DON IT Conference, West Coast 2019
Feb. 13-15, San Diego Convention Center
Session Descriptions

WEDNESDAY, FEBRUARY 13

PEO EIS Strategy Overview
Wed., 8:00 – 9:00 am

This session will provide an overview of the recently updated PEO EIS strategy and priority items for the next year.

Speaker(s): Ruth Youngs Lew (PEO EIS)

Defense Business System Certifications
Wed., 8:00 – 9:00 am

This session will provide an overview of the DBS certification process and requirements, with a Q&A session at the end.

Speaker(s): Kris Griffin/Margo Spratley (DON OCMO); Brooke Zimmerman (OPNAV N2/N6); Julius Pfeifle (HQMC C4)

USMC Risk Management Framework Course for ISSMs and Validators
Wed., 8:00 am – 4:00 pm

This interactive lecture style course is intended to provide an overview of the Marine Corps implementation of both the ISSM and Validator processes as detailed in DoDI 8510.01, Risk Management Framework for DoD IT, and the USMC Enterprise Cybersecurity Manual (ECSM) 018.

The first two days of this course are appropriate for both ISSM's and Validators. Key points will include but are not limited to: roles and responsibilities, defense in depth functional implementation architecture, alignment to the information systems security engineering process, risk scoring, and HQMC C4 CY A&A expectations.

The final day will encompass the process and procedures necessary for the successful execution of the Validator activities through the use of Marine Corps Compliance and Authorization Support Tool (MCCAST), DISA STIG Viewer, Assured Compliance Assessment Solution (ACAS) and other tools. Key points will include but are not limited to; roles and

responsibilities, assessment requirements, validation procedures, risk scoring, Security Assessment Report (SAR) development, and POA&M initialization.

Speaker(s): Mr. Josh Ingraham (HQMC C4 A&A Branch Head); Mr. Naveed Mirza (HQMC C4 A&A Tech Lead)

Facilities Related Control System Risk Management Framework Implementation
Wed, 8:00 am – 4:00 pm

The Naval Facilities Engineering Command (NAVFAC) Functional Security Control Assessor (FSCA) and Functional Authorizing Official (FAO) offices will conduct advanced training on FRCS-specific RMF implementation for the Navy, building on the previous training given during NAVFAC hosted Cybersecurity Boot Camps in 2017 and 2018.

Session 1 (2 hours, 0800-1000): RMF Steps 1 and 2. Detailed discussion of the NAVFAC FRCS inheritance model. Control selection and tailoring, hardware and software identification and documentation, development of a comprehensive Security Assessment Plan. eMASS implementation demonstrated. Review of the RMF Step 2 Checkpoint Review Checklists as guided by the NAVFAC Echelon II, FSCA and FAO business rules.

Session 2 (4 hours, 1000-1200, 1300-1500, lunch break in middle): RMF Step 3. Detailed training on NIST 800-53 and 800-82 security control implementation for FRCS systems, proper control statements in eMASS, best practices for mapping between scans, STIGs, and SRGs into the eMASS POA&M. Hands-on learning and real system examples will be used to demonstrate implementation process and expectations of the validator.

Session 3 (1 hour, 1500-1600): RMF Step 4 preparation. Detailed discussion of pre-validation site guidance and Step 4 Validator checklist to inform and familiarize field personnel with proper procedures for ensuring their FRCS are fully prepared for Step 4 on-site validation.

Government & Contractors / CAC Required for this Session

Speaker(s): Dawn Berry (NAVFAC FSCA TAE); David Wanamaker (NAVFAC FSCA Team Lead); Richard Perkins (NAVFAC Validation SME); Tara Houlden, (NAVFAC Cybersecurity Director); Paul Sparks (NAVFAC FAO Team Lead); Anthony Prudencio (NAVFAC ECH II PSO SME)

Modern Service Delivery
Wed., 9:15 – 10:15 am

This panel will provide an overview of the Navy's modern service delivery strategy, including mobility.

