – 3:30 p.m.	Beyond DoD - Expanding T&E Partnerships (Part 1)	Ballroom III
4 p.m. – 5 p.m.	Beyond DoD - Expanding T&E Partnerships (Part 2)	Ballroom III

We will strive for speed and agility to support efficient and effective interoperability testing and certification to facilitate deployment of warfighting capability.



Agile Testing

Part 1

IT Acquisition Reform Update

Agile Test and Evaluation — A Workforce Evolution

Part 2

Application of Agile Testing Process to Global Combat Support System - Joint (GCSS-J)

Sharing Agile Best Practices — The JITC Agile Center of Excellence

Evolution in testing and evaluation (T&E) approaches toward a more Agile model requires that those charged with developing the standardized methodologies and providing the T&E infrastructure must operate in an even more complex world. Concepts such as Agile T&E are necessary to keep pace with the rapid development and evolution of technology and capabilities the Department of Defense (DoD) is producing as core concepts in supporting storefront capabilities. As testers, we must change our mindset from traditional “proof testing” to a more decision-maker based test concept that provides information not just on whether a product or service meets the minimum requirements, but also on how well it performs, how secure it is, how it interoperates with other systems and components, and how effective and suitable it is for the operator – all in the context of the intended operational environment.

Beyond DoD – Expanding T&E Partnerships

Part 1

Coalition Testing — CIAV

Testing in Support of the Afghan Mission Network

IPAWS — This is Truly a Test of the Emergency Alert System

Part 2

Federal Agency Testing — Test and Evaluation Partnership with Department of Homeland Security (DHS)

In today’s threat environment, information sharing has become mission critical throughout the Department of Defense (DoD), coalition and allied nations, as well as all levels of local, state, and federal non-DoD organizations. The Department of Homeland Security (DHS) and DoD have similar mission requirements, and unique partnerships to include Defense Support of Civil Authorities activities. Unfortunately, there is an inherent lack of testing between DoD and non-DoD entities, primarily because of different funding streams and stovepipe-based organizational structures, resulting in DoD reluctance to spend money on testing external to DoD, and vice versa. Expanding and strengthening T&E partnerships throughout will enhance these information sharing requirements, and ensure mission success.

Test and Certification Today

Part 1

Unified Capabilities Requirements — Testing Products for the Approved Products List

Rolling with DICE — Interoperability Certification for Joint Task Force Communications Capabilities

Part 2

Testing and Certification — Government and Industry Perspectives,

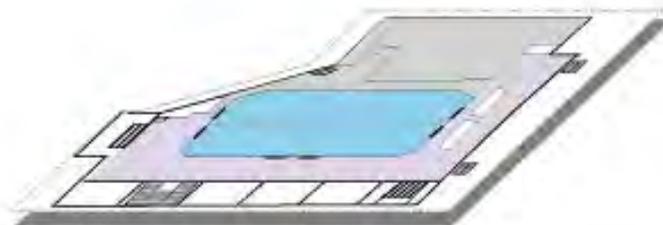
Testing and certification for products governed by the Unified Capabilities Requirements 2008 (UCR 2008) are focused on accelerating the delivery of critical communications capabilities to the nation’s warfighters while maintaining the technical and testing rigor to ensure interoperability and mission accomplishment. This track will present the Special Interoperability Certification process for UC products, the concepts and processes implemented through distributed testing to shorten the testing timeline, the upcoming changes and impacts of UCR 2008 Change 2, and the mechanisms to speed tactical solutions and requirements through the fast-track requirements process.

