

WARFIGHTER SEMINARS 2024

Moderators:

- Richard E. Sloop, Jr., P.E., FLUOR | Mission Solutions
- Matthew Beverly, Colonel, USAF, Joint Task Force-National Capital Region Liaison to USNORTHCOM
- Lucian Niemeyer, F. SAME, Building Cyber Security

Warfighter Seminar #1

Employing Existing Authorities to “Set the Theater” for Current & Future Conflicts



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

Joint Engineer Contingency Operations (JECO) COI Warfighter Seminar #1

Employing Existing Authorities to “Set the Theater” for Current & Future Conflicts

Co-Moderators: Richard E. Sloop, Jr., P.E., JECO COI Chair
Matt Beverly, Colonel, USAF, JECO COI Vice Chair

Speakers:

- Linda Specht, Deputy Assistant Secretary for Security Agreements, Bureau of Political-Military Affairs, Department of State
- Cindy Readal, SES, Assistant Commander for Contracting, NAVFACSYSCOM
- CAPT John Beattie, P.E., CEC, US Pacific Fleet Deputy Fleet Civil Engineer
- Seth Cutler, P.E., Principal Director, Facilities Investment & Management, OASD(EI&E)
- Dominic Sparacio, P.E., Engineering Capabilities/Doctrine/Planning, Joint Staff J-4

Joint Engineer Contingency Operations (JECO) COI Warfighter Seminar #1

Employing Existing Authorities to “Set the Theater” for Current & Future Conflicts

PANALISTS

INDOPACOM:

EUCOM:

CENTCOM: COL Gary Law, Eng Div Chief

NORTHCOM:

SOUTHCOM: COL Jody Owens, J38

USSPACECOM: Mr. Chester Hahn J47

TRANSCOM:

SOCOM:

Joint Staff J4:

OSD:

NAVFAC Contracting:

AFICC Contracting:

AFCEC:

ISOA:

Industry Partners:

Mr. Dom Sparacio

Mr. Seth Cutler

Ms. Cindy Readal

Mr. Craig Mellerski

Mr. Bill Valenti

Mike Shelton

Fluor, ERC, KGR, V2X,
Tigerbrain, Vertex,

Agenda

Date	Start Time	End Time	Schedule Event	Lead
14-May-24	1030	1200	Warfighter Seminar In Brief	
	1030	1115	Seminar #1: Employing Existing Authorities to "Set the Theater" for Current and Future Conflicts	R. Sloop
	1115	1200	Seminar #2: Risk Assessment and Mission Recovery from a Cyber Physical System (CPS) Attack to an Operational Asset in a Forward Deployed Location	L. Niemeyer
	1200	1210	Transition to Breakout Rooms	
	1210	1230	Introductions	
	1230	1245	Review of 2023 Warfighter Findings and Recommendations	Rick Sloop
	1245	1300	Problem Statement and Objectives / Review of Capital Week IGE Risk	Rick Sloop
	1300	1500	Open for Other Sessions	
	1500	1545	Overview of "Campaigning" Construction Requirements	Dom Sparacio
	1545	1630	Contracting Authority	SES Cindy Readal
15-May-24	1630	1730	Department of State Treaties in Force Negotiations	DAS Linda Specht
	1030	1115	Ability / Limitations of Current Construction Authorities	Seth Cutler
	1115	1200	NAVFAC Wartime Acquisition Response Planning (WARP) Exercise	CAPT Beattie
	1200	1230	Solutioning Discussion	Col Matt Beverly
	1230	1300	Review of Due Outs and Actions	Rick Sloop
	1300	1400	Seminar Lead(s) Finalize Outbrief	R Sloop / M Beverly / D Sparacio
	1430	1500	Warfighter Seminar #1 Outbrief and Senior Leader Feedback	Rick Sloop
1500	1530	Warfighter Seminar #2 Outbrief and Senior Leader Feedback	L Niemeyer	