Speaker(s): Jane Rathbun (DASN C4I/IO/Space) (tentative); Andrew Tash (PEO EIS, Technical Director); CAPT Ben McNeal (PMW 205, PM); Dave Driegert (PMW 240, Single Point of Entry Assistant Program Manager)

Business Capability Acquisition Cycle

Wed., 9:15 -10:15 am

This session will provide an overview of the BCAC process and requirements, with a Q&A session at the end.

Speaker(s): Kris Griffin/Margo Spratley (DON OCMO); Todd Barnhill (DASN (C4I); Brooke Zimmerman (OPNAV N2/N6) (tentative); Julius Pfeifle (HQMC C4) (tentative); Andrew Atkinson (PEO-EIS) (tentative)

CIO Town Hall & DON IM/IT Excellence Awards
Wed., 10:30 – 11:50 am

The Director OCIO will be joined by Mr. Modly, VADM Kohler, and BGen (sel) Mahlock to briefly discuss their priorities, challenges, and opportunities related to DON IT. Time permitting, there will be a question and answer session at the end. The town hall will end with the presentation of DON IM/IT Excellence Awards.

Speaker(s):

Mr. Thomas Modly (Under Secretary of the Navy, DON CIO, DON CMO)

VADM Matthew Kohler (Deputy Chief of Naval Operations for Information Warfare/ Director of Naval Intelligence, DON Deputy CIO (Navy)) - invited

BGen (Sel) Lorna Mahlock (Director, Command, Control, Communications and Computers (C4), DON Deputy CIO (Marine Corps))

CAPT Damen Hofheinz (Director Office of the CIO)

Navy Enterprise Commercial Cloud Blanket Purchase Agreement Workshop
Wed., 2:00 – 3:00 pm

This Navy Commercial Cloud Project Office-led (PMW 270) workshop will answer your questions about the recently Navy Enterprise Commercial Cloud Blanket Purchase Agreement (BPA). What it is, what services are available, and how you can place orders on it. Speak with representatives from NCCS, the contract ordering team, and the BPA managed service provider.

Government & Contractors / CAC Required for this Session.

Speaker(s): Travis Methvin (PMW 270, Project Manager); contract ordering team; BPA managed service provider

---

These 3 SYSCOMS Messed with Knowledge Management, See What Happened!
Wed., 2:00 – 5:00 pm

This session will share the Knowledge Management (KM) journeys embarked upon by three SYSCOMS. You'll hear and see their different approaches, which resulted in varying outcomes. Additionally, you'll have an opportunity to interact with other attendees using the Knowledge Café construct. Participating in this session will provide you takeaways and Lessons Learned to aid your organization in making your KM program more successful.

Speaker(s): Representatives from SPAWAR, NAVSEA, and NAVAIR

DON Enterprise Software Licensing Process

Wed., 3:15 – 4:15 pm

The DON ESL Team will provide an overview of the DON ESL process. This discussion will provide greater fidelity into the process, timelines, structure, and deliverables required to award enterprise license agreements. The goal is for Original Equipment Manufacturers (OEM), resellers, and members of the DON to understand how an ESL is structured and awarded, when stakeholder information is required and its impact to the agreement as a whole.

Defense contractors/vendors are invited to attend this session.

Speaker(s): LtCol Clinger (DON ESL Team Lead)

SPAWAR Technical Vision: Conflict 2037

Wed., 4:15 – 5:15 pm

How will future technologies (Artificial Intelligence, Cybersecurity, Acquisition, Data Analytics, Cross Domain Solutions, Identity Management) support the warfighters? In addition to a presentation of the SPAWAR Technical Vision, this session will include a screening of the Conflict 2037 vision video, focusing on a rescue mission that encompasses an ideal collaboration across the Department of the Navy.

