Email

DON IT Conference, West Coast 2022 - Defend Track

An informative recap of the DEFEND track speakers and topics

By Doug James - April-June 2022

The DON IT Conference, West Coast 2022 was a hybrid event with in-person and virtual components that took place Feb. 16-18. The virtual side of the conference was broadcast via Microsoft Teams. The in-person component was held at the San Diego Convention Center, in San Diego, California.

The purpose of the Department of the Navy IT conference is to share information about new and emerging IT policy and initiatives, including those that support statutory requirements, cybersecurity, privacy, and electromagnetic spectrum and to hear firsthand from DON IT Leadership and provide the opportunity for discussions between DON IT leaders and the DON IT community responsible for implementing policies and processes at the working level.

The DON IT conference sessions were organized along the three strategic objectives to Modernize, Innovate and Defend, and the two strategic assets of Data and Workforce. The sessions were led by subject matter experts and program managers translating policy decisions into decisive actions to transform the DON's internet technology platform to support cloud services, a zero-trust architecture, machine learning and artificial intelligence, emerging technologies, data-driven decisions and a digital workforce.

DEFEND Track

The DEFEND Track of the conference was kicked-off by DON Chief Information Officer (CIO) Aaron Weis. He spoke about the DON's efforts to design the network's user experience to allow the warfighter to orient on the situation rapidly. He highlighted the fact that we must provide properly credentialed Sailors and Marines access to information to fight from anywhere and the path forward to achieve this vision was through one, logical, software-defined network leveraging elastic compute infrastructures, identity management and modern software development.

Mr. Weis was followed up by DON Principle Cyber Advisor (PCA) Mr. Chris Cleary who touched the topic of "One Year Down"; which was a heartfelt discussion on what the future holds for cybersecurity, cyber resiliency and cyber warfighting.

Dr. Larry Totimeh provided on overview of the DON's Cybersecurity Strategy which incorporates Cyber Risk-to-Mission (CRTM) analysis into design, engineering, and operational processes for Platform Information Technology (PIT) and Operational Technology (OT).

Mr. Danny Cain from the DON CIO touched on the subject of "Why Does Privacy Matter?" Mr. Cain outlined that the DON is working hard to modernize our networks and systems leveraging emerging technologies. He also stated that during this change, the DON must ensure they stay vigilant to protect our data wherever it resides.

The NAVFAC Cyber Planning and Response Center (CPRC) held a working session with Mr. Michael Kilcoyne from Naval Facilities Engineering Systems Command (NAVFAC), Mr. Ryan Knight from NAVFAC, and Mr. Michael Barnhart from Mandiant. This DEFEND session provided a brief description of the CPRC, a threat intelligence brief and a description of the capabilities being built by NAVFAC's CPRC.

Navy RMF Reform Risk Assessment Methodology and SE Integration was briefed by Ms. Megan Cane from N2N6D6, Mr. Hank Osborne from NIWC Atlantic, Ms. Kama Stone from Fleet Cyber Command(FCC)/10th Fleet, along with Mr. Rob Bartnicki and Mr. Steve McPhillips, both from Naval Information Warfare Systems Command (NAVWAR). This session provided a deep dive into consistent cyber risk assessment methodology and integrating cybersecurity into system engineering and test and evaluation.

Mr. Sean Perryman from Program Executive Office (PEO) Digital provided an in-depth Inside Look at Navy Enterprise Networks Processes to Speed up RMF. This briefing provided a look inside of the specific RMF processes in use by the Navy Enterprise Networks, which enables them to update and maintain more changes at a faster pace despite the scale of the enterprise.

Ms. Renata Spinks from Headquarters, U.S. Marine Corps (HQMC) DC briefed on "What is Zero Trust and Why IT Matters?"; which provided an overview of the DON's Zero Trust approach which is a

Related CHIPS Articles

Marines in acquisition: Leveraging enlisted experience for battlefield success

Commander, U.S. Cyber Command rolls out new strategic priorities

Missed the 2023 DON IT Conference East?

Forging partnerships in the Americas: Naval leaders gather at SIANC S&T Conference

Pentagon cyber official provides progress update on Zero Trust Strategy Roadmap

Related DON CIO News

Missed the 2023 DON IT Conference East?

2023 DON IT Conference East Presentations Available

2023 DON IT Conference East Final Details and Virtual Links Now Available

DON 5G Newsletter – April 2023

DON CIO Bids "Fair Winds and Following Seas" in Departure Announcement

Related DON CIO Policy

DON Enterprise Service Designation for Naval Integrated Modeling Environment

Optimize the Information Environment for Cloud

Operations Security Awareness Month

FY 23 DON Information Superiority Vision Campaign Plan

Rapid Assess and Incorporate Software Engineering 2.0

and Why IT Matters?", which provided an overview of the DON's Zero Trust approach which is a

philosophical approach to security that the DON thinks is essential for every business, organization or entity that has a presence online. Ms. Spinks highlighted that fact that Zero Trust works on the assumption that you can't separate the "good guys" from the "bad guys" and that traditional approaches that focused on establishing a strong perimeter to keep the bad guys out no longer work.

Ms. Renata Spinks from HQMC DC and Ms. Clarice Kent from Defense Information Systems Agency (DISA) Cyber Readiness briefed on "A Threat Informed Approach to Risk Management Framework Implementation" which provided highlights of the DON's Cyber Ready efforts. They emphasized that fact that the DON currently has implemented Risk Management by way of incident response processes rather than threat intelligence, adherence to predefined standards and policies in security architecture and engineering practices, and compliance verification in the operational domain. Their briefing noted that the DON needs to refocus on evolving as an integrated cyber security organization structured to place threats at the forefront of strategic, tactical and operational practices.

Mr. Kevin Dulany, director of DOD CIO Cybersecurity Policy and Partnerships (DCIO-CS/P&P) and Ms. McKay Tolboe from DCIO-CS/P&P, provided updates on the DoD's Cybersecurity Programs and Reporting Scorecards. They shared insights about how the scorecards provide insight into status of activities meant to mitigate risk to our systems and networks.

Ms. Sharon Fitzsimmons from the Systems Engineering Transformation group and Mr. Richard Grabenstein, acting director of Naval Air Warfare Center Aircraft Division (NAWCAD) Cyber Warfare Department touched on Cybersecurity and MBSE: We Can Work It Out- Integrating Risk Management Framework and Cyber Survivability Risk Assessments using MBSE. They provided an overview of the integration of cybersecurity practices with Model Base Systems Engineering and the combined application to Risk Management Framework (RMF) and Cyber Risk Assessments.

Mr. Steve Pitcher from Joint Staff/J-6 spoke about Cyber Survivability Requirements for Acquisition - Going Beyond JCIDS. This discussion was on how the Joint Capabilities Integration and Development System (JCIDS), System Survivability KPP and the Cyber Survivability Endorsement (CSE) framework provides a shared understanding of the cybersecurity and cyber operational resilience levels required throughout a system's lifecycle.

Mr. Doug James is a cybersecurity expert and provides contractor support to the DON CIO Chief Information Security Officer (CISO) Directorate.

TAGS: CDIO: EA, CISO: Cybersecurity, CTO: Cloud, CTO: IT Modernization, Identity & Access, Cybersecurity, Digital Workplace/O365, Emerging Tech, DEVSECOPS, Infrastructure, NNE, Strategy, Workforce

CHIPS is an official U.S. Navy website sponsored by the Department of the Navy (DON) Chief Information Officer in partnership with the Naval Information Warfare Center (NIWC) Atlantic.

Online ISSN 2154-1779; Print ISSN 1047-9988
Hyperlink Disclaimer