Review of 2023 JETC Warfighter Seminar Findings and Recommendations



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

JETC 2023 Warfighter

“Adaptability of Multiple Award Contingency Contracts to Current Global Threats”

Finding	Recommendation	Action
#1 Multiple Contracting Agencies in a single area create unintended Consequences (i.e. Contractor Fratricide)	Assign Contracting Agency by region, island, etc.	None - Open
#2 Prior to T.O. Award, there is little to no time for “Contingency” MATOC Contractors to plan or respond to requirements	Conduct early planning, training and/or exercises between operational contracting agencies and “Contingency” MATOC Contractors	GCSMAC Wartime Acquisition Response Planning (WARP) Exercise April 2024
#3 Moratorium on use of any type of contract other than firm-fixed price for MILCON construction creates an unbalanced and unacceptable risk within the INDOPACOM region (or any other logistically challenged region)	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	Parallel effort with Construction COI. Overcome by events with the issuance of 10 USC 2817, Authority for Certain Construction Projects in Friendly Foreign Countries. Awaiting OSD Guidance
#4 Construction and services activities in INDOPACOM (or any other remote areas) are really more of a logistics effort than a construction or service effort.	Use hybrid contracts to break out logistics as a cost reimbursable service while executing the actual construction as FFP	Hybrid Contract Concept presented during JECO IGE at Capital week with follow up at 2024 JETC.

JETC 2023 Warfighter

“Adaptability of Multiple Award Contingency Contracts to Current Global Threats”

Finding	Recommendation	Action
#5 Contract administration and management should be accomplished on location (i.e., not as a reach-back effort through multiple time zones)	On-site leadership should be trained and given limited contracting authority necessary to effect timely actions.	None – Open
#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.	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.	None - Open
#7 FFP contracts are placing substantially all risk on contractors to include potential penalties.	Review and adjust FFP terms and conditions to achieve a more balanced risk share.	Hybrid Contract Concept presented during JECO IGE at Capital week with follow up at 2024 JETC.
#8 INDOPACOM AOR has inadequate labor resources (USN / TCN) to meet its projected requirements.	Implement early contractor involvement in contingency project planning to address mobilization of labor from outside INDOPACOM.	GCSMAC Wartime Acquisition Response Planning (WARP) Exercise April 2024

JETC 2023 Warfighter

“Adaptability of Multiple Award Contingency Contracts to Current Global Threats”

Finding	Recommendation	Action
<p>#9 Time/cost/risk for construction within INDOPACOM is driven by logistics.</p>	<p>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).</p>	<p>GCSMAC Wartime Acquisition Response Planning (WARP) Exercise April 2024</p>
<p>#10 Treatment of contractors in support of the military is inconsistent across INDOPACOM Host Nations.</p>	<p>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.</p>	<p>JECO COI Hosted DAS Specht presentation on Treaties in Force, follow up support for 2024 JETC Warfighter Seminar</p>

Problem Statement and Objectives / Review of CapWeek IGE Summit



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

Why Are We Here?

- Support the National Defense Strategy – Transition from the VEO fight to Strategic Competition
- How do we achieve CCMD Warfighter Objectives using all available authorities, specifically:
 - Indo Pacific Posture (section 2810) – Expires 2029
 - “Certain Construction in Friendly Countries” (section 2817) - Enduring
- How do we achieve objectives in a high risk, contested and difficult logistical environment?
- How can we improve Industry-Government partnership to help achieve those objectives by fairly and equitably sharing risk?

