Warfighter Seminars Out-Brief

May 3, 2023, 2:30 p.m.

2023 Warfighter Seminars Highlights

Discussed two (2) relevant current and future Joint Engineer Issues

Conducted seven (7) total hours of discussions over two (2) days

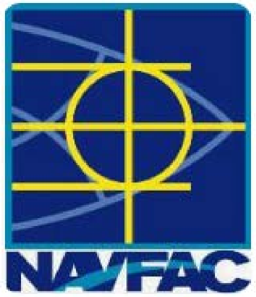
258 JETC attendees participated in the Seminar Working Sessions

Thirty-Seven (37) Seminar Moderators, Leaders, and Panelists from:

- 16 US Government Organizations and Agencies
- 21 Industry Organizations

Next Step: Brief to Joint Staff Engineers in June 2023 for possible inclusion of findings and recommendation into the JOEB Annual Work Plan, Joint Logistics Estimate, Joint Assessments or other mechanisms.

Warfighter Seminar #1 - Participating Organizations



Warfighter Seminar #2 - Participating Organizations

1898 & CO℠
PART OF BURNS & McDONNELL

HDR

RMC
ASSURING TOMORROW

VISIONEERIT

ALETA
Technologies

NAVFAC

Michael Baker
INTERNATIONAL

Booz | Allen | Hamilton®

DEPARTMENT OF THE AIR FORCE
UNITED STATES OF AMERICA
MCMXLVII

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

UNITED STATES NORTHERN COMMAND

UNITED STATES STRATEGIC COMMAND

UNITED STATES CYBER COMMAND

TETRA TECH

The PMC Group LLC
Engineering a better tomorrow today

LUTRON®

PARSONS

US INDO-PACIFIC COMMAND

UNITED STATES SPACE COMMAND

US Army Corps of Engineers®

UNITED STATES CENTRAL COMMAND

Chinook

Salas O'Brien

NOZOMI
NETWORKS

CLAROTY

Warfighter Seminar #1

Adaptability of Multiple Award Contingency Contracts to Current Global Threats

Seminar #1: Adaptability of Multiple Award Contingency Contracts to Current Global Threats

Seminar Moderator: Rear Adm. Chuck Kubic, P.E., F.SAME, USN (Ret.), Kubic Engineer Group
Seminar Co-Leader: Col. Matthew Beverly, USAF, PACAF Civil Engineer Consultant
Seminar Co-Leader: Lt. Col. Rick Sloop, USAF (Ret.), Fluor Mission

Panelists

Government
Seth Cutler, P.E., OASD (EI&E)
Capt. Chris Coggins, CEC, USN, INDOPACOM J44
Lt. Col. Seth M. Lorimer, USAF, INDOPACOM J442
Capt. William F. Boudra, CEC, USN (Ret.), JPMO
Renee Comfort, GCCMAC/GSCMAC
Col Kevin Golinghorst, USA, USACE
Cdr Anant Patel, CEC, USN (Ret.), NAVFAC Southeast
James Garred, 772 ESS/PKD
Robert Mellerski, AFCEC/CXA
Dominic Sparacio, P.E., Deputy Director, Expeditionary Directorate, NAVFAC

Industry
Rich Belmonte, V2X
RADM Mike Shelton, USN (Ret.), Planate
Col. Mike Hass, USA (Ret.), IAP
Col. Robert Nicholson, USA (Ret.), KBR
David Bluestein, ECC

Seminar #1: Adaptability of Multiple Award Contingency Contracts to Current Global Threats

Description: Multiple Award Contingency Contracts, such as LOGCAP, AFCAP, GCSMAC and GCCMAC, have been in place for nearly three decades and have served as force multipliers during a wide range of global contingencies to include combat operations and natural disasters. Also, over the decades the USA has entered multiple “Treaties in Force” and Country Agreements with other nations which have direct impact on contract risk, cost, and schedule when urgent requirements arise.

Now and in the future, threats in INDOPACOM will likely stress these “workhorse contracts” and those dedicated “battlefield contractors” who must execute complex taskings for deliberate and contingency construction and logistics in numerous countries each with their own governing relationship with the USA.

Looking ahead, it is time to examine strengths and weaknesses of these critical contract vehicles and associated foreign nation agreements; and, to identify necessary structural and process adjustments to ensure speedy, effective, and cost-efficient response to evermore challenging combined military and civilian Engineer Operations in the remote and increasingly dangerous Western Pacific and elsewhere around the globe.

