

Briefing

Strategic Market Analysis

CDCA 2020 Report

**Lenny Long, DON Strategic Market,
Senior Director**



A TECH DATA COMPANY

CDCA 2020 Recap



The Charleston Defense Contractors Association (CDCA) Defense Summit is one of the largest defense-focused events on the East Coast, bringing together more than 1,000 government and industry leaders to spark ideas, innovation and solutions to technological challenges. Presentations, demonstrations and collaborative discussions include the full spectrum of defense technologies, with a focus on the areas of C5ISR, information warfare and cyber security.

Overview

The event explored topics including the 12 points of National Defense Strategy, rapid innovation, unmanned systems, Internet of Things (IoT), research & development and cyber hardening. With the latest in end-to-end IT enterprise technology, the Defense Summit is the place to be on the East Coast to educate, network and increase understanding of DoD, modernization solutions and improved support for the Warfighter.

The 13th annual CDCA Defense Summit theme was “Accelerate to Dominate Increasing the Speed of Warfighter Innovation” and kicked off December 10th with two technical training sessions focused on cloud computing. The first session featured Amazon Web Services (AWS) Technical Essentials and intro-

duced everyone to AWS products, services and common solutions. It provided the conference with fundamentals to become more proficient in identifying AWS services to make informed decisions about IT solutions based on your business requirements. The other training featured Microsoft Azure Fundamentals which introduced the principles of cloud computing. Attendees became familiar with how these principles have been implemented in Microsoft Azure. In addition, this course explained how to implement the core Azure infrastructure, consisting of virtual networks and storage. With this foundation, people learned how to create the most common Azure services, including Azure Virtual Machines, Web Apps and Azure SQL Database. The course concluded by describing features of Azure AD and methods of integrating it with on-premises Active Directory (AD).

Key Takeaways

CYBERSECURITY MATURITY MODEL CERTIFICATION REQUIREMENT



Key takeaways from the 13th annual CDCA Defense Summit focused on a few major topics and most notably the DoD's impending Cybersecurity Maturity Model Certification (CMMC) requirement. CMMC will be so impactful for everyone that wants to do business with the DoD that all contractors have cause for concern and especially among small businesses worried about the cost. But the Pentagon's made the case Wednesday that the move is necessary and, in some cases, will help small contractors.

"We need to lower the barriers. We need to speed up acquisition. But we also need to secure the defense industrial base," said Katie Arrington, chief information security officer for the assistant secretary for defense acquisition. "With 70-80 percent of our data living on contractors' networks, I don't have a choice but to worry about how they're doing it."

Defense contractors have been required to have a base level of cybersecurity on their systems through laws, policies and executive orders. However, those policies require vendors to self-certify—a method that is unreliable and, often, can put compliant businesses at a disadvantage. Under the new framework, all vendors doing business with the DoD will be required to be certified by a third-party assessor as fully compliant or be prohibited from being awarded a contract. The DoD is moving at a pace to have the compliance regime in place by mid-2020.

Arrington said that by codifying CMMC compliance, DoD can—and will, by her assertion—consider it as an allowable cost of having the required certification level. By Arrington's assessment, this will not only ensure that defense contractors have a base level of cybersecurity, but also that they are getting paid a reasonable amount to maintain that security.

The Pentagon released the seventh draft version of the standards Wednesday, paired down from 380 practices and 85 capabilities to just 173 and 43, respectively. The result is a five-tiered system, with the first three mapping to standards most of the defense industrial base should already be familiar with. According to Arrington, a Level 1 certification maps to Federal Acquisition Regulation 52.204-21—the basic cybersecurity standard for federal contractors—while Level 2 and 3 maps to National Institute of Standards and Technology (NIST) 171 and 171.b, respectively. She added that the department plans to acknowledge existing certifications for those standards, so vendors don't have to recertify.

The accreditation body that will govern the program in being set up now, Arrington said, with the full process being turned over by January. Once the memorandum of understanding is in place, the body will begin to accredit third-party assessment organizations, or C3PAOs, that will do the certification and continuous monitoring work. Arrington noted those C3PAOs will be limited to auditing work and will not be companies that provide cybersecurity solutions. From there, Arrington said the first solicitations to include CMMC requirements will be posted by June or July. For vendors that think the cost of compliance will be prohibitive, Arrington says, "Good riddance."