Secretary of the Air Force Frank Kendall 2024 AFA Warfare Symposium

- “We have the most pacing challenge we have ever faced – China, China, China. Ladies and gentlemen, **we are out of time, we are out of time, we are out of time**”
- “The United States does not seek a conflict; we have every hope that one can be avoided. We are, however, **involved in a competition, an enduring competition that could turn into a conflict at any time.** We can no longer regard conflict as a distant possibility or futured problem that we might have to confront.”
- “Our job, our fundamental mission – the reason we exist – is so we can be ready now and always. **The name of the game is deterrence. But deterrence rests on strength and the will to use it**”

Problem Statement

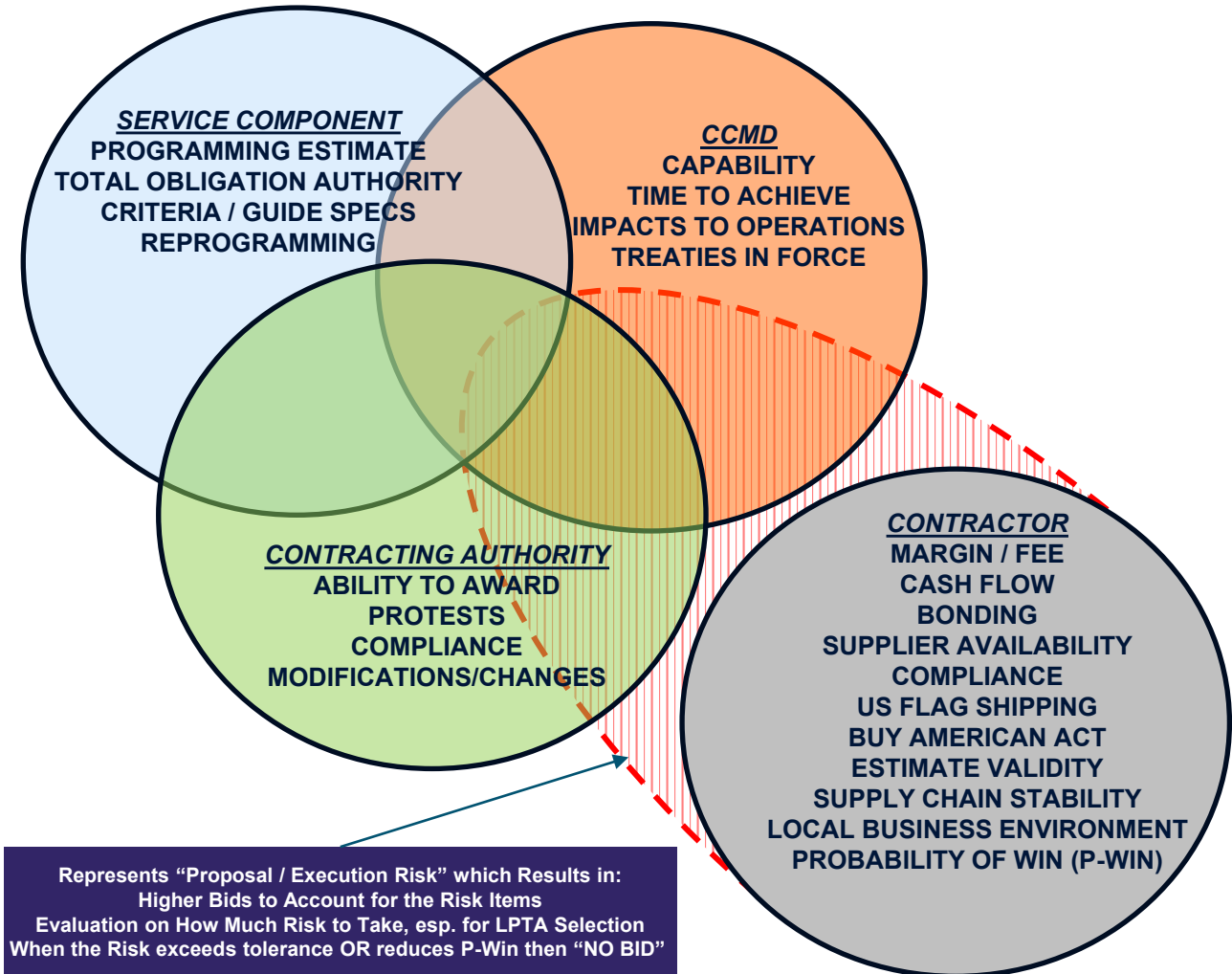
Four Main Players

- CCMD: The “need” / requirement
- COMPONENT: The money, specs and management
- CONTRACTING: The Authority
- CONTRACTOR: The “How” it gets done