Government Only / CAC Required for this Session

Speaker(s): Chris Raney (Technical Director, SPAWAR Systems Center Pacific)

THURSDAY, FEBRUARY 14

Navy SCA/NAO RMF Training
Thurs., 8:00 – 11:45 am

The Navy Authorizing Official (NAO) and the Navy Security Control Assessor (SCA) will be providing high-level review of the complete Navy Risk Management Framework (RMF) process. Each RMF step will be addressed and the discussion will include some of the challenges currently faced by the Navy RMF community. The session will conclude with a brief on package review metrics, lessons learned, and best practices that are useful for expediting the RMF process. There will also be a question and answer period, time permitting.

Speaker(s): Navy Authorizing Official; Navy Security Control Assessor

---

USMC Risk Management Framework Course for ISSMs and Validators
Thurs., 8:00 am – 4:00 pm

This interactive lecture style course is intended to provide an overview of the Marine Corps implementation of both the ISSM and Validator processes as detailed in DoDI 8510.01, Risk Management Framework for DoD IT, and the USMC Enterprise Cybersecurity Manual 018.

The first two days of this course are appropriate for both ISSM's and Validators. Key points will include but are not limited to: roles and responsibilities, defense in depth functional implementation architecture, alignment to the information systems security engineering process, risk scoring, and HQMC C4 CY A&A expectations.

The final day will encompass the process and procedures necessary for the successful execution of the Validator activities through the use of Marine Corps Compliance and Authorization Support Tool (MCCAST), DISA STIG Viewer, Assured Compliance Assessment Solution (ACAS) and other tools. Key points will include but are not limited to; roles and responsibilities, assessment requirements, validation procedures, risk scoring, Security Assessment Report (SAR) development, and POA&M initialization.

Speaker(s): Mr. Josh Ingraham (HQMC C4 A&A Branch Head); Mr. Naveed Mirza (HQMC C4 A&A Tech Lead)

Navy Information Application Product Suite (NIAPS)
Thurs., 8:15 – 9:15 am

The Navy Information Application Product Suite (NIAPS) provides Sailors access to courses, programs, and Navy websites at times when internet connectivity is slow or non-existent by minimizing bandwidth requirements through the use of data compression and replication technologies. This session will provide an overview of NIAPS, specifically what it is, how it works, and the process for getting applications hosted on the platform.

Speaker(s): Dave Arellano (PMW 250, APM NIAPS)

ONR Data and Analytics
Thurs., 8:15 – 9:15 am

The Office of Naval Research (ONR) established a Data & Analytics Division in February 2018 to support strategic decision making with in-depth analysis of the Naval Research Enterprise (NRE) portfolio to enhance mission effectiveness for U.S. Naval Forces. This session will provide an overview of the division at the one-year point; how it was formed, the challenges we overcame and those we are still battling, solutions and tools we've produced and those we are still building. This is also an opportunity to connect with you and continue to grow the Naval data and analytics network of professionals.

Speaker(s): Mary Thoms (ONR PIIM Directorate); Matt Poe (ONR PIIM D&A Division)

DITPR/DADMS Update
Thurs., 9:30 – 10:30 am

This session will provide an update on the status and capabilities of DITPR-DON/DADMS. The presentation will include an overview of new capabilities that have been implemented within the system as well as future changes under consideration for the next block upgrade. Program office officials will also discuss high-level plans to perform a version upgrade of the system's core commercial off-the-shelf (COTS) software.

Speaker(s): Patsy Donovan (PMW 250, APM DITPR/DADMS); Amber Sandvick (PMW 250, DITPR/DADMS Project Director)

GSA Best-in-Class Contracts for Information Technology Solutions
Thurs., 9:30 – 10:30 am

This session provides an overview of GSA Information Technology Indefinite Delivery Indefinite Quantity (IDIQ) contracts that include Best-In-Class (BIC) ratings by the Office of Management and Budget (OMB) and help all federal agencies meet category Spend Under Management (SUM) objectives. Government Wide Agency Contracts include; VETS 2, Alliant, Alliant Small Business, and 8(a) STARS II. These contracts enable government IT professionals to gain fast access to cutting-edge IT, communications, and infrastructure products and services that offer integrated customizable solutions for your technology life cycle needs. These pre-competed contracts are with industry leaders and veteran owned businesses capable of providing support services in a secure DOD environment.