The Evolution of the T&E Infrastructure

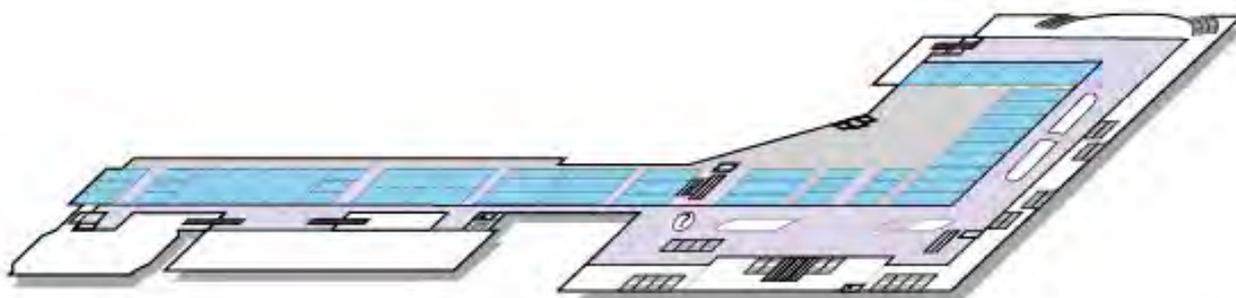
Converging Test and Evaluation Network Services and Test Forge and Virtualization

Presentations within this track will focus on how DISA and the Joint Interoperability Test Command (JITC) provision test and evaluation (T&E) network, modeling and simulation, and instrumentation capabilities to customers; provide some insight into DISA’s effort to converge Department of Defense (DoD) T&E networks onto the Defense Information System Network (DISN); and lay out the way ahead for how DISA and JITC intend to provision compliance, virtualization, mission scenarios, and other testing capabilities as a service via testforge.mil.