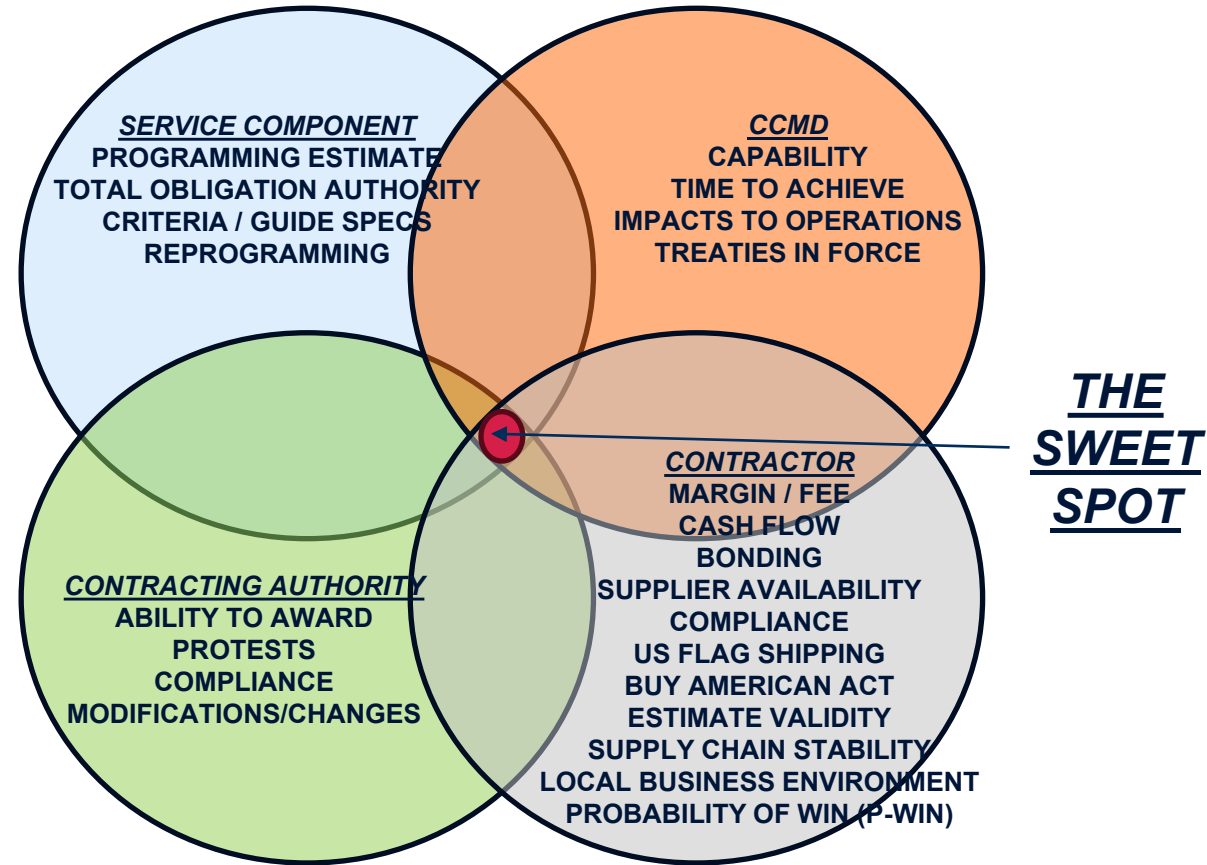
Each Have its own “Risk Bubble” which expands and contracts, depending on:

- Contract Type (FFP – CR)
- Penalty Clauses (LD’s, etc)
- Exception Clauses (EPA, etc)
- Funds Availability (to pay & to finance)
- Permissibility (Military v. Business)

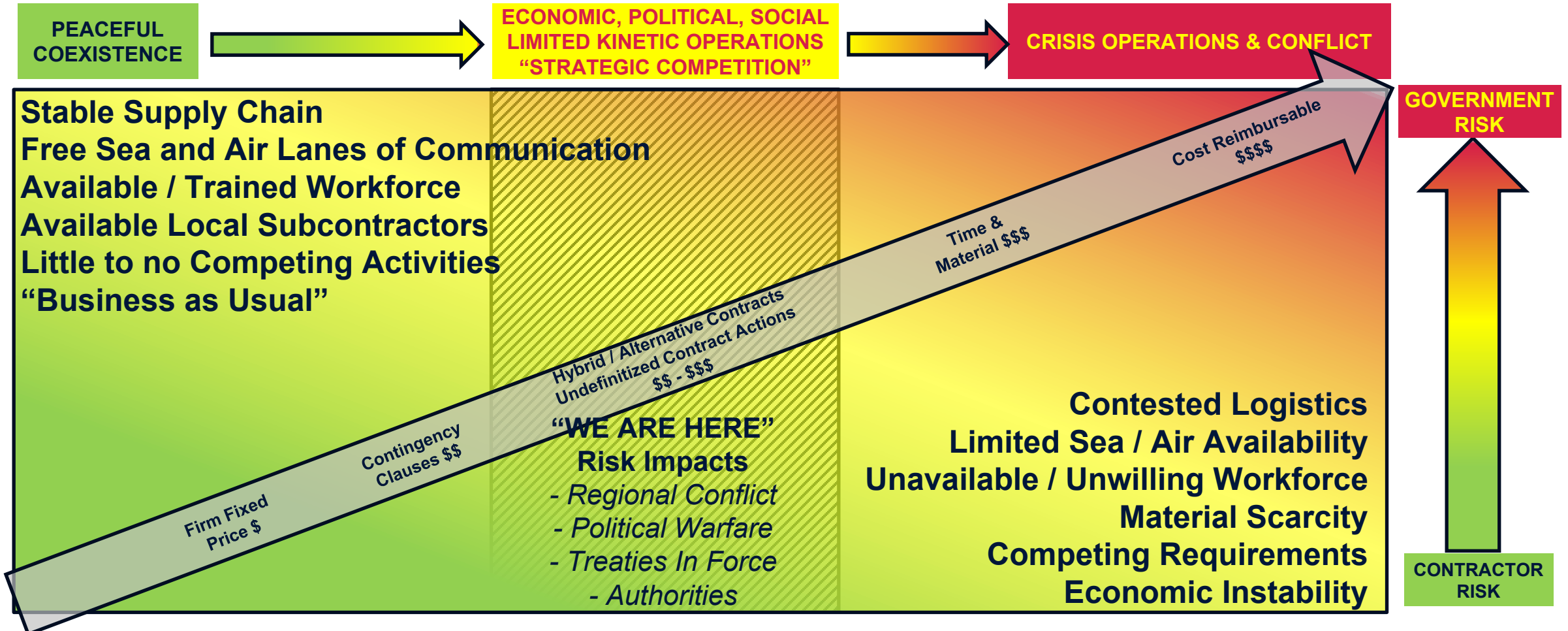
Under Current Acquisition process, the Contractor must either “go outside” their risk profile to get into the Government’s Risk Profile OR choose the “NO BID” Option



Here's Where We Want to Be



Where are we Now on the Risk Scale?