Speaker(s): Mark Carico (GSA); Eric Higginbottom (GSA)

MPT&E Transformation
Thurs., 10:45 – 11:45 am

This presentation will cover Manpower, Personnel, Training, and Education (MPT&E) Transformation. MPT&E will consolidate the existing family of MPT&E programs into a single system of systems, which will be built on the core of existing capabilities. MPT&E

Transformation includes four key capability areas: Single Point of Entry, Navy Personnel and Pay, Authoritative Data Environment and Learning Stack. The discussion will cover examples such as MyNavy Portal, Mobile, and Identity and Access Management (IdAM).

Speaker(s): Julianne Lefevre (PMW 240, DPM)

Protecting Yourself from Identity Theft
Thurs., 10:45 – 11:45 am

This session has been very popular in previous conferences and has been updated to provide the latest information regarding identity theft, one of the fastest growing crimes in America. Practical information will be provided to include ways individuals can mitigate or prevent identity fraud from happening, signs that identify whether an individual is a victim, and steps that can be taken to deal with identity theft once they are a victim.

Speaker(s): Steve Muck (DON OCIO Privacy Lead)

PEO EIS Cloud Enablement
Thurs., 1:45 – 2:45 pm

This session will provide an update on PEO EIS's cloud strategy and initiatives.

Speaker(s): Travis Methvin (PMW 270 Project Manager)

USMC Cyber Range Exercise/Training Opportunities Briefing
Thurs., 1:45 – 2:45 pm

The Marine Corps Cyber Range (MCCR) replicates the functionality of the Marine Corps Enterprise Network in support of Training, Exercise, and Testing. The briefing will cover how the MCCR replicates the Quantico and Camp Pendleton MITSC's, Defensive Boundaries, and NACCR capability sets as well as enterprise services of the MCEN. Collocated with the DoD Cybersecurity Range replicating the DISA DODIN Services, Virtual JRSS and Virtual Internet Access Point, the MCCR is uniquely aligned to support defensive and operational engagements leveraging the totality of DoD Defensive Cyber operations. Additionally, the MCCR hosts the Cyber Test and Evaluation Platform (CTEP) learning management system supporting hands on courseware utilizing a built in hypervisor to create simulated networks and labs to allow students hands on skills practice of their craft.

Speaker(s): Jeff Combs (Marine Corps Cyber Range Manager)

NAVFAC / NAVSEA Risk Management Framework (RMF) Assess Only
Thurs., 2:00 – 4:00 pm

The DON's RMF Assess Only process provides a streamlined method by which IT services and products become authorized for use. Although all IT services and products have cybersecurity considerations, not all require triage through the full RMF 6-Step process. This session will provide an overview of how the Assess Only process will be executed under the Functional Authorizing Official (FAO) construct and managed using the eMASS Assess Only module.

Speaker(s): Paul Sparks (NAVFAC), Mr. David Wannamaker (NAVFAC), Tiffannie Farrington (NAVSEA), Mr. George Alves (NAVSEA)

Navy ERP Transition to Suite HANA and Migration to Commercial Cloud
Thurs., 3:00 – 4:00 pm

The Navy Enterprise Resource Planning (ERP) is executing a technical refresh and has a contract with SAP National Security Services to provide IaaS, partial PaaS and to assist with the application transition to the SAP Suite HANA solution. The system to cloud hosting and managed services will be operated via the NAVAIR Cloud Broker. This session will provide an overview of the technical refresh, specifically what it is, how it benefits the Navy, how it complies with the Navy Cloud Broker policy, and how we can support other communities of applications by establishing a SAP HANA platform.