"Companies that say, 'I'll never get certified, I don't want to, this is too high of a bar to reach to work with the Department of Defense. It's already cumbersome enough to work there.' Here's my thing: I love ya, but good riddance," Arrington said. "We don't want to lose you. The companies that don't want to acquiesce, I don't want them to go. But they have a business decision to make."

That said, Arrington's goal will be to keep costs to a minimum. "If it costs you more than a few thousand dollars to get certified at CMMC Level 1, I have failed." She also noted the program will have Title 3 author-

CDCA 2020 Recap



“We need to lower the barriers. We need to speed up acquisition. But we also need to secure the defense industrial base. With 70-80 percent of our data living on contractors’ networks, I don’t have a choice but to worry about how they’re doing it.”

-Katie Arrington, Chief Information Security Officer for the Assistant Secretary for Defense Acquisition

ity to provide some funding assistance, similar to when the DoD mandated the shift from the Defense Information Assurance Certification and Accreditation Process (DICAP) to the Risk Management Framework. Once the CMMC process reaches a level of stability, Arrington said her next effort—CMMC 2—will focus on the products vendors use to secure their systems.

NAVALX PALMETTO TECH BRIDGE

NavalX announced the Palmetto Tech Bridge that is intended to offer a continuing evolution of Naval Information Warfare Center (NIWC) Atlantic’s engagement with leading academic research institutions, world-class industry partners, renowned federal labs and forward-thinking state organizations. With the utilization of diverse, off-base facilities across South Carolina, the Palmetto Tech Bridge serves to encour-



age creative and innovative research, host collaborative workshops, and sponsor unique problem-solving events. Drawing on the talents from across South Carolina industry and academia, NIWC Atlantic will focus and facilitate this considerable innovative force on developing dual-use solutions to meet both national defense needs and enhance the region’s economic strength with innovative commercial products.

With strong partnership from the Office of Naval Research, NavalX Tech Bridges will connect, reinforce, and sustain acceleration ecosystems in off-base locations across the U.S. Department of the Navy (DON). The Tech Bridges will partner with startups, academia, corporations, small businesses, non-profits, private capital and government entities. In this way, NavalX builds sustainable networks for collaboration and accelerates problem solving. NavalX

works with partners to support collision spaces and generate dual-use solutions. These spaces will lower barriers that traditionally hamper external collaboration. The Tech Bridges are strategically positioned in Newport, RI, Crane, IN, Keyport, WA, Orlando, FL, San Diego, CA and Charleston, SC. For more information can be found at <https://www.secnav.navy.mil/agility/Pages/techbridges.aspx>