Seminar #1: Adaptability of Multiple Award Contingency Contracts to Current Global Threats

Learning Objectives:

- Understand the capabilities of the current Contingency Contracts and the Contractors who execute contingency Task Orders.
- Understand the types of Treaties in Force and Country Agreements and the basic protections they may or may not provide.
- Learn the contracting and financial requirements which regulate the award and administration of Contingency Contracts.
- Analyze the effectiveness of the current competitive contract/task order award process and its responsiveness to military operations.
- Discuss the need to adjust contingency contract terms and conditions to balance operational, security, logistics and host nation risks based upon a Hypothetical Scenario.
- Recommend how best to incorporate the requirements for "Contingency Contractors on the Battlefield" into formal OPLAN Annexes.

Seminar #1: Adaptability of Multiple Award Contingency Contracts to Current Global Threats

Findings and Recommendations

Finding #1: Multiple contracting agencies in a single area create unintended consequences (i.e., contractor fratricide)

Recommendation: Assign contracting agencies by region, island, etc.

Finding #2: Prior to Task Order award, there is little to no time for “Contingency” MATOC Contractors to plan or respond to requirements.

Recommendation: Conduct early planning, training, and/or exercises between operational contracting agencies and “Contingency” MATOC Contractors

Finding #3: The moratorium on use of any type of contract other than firm-fixed price for construction creates an unbalanced and unacceptable risk within the INDOPACOM region (or any other logistically challenged region)

Recommendation: Develop a White Paper by SAME JECO COI justifying and supporting the waiver of this moratorium in INDOPACOM to facilitate executing construction with cost reimbursable contracts.

Seminar #1: Adaptability of Multiple Award Contingency Contracts to Current Global Threats

Findings and Recommendations

Finding #4: Construction and service activities in INDOPACOM (or any other remote area) are really more of a logistics effort than a construction or service effort.

Recommendation: Use hybrid contracts to break out logistics as a cost reimbursable service while executing the actual construction as firm fixed price.

Finding #5: Contract administration and management should be accomplished on location (i.e., not as a reach-back effort through multiple time zones)

Recommendation: On-site leadership should be trained and given limited contracting authority necessary to effect timely actions.

Finding #6: There exist other contract vehicles outside of the Contingency MATOCs (LOGCAP, AFCAP, GCSMAC and GCCMAC) that could meet service requirements for construction, repairs, commodities and/or services.

Recommendation: Establish a Contracting Coordination Board within INDOPACOM similar to the European Contracting Coordination Board (ECCB) to review all existing contracts for applicability to INDOPACOM requirements and to identify potential modifications which could improve current Contingency MATOCs.

Seminar #1: Adaptability of Multiple Award Contingency Contracts to Current Global Threats

Findings and Recommendations

Finding #7: Presently, FFP contracts are placing substantially all risk on contractors to include potential penalties.

Recommendation: Review and adjust FFP terms and conditions to achieve a more balanced risk share.

Finding #8: INDOPACOM AOR has inadequate labor resources (USN / TCN) to meet its projected requirements.

Recommendation: Implement early contractor involvement in contingency project planning to address mobilization of labor from outside INDOPACOM.

Finding #9: Time/cost/risk for construction within INDOPACOM is driven by logistics.

Recommendation: Implement early contractor involvement in contingency project planning to address logistics from within and from outside the INDOPACOM AOR; and, identify potential logistics support by military assets (sea and air).

Finding #10: Treatment of contractors in support of the military is inconsistent across INDOPACOM Host Nations.

Recommendation: Initiate coordination between DoD and DoS to clarify status of contractors in support of the military and to gain approval to treat deployed U.S. contractors similarly to U.S. military personnel.

Senior Leader & Attendee Comments

Warfighter Seminar #2

Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Seminar Moderator: Lucian Niemeyer, CEO Building Cyber Security
Seminar Co-Leader: Brian May, Senior Vice President - Air Force Market Lead, Michael Baker International
Seminar Co-Leader: Daryl Haegley, SL, GICSP,OCP Department of the Air Force Technical Director, DAF Control Systems Cyber Resiliency
Seminar Co-Leader: David A. Forbes, Principal, Booz | Allen | Hamilton

Panelists

Government

HQ NAVFAC
US Army Corps of Engineers
US SPACE COMMAND
US NORTHERN COMMAND
US INDOPACIFIC COMMAND

US CENTRAL COMMAND
NFEXWG
US STRATCOM
NSA
US CYBERCOM

Industry

Aleta Technologies
Chinook Systems
Claroty
HDR
Lutron
Nozomi Networks
1898

Salas O’Brien
TetraTech
RMC
PMC Group
VisioneerIT
Parsons

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Description: National Defense Strategies have noted that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. Increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.