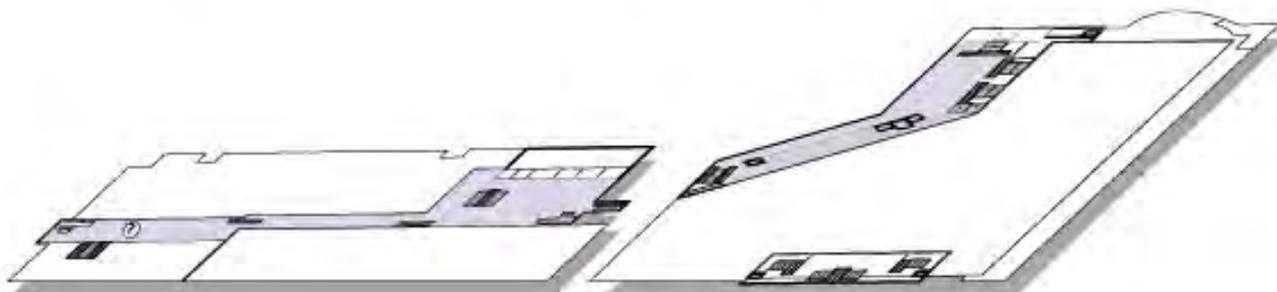
Baltimore Convention Center



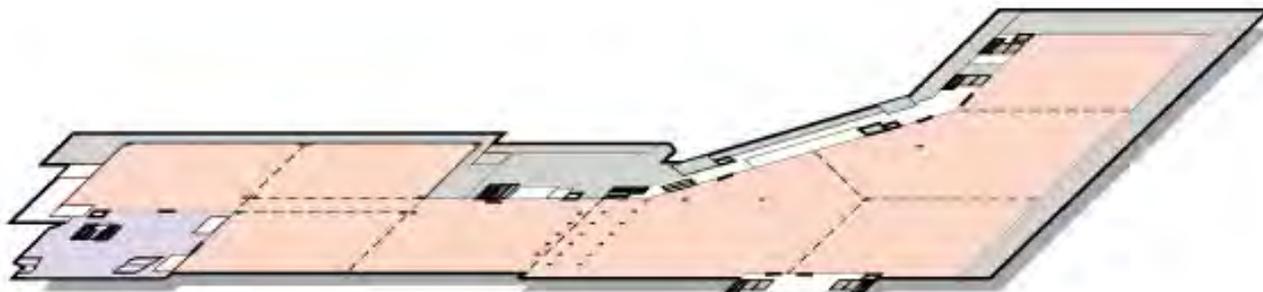
Level 400



Level 300



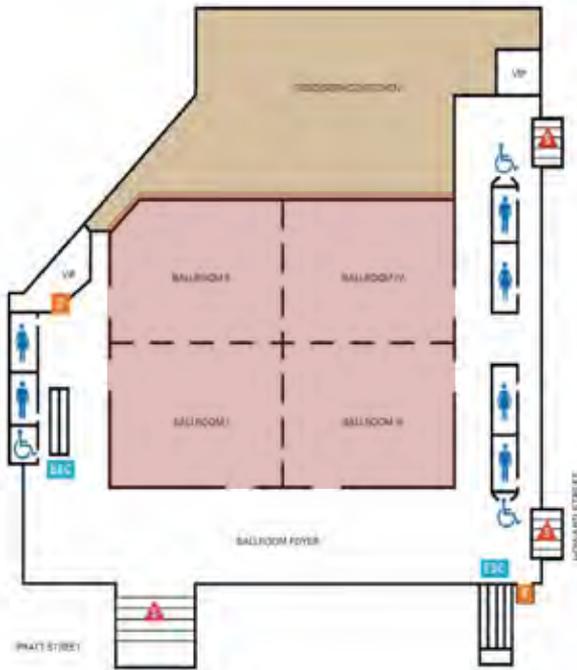
Level 200



Level 100

Level 400