INFORMATION WARFARE RESEARCH PROJECTS

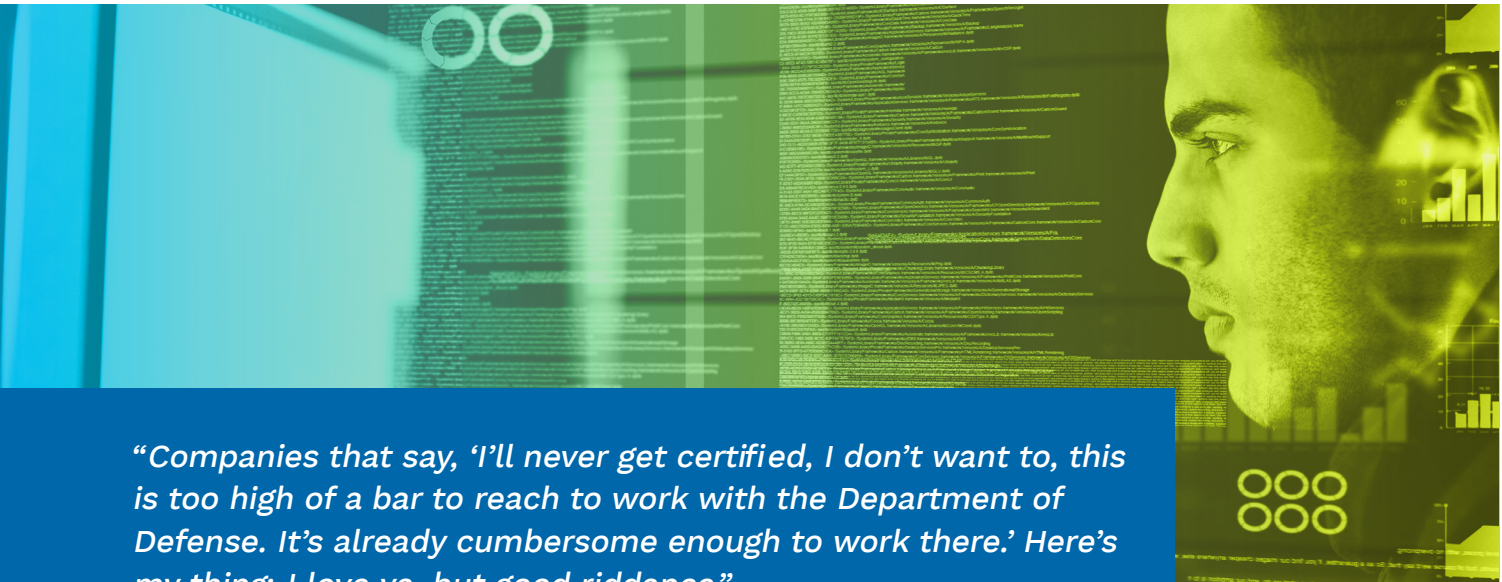


Information Warfare Research Projects (IWRP) continues to be the contracting method of choice for advancing naval information warfare through rapid prototyping on a global scale. IWRP uses an alternative acquisition method called Other Transaction Authority (OTA) to greatly increase speed to award, reduce barriers to competition, increase access to innovative, commercial solutions and leverage advanced commercial technologies. Specific technology focus areas include:

- **Cyber Warfare:** Defensive and offensive technologies used to operate, configure, control, secure, maintain, and restore the infrastructures and resident data, including Internet Protocol (IP) networks, radio frequency (RF) networks, computer systems, embedded processors and controllers, process, and physical systems
- **Data Science/Analytics Technologies:** Technologies and technical processes enabling and enhancing the reliability, assurance, integration, interoperability, delivery, value of data and information assets. Data may be derived from diverse verticals [Combat, Intelligence, Surveillance & Reconnaissance (ISR), Electromagnetic Maneuver Warfare (EMW), Cyber, etc.] includes specialized technology capabilities that capture, ingest, persist, analyze, and visualize data and help our customers perceive, visualize and make decisions about their environment

- **Assured Communications:** Technologies providing robust, protected, resilient, and reliable information infrastructure undergirding the DON's overall information environment and allowing uninterrupted worldwide communication between deployed units and forces ashore. Technologies will include application in multiple transmission spectrums, including RF, millimeter wave, optical; networking technologies such as application awareness, resilient routing, and attack tolerance
- **Cloud Computing:** On-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS); private cloud, community cloud, public cloud, hybrid cloud
- **Enterprise Resource Tools:** Collection of computer programs with common business applications, tools for modeling, and development tools for building organization unique applications focused on solving enterprise-wide problems to improve the enterprise's productivity and efficiency
- **Collaboration and Social Networking:** Collaboration/social interaction for sharing design patterns and best practices into our engineering culture, allowing social interaction to be aggregated, assessed, and pushed back into the supporting systems as structured data that can be used to support better decision-making.
- **Autonomy:** Techniques applicable to systems, incorporating assistants and decision support systems implemented through artificial intelligence and machine learning enabling them to adapt their actions to changes in their mission and operating environment without the intervention of a human operator
- **IoT Embedded Systems:** Various connected sensors that can be accessed or controlled remotely

CDCA 2020 Recap



“Companies that say, ‘I’ll never get certified, I don’t want to, this is too high of a bar to reach to work with the Department of Defense. It’s already cumbersome enough to work there.’ Here’s my thing: I love ya, but good riddance.”