Capital Week IGE - Session Results / Output

Additional Risks	Challenges/Barriers	Solutions / Opportunities
CCMD: Ability to complete and operationalize fixed and expeditionary sites within the timeline established.	Ability to modify existing contracts to match the warfighter need	Use Existing Authorizations – Expand use of existing clauses to additional elements; Leverage Changes Clauses
Component: Ability to provide O&M after sites are established and available for use.	USG, Contractor and Local National Objectives - when does compliance become a USG to HN negotiation?	Engage Contractors early via planning efforts (e.g. planning task orders – EXAMPLE: NAVFAC WARP
Component: Balance between operational need and existing standards / specifications	US Labor Market is highly competitive; use of 3rd country nationals may be limited by HN law; USG “cleared” contractor personnel	Implement Aspects of other Contract Vehicles that help manage risk (e.g. GSA OASIS)
Contracting / Contractor: Potential for corruption without strong contractual language and management.	Internal Government tendency to be conservative regarding alternative acquisition methods	Use of DLA for Materials in Theater as Government Furnished Materials (GFM)
CCMD/Component: Contractors not prepared for a Classified Environment.	Accountability in an expeditionary environment using subK’s without adequate cost accounting, estimating or procurement systems.	More Acquisition Community involvement during the planning stage.
Component: Continuing Resolutions impact ability to solicit, award and fund requirements.	Existing Congressional Language and Federal Acquisition Regulations limit ability to “hybridize” contracts	Contractor Propose a schedule instead of dictating a mobilization or FOC Date (Use as a Best Value Criteria).
Contractor/Component: Unforeseen site conditions (e.g. UXOs, cultural sites, etc.)	Difference in Risk tolerance and mitigation approaches between Public and Private contractors.	Issue Draft RFP/PWS along with Acquisition Schedule as early as practical (even if the PWS is not 100%)
CCMD/Component/Contractor: “Smokeless War” where peer adversaries disrupting political, economic & social environments	Undefinitized Contract Obligations (UCO) viewed as “bait and switch” where fee and cost allowability are negotiated later	“Co-Creation” methodology to develop PWS and RFP, involving CCMD, Component, Contracting and Contractor.
Permissibility of the business environment for Contractors Accompanying the Force	Inherent difference between “partnering” and the actual contract language which drives an owner-vendor relationship.	Reduce or remove bonding requirements for expeditionary or contingency requirements; Limit or Remove LDs
Component / Contracting: Use of Artificial Intelligence (AI) in the development of proposals	Accounting for different “Colors of Money” when execution a hybrid contract	Use of Incentive or Award Fee structures.
Component/Contracting/Contractor: Auditor (DCAA / DCMA) activities for cost reimbursable contracts	Use of “Best Value” award criteria when the RFP does not identify what the USG considers a “Best Value”	Use of Past Performance as a Best Value selection criteria. Expand use of Other Transactional Authorities (OTA) Leverage the Changes Clause.
	Inconsistency of the CPAR process	Implement the Integrated Design And Construction process, where applicable.
	Availability of trained staff to execute and manage alternative or cost type contracts (both Government and Contractor)	

Warfighter Seminar #1 - Objective

- Identify Actionable Recommendations that:
 - Matches Requirements with the Appropriate Authorities
 - Help Navigate the Maze of Law, Regulations, and Treaties to mitigate Risk
 - Establishes fair and equitable Risk Profiles between the Government and the Industrial Base

Leadership

Inputs / Comments / Recommendations



Repair Pavements, Ascension Auxillary Airfield



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL)



[#SAMEJETC24](https://www.linkedin.com/company/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.instagram.com/SOCIETY_OF_AMERICAN_MILITARY_ENGINEERS)

Warfighter Seminar #2: Cyber/Physical Attack to an Operational Asset in a Forward Deployed Location



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

JETC 2024 Warfighter Training Session

Seminar #2: Cyber/Physical Attack to an Operational Asset in a Forward Deployed Location

Lucian Niemeyer, F. SAME



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



@SAMENATIONAL



@SAME_NATIONAL | #SAMEJETC24



"SOCIETY OF AMERICAN MILITARY ENGINEERS"

2023 RECCOMEDATIONS

- **Facility teams** must be trained to consider and recognize a cyber attack
- An OT cyber attack **must be considered an immediate threat to human safety** until a damage assessment is completed
- Facility Engineers must **review and practice TTPs with IT and network staffs**
- Facility engineers must **maintain inventories of smart building systems** and Fully Mission Capable (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**

2024 THREAT ASSESSMENT OF THE U.S. INTELLEGENCE COMMUNITY

"**China** remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."