Speaker(s): Shannon Seay (PMW 220, PM)

USMC Cyber/IT Workforce Update/Way Forward
Thurs., 3:00 – 4:00 pm

This session will provide a review of Cyber Workforce Modernization in the Marine Corps including: (1) Review of DoD 8140 Manual, SECNAV Manual 5239 and Enterprise Cybersecurity Manual 024; (2) Deputy Commandant Information's role in the Cyber Community of Interest (COI) and updates to the Cyber IT/Cybersecurity COI; and (3) Changes in workforce coding, training, certification and permission qualification requirements.

Speaker(s): Mr Alfredo Rodriguez (Cyber IT/CS COI Lead); MSgt Michael Dahlke (HQMC C4 Workforce Lead)

Navy Cloud Broker Update
Thurs., 4:15 – 5:15 pm

This panel will provide an overview of the Navy Cloud Brokerage (NCB) structure, the readiness of each NCB, the services each provides, and how to engage with them.

Speaker(s): Travis Methvin (PMW 270, Project Manager); Teri-Lee Holland (SSC LANT, Atlantic Data Center and Cloud Hosting Services Division Head), NAVAIR

Command Cyber Operational Readiness Inspection (CCORI) Brief
Thurs., 4:15 – 5:15 pm

U.S. Fleet Cyber Command's Office of Compliance and Assessment (OCA) launched its Command Cyber Operational Readiness Inspections (CCORI) program in 2018, marking the first time this type of inspection will be directed and conducted by the Navy as service cyber component of U.S. Cyber Command. The CCORI program is fundamentally different from

previous Command Cyber Readiness Inspections (CCRIs). This new inspection program is mission-based, threat-focused and operationally relevant. A CCORI team consists of two dozen personnel, divided into three teams, including the OCA inspection team, supporting commands and site trusted agents. The Mission Element provides an assessment of the impact to the organization's mission if critical systems are compromised, the Vulnerability Element identifies technical and non-technical vulnerabilities, and the Threat Element assesses external, internal and insider attack vectors based on the identified vulnerabilities. CCORI assesses risk to organizational mission by evaluating threats to, and vulnerabilities found within information systems, networks, applications and data.

Additionally, OPNAV N2N6 will share the latest information with respect to the Risk Management Framework (RMF). Focus will be on changes in the last 12 months and a look ahead at the ongoing transition from DIACAP to RMF before DEC 2020.

Speaker(s): CAPT Kristian Kearton, Director, Office of Compliance and Assessment (OCA), FLTCYBERCOM; Representative from OPNAV N2N6

FRIDAY, FEBRUARY 15

DOD Enterprise Software Initiative and IT Category Management
Fri., 8:00 – 9:00 am

This session will provide an overview of the DON and DoD IT Strategic Sourcing and IT Category Management efforts. Discussion will include best practices from DoD Enterprise Software Initiatives (ESI) in alignment with:

- Statutory requirements - Making Electronic Government Accountable By Yielding Tangible Efficiencies (MEGABYTE) Act and National Defense Authorization Acts (NDAA)
- OMB IT Category Management
- DoDD 8470.1E (DoD Executive Agent (EA) for Commercial Software Product Management of Core Enterprise Technology Agreements (CETA)), which designates the Navy as the DoD EA for CETA management

Speaker(s): Floyd Groce (PEO EIS); Chris Pratt (PEO EIS)

USMC Strategic Update Panel
Fri., 8:00 – 10:00 am

This panel will provide an overview and a Q&A forum to discuss the following topics: (1) Office 365/Cloud Implementation; (2) Network Access Control/Compliance Remediation (NACCR); (3) Trusted Proxy/Privileged User; (4) Break & Inspect; (5) Enhanced Web Security; and (6) HTTPS/HSTS Implementation