-Katie Arrington, Chief Information Security Officer for the Assistant Secretary for Defense Acquisition

across an existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems resulting in improved efficiency, accuracy, and economic benefit in addition to reduced human intervention; encompasses computer systems that performing a particular function within a larger system without direct human interactions

- Mobility: Includes the wireless technology and infrastructure to connect and authenticate to the enterprise while enforcing enterprise specific security policies on mobile devices to access to enterprise data
- Model Based Systems Engineering (MBSE): Technologies used to support the development, management, and application of virtual constructs of varying fidelity across the spectrum of systems

engineering activities; including operational capability functions, system requirements, design, analysis, verification, validation, operations, and maintenance activities

- On-Demand Manufacturing: Additive and/ or traditional manufacturing methods such as stereo lithography (SLA), selective laser sintering (SLS), direct metal printing (DMP), color jet printing (CJP), fused deposition modeling (FDM), and 3D additive manufacturing (AM)
- Assured Command and Control (AC2): Capability to exercise authority and direction when access to and use of critical information, systems and services are denied, degraded or exploited. AC2 is enabled by essential network and data link services across secured segments of the electromagnetic spectrum to transport, share, store,

protect and disseminate critical mission/combat information.

- Integrated Fires (IF): Capability to fully employ integrated information in warfare by expanding the use of advanced electronic warfare and offensive cyber effects to complement existing and planned air, surface and subsurface kinetic weapons.
- Battlespace Awareness (BA): Advanced means to rapidly sense, collect, process, analyze and evaluate information content to exploit the warfighting operating environment. BA uses AC2 and IF elements to provide the characteristics and conditions to understand the operating environment. BA is aided by passive discrimination, identification and tracking of objects, persistent sensing and real-time/multi-spectral awareness, and cyber situational awareness within the operating environment.

For more information go to <https://www.theiwrp.org>.

DEVSECOPS

Finally, the show concluded with a technical discussion



about DevSecOps Moderated by Kathryn Murphy, senior scientific technical manager for software engineering at NIWC Atlantic and Panelist: Mr. Edmond Kuqo, NIWC Atlantic, Mr. Jason Anderson, NIWC Atlantic, Ms. Delores Washburn, chief engineer, NIWC Pacific, Mr. Steve Fraile, expeditionary intelligence technology improvement, innovation, & quick reaction capability IPT lead. DevSecOps is DoD's cultural revolution and is defined as the continuous and secure deployment of software to the Warfighter.

DevSecOps is an organizational software engineering culture and practice that aims at unifying software development, security and operations. The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software

lifecycle: plan, develop, build, test, release, deliver, deploy, operate and monitor. In DevSecOps, testing and security are shifted to the left through automated unit, functional, integration, and security testing - this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously.

The DoD Enterprise DevSecOps reference design leverages a set of hardened DevSecOps tools and deployment templates that enable DevSecOps teams to select the appropriate template for the program application capability to be developed. For example, these templates will be specialized around a specific programming language or around different types of capabilities such as web application, transactional, big data, or artificial intelligence (AI) capabilities. A program selects a DevSecOps template and toolset; the program then uses these to instantiate a DevSecOps software factory and the associated pipelines that enable continuous integration and continuous delivery (CI/CD) of the mission application.

The Navy's new Combat to Connect in 24 Hours (C2C24) is an ambitious program that has the potential to change naval warfare as we know it. The program is designed to improve operational efficiency by automating the Navy's risk management framework (RMF) efforts; providing sailors with near real-time access to critical data; and accelerating the Navy's ability to deploy new applications in 24 hours rather than the typical 18 months. Most importantly, C2C24 is using open source technologies and a unique cloud infrastructure to reduce the network attack surface and vulnerabilities. The Navy is standardizing its network infrastructure and data on open source code, and using a combination of shore-based commercial cloud and on-ship "micro cloud" for information access and sharing.

Are you attending AFECA West 2020?
Visit us at booth #1821.



For more information, contact
your DLT Sales representative or
email sales@dlt.com to schedule
time with Lenny Long, Senior
Director, DON Strategic Market.

DLT
A TECH DATA COMPANY