"PRC operations discovered by the U.S. private sector probably were **intended to pre-position cyber attacks against infrastructure in Guam** and to enable disrupting communications between the United States and Asia."

"If Beijing believed that a major conflict with the U.S. were imminent, it would consider **aggressive cyber operations against U.S. critical infrastructure and military assets**. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."



2024 THREAT ASSESSMENT OF THE U.S. INTELLEGENCE COMMUNITY

"Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war.

Moscow views **cyber disruptions as a foreign policy lever to shape other countries' decisions** and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets.

Russia maintains its ability to **target critical infrastructure, including underwater cables and industrial control systems**, in the United States as well as in allied and partner countries."



2024 THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

"Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied and partner networks and data.

Tehran's opportunistic approach to cyber attacks puts U.S. infrastructure at risk for being targeted, particularly as its previous attacks against Israeli targets show that Iran is willing to target countries with stronger cyber capabilities than itself.

Honorable Avril D. Haines Director of National Intelligence

HEARING TO RECEIVE TESTIMONY ON WORLDWIDE THREATS Thursday, May 2nd, 2024

US Senate Committee on Armed Services

RECENT ICS NEWS

- Iranian officials sanctioned by U.S. government over Aliquippa, Pennsylvania water facility hack (Feb 2024)
- Russian linked hacking group suspected of carrying out cyber attack on **Texas & Indiana** water facilities (Apr 2024)
- Iran linked to Israeli Real Estate Companies DDoS attacks (May 2024)

Feb 7, 2024 – **Joint Cybersecurity Advisory**



“The **People’s Republic of China (PRC)** state-sponsored cyber actors are seeking to pre-position themselves for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.”

“Confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in **Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors.**”

“**Critical infrastructure organizations** are urged to apply the mitigations in this advisory and to hunt for similar malicious activity.”

VOLT TYPHOON

Expert Testimony



FBI Director Chris Wray - “China’s hackers are positioning on American infrastructure in preparation to **wreak havoc and cause real-world harm to American citizens and communities**, if or when China decides the time has come to strike.. Let’s be clear: **Cyber threats to our critical infrastructure represent real world threats to our physical safety.**”



CISA Director Jen Easterly - “Imagine not one pipeline, but many pipelines disrupted and telecommunications going down so people can't use their cell phone. People start getting sick from polluted water. Trains get derailed. Air traffic and port control systems are malfunctioning,“



Chairman Mike Gallagher - We are no longer discussing hypotheticals – China’s action, “**is the cyberspace equivalent of placing bombs on American bridges, water treatment facilities, and power plants.** There is no economic benefit for these actions. There is no intelligence gathering rationale. **The sole purpose is to be ready to destroy American infrastructure,** which will inevitably result in mass American casualties.”

VOLT TYPHOON Attack Scenario

CCP/Russia forces conducting a joint blockade to cut off maritime and air traffic to force Taiwan's surrender.

CCP/Russia aligned units conducting a limited a coercive campaign, including computer network and cyber attacks against Taiwan's political, military and economic infrastructure.