Track Sessions



Level 300

Breakfast

Track Sessions



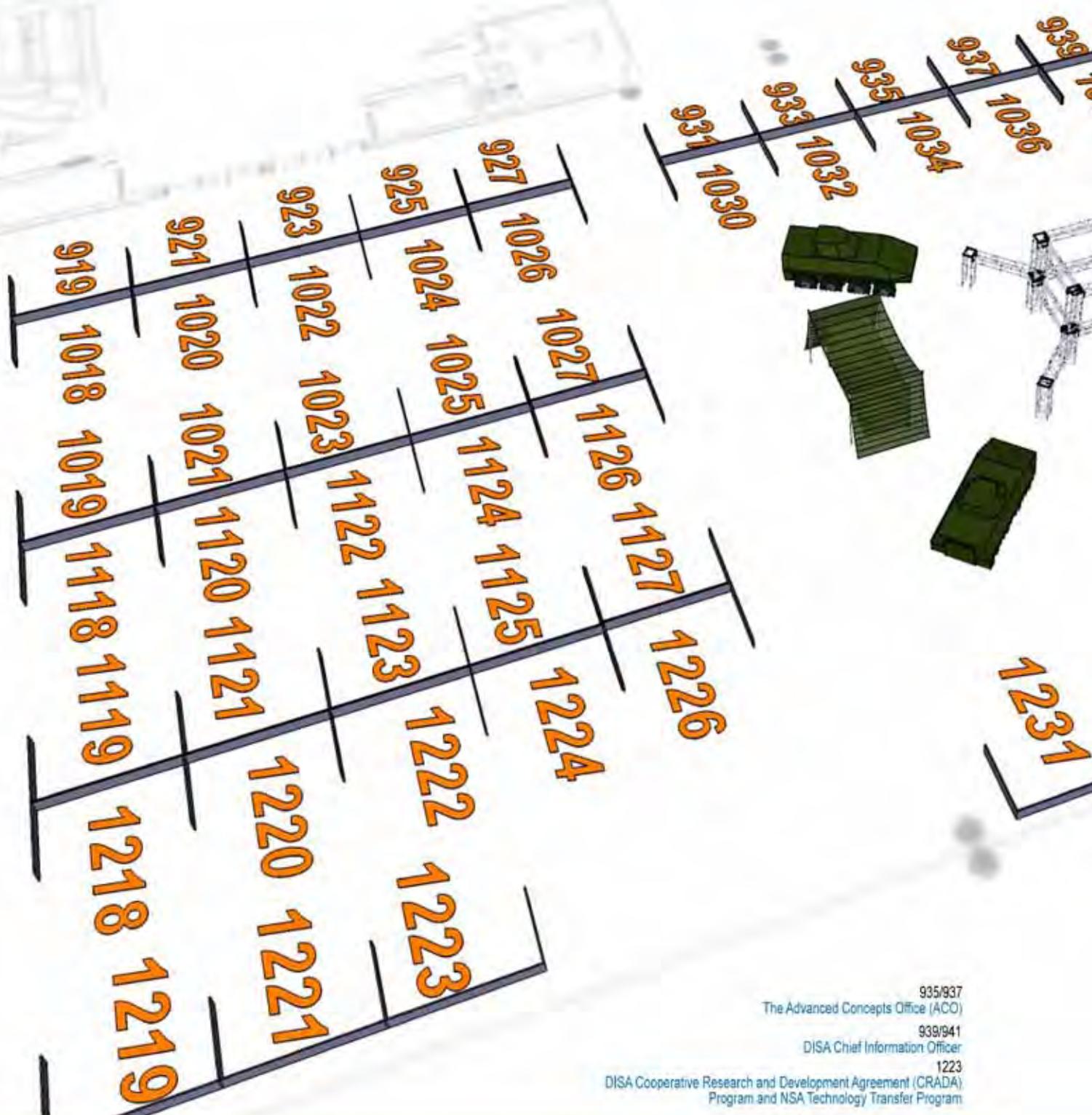
Level 100

Registration

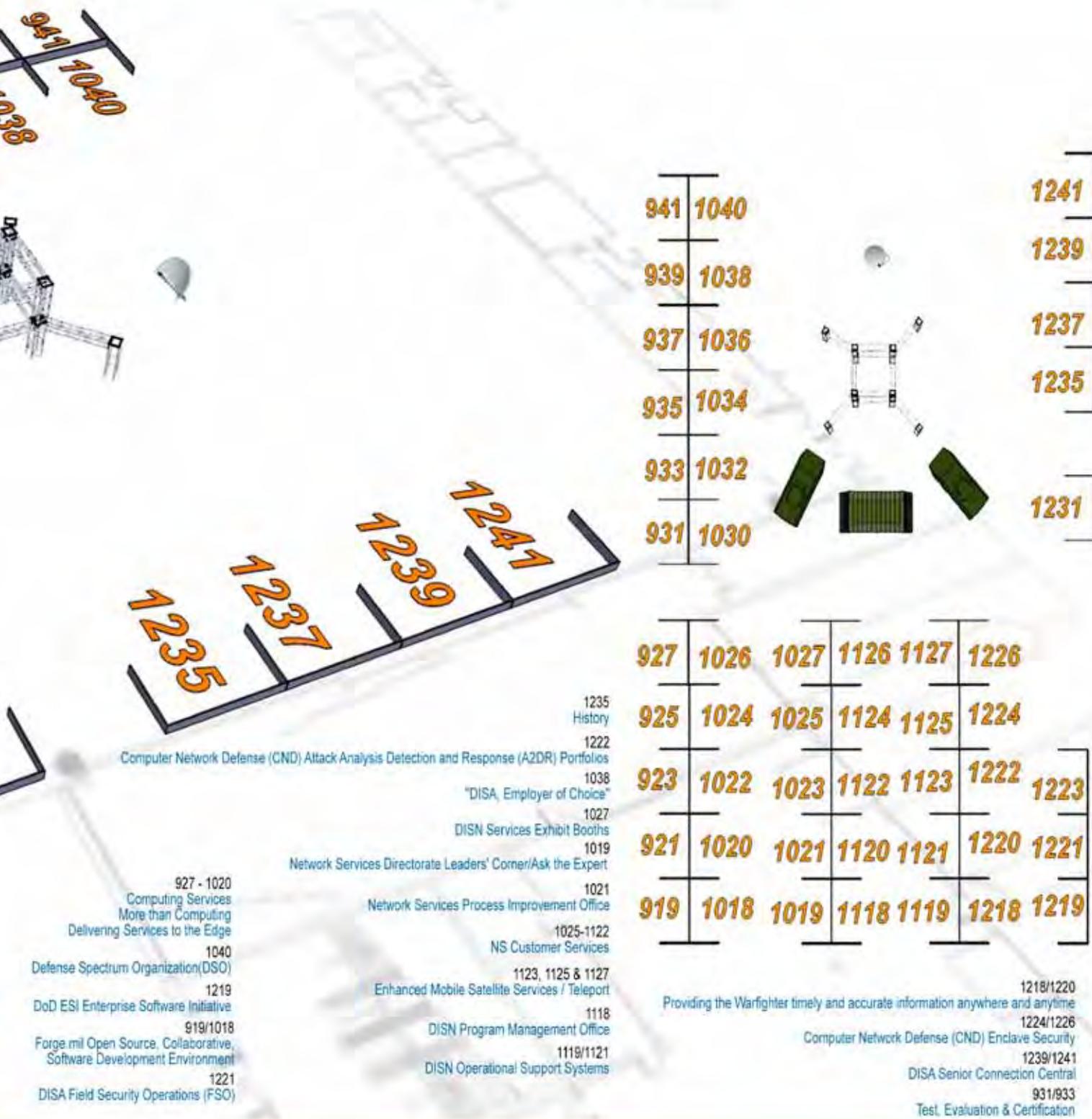
DISA Exhibit and AFCEA Technology Showcase