Using a designed scenario specifically targeting a mission essential building system at a notional military asset to deny a national security mission, the panel will discuss the processes and protocols needed by military engineers to meet federal guidance to quickly identify, protect, detect, respond, and recover from a cyber-physical attack. The scenario will highlight the operational technology mapping requirements for national security critical assets required by Congress via Sec 1505 of the National Security Authorization Act for Fiscal Year 2022.

The discussion will focus on roles and responsibilities of building systems military, industry, and contractor stakeholders to mitigate the risk and impact of a cyber attack, spanning from building design through continuous facility operations. The seminar will review and/or develop tactics, techniques, and procedures to immediately respond to and recover essential mission functions. The scenario includes input from building system manufacturers, supply chain specialists, facility designers, facility operators, and cyber security experts, providing engineers unique insights and a comprehensive understanding of the risks.

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Learning Objectives:

- Review processes to identify critical systems and cyber vulnerabilities within a risk management framework;
- Identify proactive measures to protect critical systems and mitigate risk of a cyber physical attack;
- Present methods to detect and confirm the origin and method of a cyber attack and damage assessment;
- Develop checklists and protocols to quickly isolate, respond and communicate progress to the incident;
- Assess options, probabilities and timing for the recovery missional essential system; and
- Identify programs to share information within the National Security command structure on the incident

Findings/RECOMMENDATIONS

- Facility teams must be trained to consider and recognize a cyber attack
- Responding to an OT cyber attack must consider an immediate threat to human safety
- Facility Engineers must review and practice TTPs with IT and network staffs
- Facility engineers must maintain inventories of smart building systems and FMC capabilities
- Installation IT teams must recognize and protect the OT on networks
- Facility engineers must provide clear guidance to manufacturers and maintainers on the configurations of digital components in building systems
- Facility engineers must be trained on established processes for cyber response
- Facility engineers must invest in protections and risk mitigation to OT systems

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Findings and Recommendations

Finding #1: Training and awareness is lacking on impact of cyber on OT systems

Recommendation: Cyber attack and defense needs to be integrated into curriculum for PME for engineering community. Initial training pipelines need to include this for both enlisted and officers. The EAG should formally invite their cyber counterparts to a shared forum.

Finding #2: Decision process at first response call center in order to deduce response time for decision makers

Recommendation: Incorporation of cyber as a potential root cause to drive troubleshooting questions and notification of Comms and CSSP in SOPs. Characterization of extent of impact.

Finding #3: A cyber attack on/to OT should be treated as kinetic attack

Recommendation: Establish Roles and Responsibilities for initial Damage Assessment and declaration of building safety and incident response, including Deny, Destroy, Degrade, Disrupt, Deceive

Finding #4: There is not enough information sharing across the Services

Recommendation: Establishment or restoration of a Cross-Service WG to innovate and standardize OT response, including use of MOSAICS, CRADA's and other similar frameworks.

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Findings and Recommendations

Finding #5: Annual Installation TTX and Facility TTX are not being implemented

Recommendation: Incorporate Cyber Evaluations into formal Mission Readiness Inspections and reinforce the necessity for installation TTXs to include all installation support functions, (i.e. PA, IT/Comms, Contracting), within an installation response team.

Finding #6: MILCON and Facilities Acquisition contracts are not currently spec'd with OT Cyber and an RMF ATO

Recommendation: Amend the definition of a complete and usable facility to include an authority to operate for all systems.

Finding #7: Current direction, guidance, and policy for OT cybersecurity are not understood or implemented at installation levels

Recommendation: Train O&M teams and Project Management teams on OT Cyber threats and requirements.

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Findings and Recommendations

Finding #8: Concern that Installations don't have a full inventory of connected systems, current Full Mission Capable (FMC) baselines, Jump Kit Toolsets, and update procedures.

Recommendation: Emphasize the requirement to have these back-up systems for mission critical facilities.

Senior Leader & Attendee Comments

Q&A

- Jim Romasz, james.romasz@wsp.com