Speaker(s): Dr. Ray A. Letteer (HQMC C4 Cybersecurity Chief); Ms. Bonnie Bienz (CY Architecture Branch Head); Daniel Norton (CY Assessments Branch Head); TBD (CIO Division)

Enhanced Contractor Security Controls for Sensitive DoD Information

Fri., 8:00 – 10:15 am

Defense Acquisition University (DAU) will facilitate a discussion that focuses on the DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, which applies to all current Department of Defense contractors. This clause requires contractors/subcontractors to: (1) provide adequate security to safeguard covered defense information that resides on, or is transiting through, a contractor's internal information system or network; (2) report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support; and (3) flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information.

Defense contractors are invited to attend this session.

Speaker(s): Chris Newborn and Paul Shaw (Professors of Information Technology, Cybersecurity, Defense Acquisition University)

USMC Risk Management Framework Course for ISSMs and Validators
Fri., 8:00 – 11:45 am

This interactive lecture style course is intended to provide an overview of the Marine Corps implementation of both the ISSM and Validator processes as detailed in DoDI 8510.01, Risk Management Framework for DoD IT, and the USMC Enterprise Cybersecurity Manual (ECSM) 018.

The first two days of this course are appropriate for both ISSM's and Validators. Key points will include but are not limited to: roles and responsibilities, defense in depth functional implementation architecture, alignment to the information systems security engineering process, risk scoring, and HQMC C4 CY A&A expectations.

The final day will encompass the process and procedures necessary for the successful execution of the Validator activities through the use of Marine Corps Compliance and Authorization Support Tool (MCCAST), DISA STIG Viewer, Assured Compliance Assessment Solution (ACAS) and other tools. Key points will include but are not limited to; roles and responsibilities, assessment requirements, validation procedures, risk scoring, Security Assessment Report (SAR) development, and POA&M initialization.

Speaker(s): Mr. Josh Ingraham (HQMC C4 A&A Branch Head); Mr. Naveed Mirza (HQMC C4 A&A Tech Lead)

DON Enterprise Software Licensing Q&A
Fri., 9:15 – 10:15 am

The DON ESL Team would like to have an open Q&A with USG/DON members to discuss current and future DON enterprise license agreements (ELA). The goal is to provide a forum and areas for breakout sessions with the project officer to discuss funding issues/concerns, contract structure, areas of improvement, and initial discussions for future ELAs.

Govt. Only / CAC Required for this Session.

Speaker(s): LtCol Clinger (DON ESL Team Lead)

USMC CCRI to CCORI Transition
Fri., 10:15 – 11:15 am

HQMC C4 Cybersecurity Division (CY) will provide an overview of the DOD Cybersecurity Inspection Program, as it shifts focus from compliance based inspections (CCRIs) to a program that incorporates cybersecurity compliance inspections, operational risk-to-mission evaluation, and mission assurance determination to gauge mission readiness of the DODIN. The overview will include current efforts and way ahead for Marine Corps CCORI program.

Speaker(s): Mr. Daniel Norton (HQMC C4 CY Assessments Branch Head)

RMF Inheritance from Navy Enterprise Networks (NMCI/ONE-Net)
Fri., 10:30 – 11:30 am

Just exactly how does one leverage the world's largest commercially operated network into an efficient inheritance vehicle for Navy and DoD information systems while not losing sight of the new demands of the Risk Management Framework (RMF)? Learn about the granularity of the Naval Enterprise Networks (NEN) inheritance process under RMF with the NMCI and ONE-Net ISSMs as they discuss what is required of their new process, explain new improvements over past processes and clarify roles and responsibilities under RMF. The discussion will cover not just the start-to-finish process currently executed, including required materials and explanation of their use, but also offer attendees a chance to learn more about inheritance under RMF.

Speaker(s): Sean Perryman, PMW 205, NMCI ISSM; Chico Hum, PMW 205, SSC Pacific ONE-Net ISSM