Plenary Sessions





935/937
The Advanced Concepts Office (ACO)
939/941
DISA Chief Information Officer
1223
DISA Cooperative Research and Development Agreement (CRADA)
Program and NSA Technology Transfer Program



The DISA Campaign Plan defines our mission, vision, and objectives and illustrates our roadmap for success. This plan guides the allocation of our resources and the execution of critical investment decisions. The actions and tasks within this plan provide the basis upon which we set performance measurement goals and continuously assess our progress. It is a living document. As the goals of the Department evolve, we will adjust our direction and update the plan annually.

The Campaign Plan is also the foundation of our planning, Program Objective Memorandum (POM), and budget, which are inextricably linked. Each responsible organization will make the successful execution of the Campaign Plan tasks their top priority within the performance of their basic missions. The planned actions and tasks will be executed to the degree resources are available. In those areas where resources are not presently available, the DISA Strategic

Planning and Information Directorate and the DISA Comptroller will work with the responsible organizations to develop funding strategies, as appropriate, to ensure alignment with the Agency's ongoing and emerging priorities.

As in the 2010 Campaign Plan, we are organized into three Lines of Operation (Enterprise Infrastructure; Command and Control and Information Sharing; and Operate and Assure) and nine Joint Enablers (Acquisition; Contracting; Engineering; Information, Knowledge Management, and Process Improvement; People; Planning; Resources; Spectrum; and Testing).

The Lines of Operation and Joint Enablers provide the framework for planning and budgeting, set our priorities, and describe the ways and means by which we will attain our strategic objectives. Underpinning our way ahead and fundamental to all that we do are the following seven guiding principles.



DISA'S GUIDING PRINCIPLES

1 OUR MISSION AND RESPONSIBILITIES ARE GLOBAL.

DISA is required to provide information at Internet speed with available and emerging technologies, such that anyone who can connect to the network can provide and consume data and services anywhere on the network globally.

2 OUR ENTERPRISE SUPPORTS THE DEFENSE DEPARTMENT AND ITS MISSION PARTNERS.

Over the decades, DISA has been engaged in every mission the Department has undertaken. These engagements have become increasingly interagency and international, and our partnerships have increased to reflect this.

3 WE MUST SUPPORT THE FULL SPECTRUM OF OPERATIONS.

The capabilities and services we provide support information sharing and facilitate decisionmaking no matter the challenges faced and no matter where the information is located or sourced.

4 WE OPERATE IN A CONTESTED BATTLE SPACE.

Mission success is dependent upon our ability to fight through a concentrated attack while reducing the attack surface, continually improving our command and control of the network, and assuring safe sharing of information.

5 WE PROVIDE INTEGRATED, INTEROPERABLE, ASSURED INFRASTRUCTURE, CAPABILITIES, AND SERVICES THAT RECOGNIZE THE ENTERPRISE BEGINS AT THE EDGE.

The edge is where any individual or system associated with defense of our Nation is located, and we are committed to the user wherever on the globe the user operates.

6 OUR GOAL IS TO ENABLE AND ENSURE END-TO-END SERVICE.

We and our mission partners are engaged from user to user – from wherever information is produced to where it is consumed.

7 THE DISA ENTERPRISE MUST BE ALWAYS-ON.

The capabilities and services DISA provides are expected to be on and available to users 24x7x365.

READ THE EXECUTIVE
SUMMARY OF THE DISA
CAMPAIGN PLAN AT

[www.disa.mil/
campaignplan](http://www.disa.mil/campaignplan)



www.DISA.mil