USINDOPACOM/CC initiating Phase 1 Oplans

- **Strategic assets deployed on Anderson AFB**
- **DEFCON Charlie**
- **FPCON BRAVO**

VOLT TYPHOON Attack Scenario

THE TARGETS

HANGER 5

- 4,700m², climate controlled concrete aircraft maintenance hangar(s)
- 800 metric tons of reinforcing steel and over 50,000 yards of reinforced concrete
- Constructed in 2022 for \$134.3 million.
- Protective shelter for two (2) B-2 or B-21 aircraft and other tactical fighter aircraft in a pre-hostility posture



VOLT TYPHOON Attack Scenario

THE DELIVERY – Vector of Attack

- **Fire Suppression System**
 - High Expansion Foam (HEF) dispersion system
 - Wet Pipe Fire Extinguishing system
 - Heat detection system
 - Multispectral flame detection system
 - Fire alarm/mass notification system
 - GSA-REL Fire Suppression controllers



VOLT TYPHOON Attack Scenario

EFFECTS

- Release of over 17 ft. of HEF on both hangered aircraft and maintenance personnel
- Several personnel injured due during evacuation due to HEF inhibiting line of sight and partially suppressing sound
- First responder operations hampered
- Damage to critical aircraft and maintenance equipment



VOLT TYPHOON Attack Scenario

OPERATIONAL MISSION EFFECTS

1. **Injury** to maintenance personnel
 - **Disruption** of maintenance operations
 - **Disruption** of flight operations
2. Temporary **Disablement** of assets
 - **Degradation** of strategic targeting
 - **Disruption** of maintenance operations
 - **Disruption** of flight operations
3. Temporary **denial** of essential hardened facilities

Deceive

Degrade

Deny

Disrupt

Destroy

VOLT TYPHOON Attack Scenario

OPERATIONA MISSION EFFECTS

4. **Loss of confidence** by mission owners of other essential facilities
 - **Degradation** of local mission command
 - **Deception** of adversary's means, motives & capabilities
5. **Denial** of hardened protection for critical assets
6. **Degradation** of local commander's confidence in the safety systems within flightline facilities



WARFIGHTING SCENARIO TEAM

Moderator: Lucian Niemeyer, CEO, Building Cyber Security

Co-Leader: Brian May, Senior Vice President - Air Force Market Lead, Michael Baker International

Co-Leader: Daryl Haegley, SL, GICSP, OCP Department of the Air Force Technical Director, DAF Control Systems Cyber Resiliency

Facilitators:

Jason Hall, Booz | Allen | Hamilton

Mark McCoy, Booz | Allen | Hamilton

Stacey Shepard, Shepard Global Strategies



WARFIGHTING SCENARIO TEAM

PARTICIPANTS

Government

OSD NSA
HQ NAVFA
US CENTRAL COMMAND
US Army Corps of Engineers
NFEXWG
US SPACE COMMAND
US NORTHERN COMMAND

Industry

Johnson Controls
SEL
Nozomi Networks Aleta
Technologies
Salas O'Brien
Chinook Systems
TetraTech Claroty
RMC HDR
PMC Group
Parsons Veridify
Forescout



20
24

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL)



[#SAMEJETC24](https://www.linkedin.com/company/samejetc24) "SOCIETY OF AMERICAN MILITARY ENGINEERS"

Training Schedule

Tuesday, May 14 3:00 pm - 5:00 pm

- Intro of the team and learning objectives (10 minutes)
- Review of last year's recommendations (5 minutes)
- Introduction to the Cyber Threat for Federal Engineers (20 minutes)
- NSA Presentation on OT Binding Operational Directive (30 minutes)
- 2024 National Cyber Risk assessment and timing of Volt Typhoon (20 minutes)
- Review of National headlines since last year (10 minutes)
- Review of scenario and audience feedback (25 minutes)

Training Schedule

Day 2, Wednesday, May 15, 2024 10:30 am - 12:30

- Scenario Training and discussion (30 minutes)
- Resources and Capabilities (30 minutes)
- Preparation of Recommendation ((20 minutes)
- **Meeting of the Cyber IGE engineering training standardization team**

3:00pm-4:30pm – Outbrief to Senior Leaders (Osceola Ballroom B)

Please join us for the **Warfighter Breakout Sessions:**

“Set the Theater” - Osceola 4-6
Cyber/Physical Attack - Osceola 1-3

(Both Across the Hall)



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)