ARCTIC EDGE 26

C-UAS Academic Workshop and TTX

10-12 March, 2026

ARCTIC EDGE 26 C-UAS Academic Workshop and TTX, 10-12 March, 2026

Executive Summary

BLUF: From 10-12 March 2026, the Arctic Edge 26 Counter-UAS Academic Tabletop Exercise (TTX) convened over 70 academic researchers, U.S. government interagency, and DoW stakeholders to examine the challenges associated with detecting, understanding, and responding to unmanned aircraft system (UAS) threats in the Arctic operating environment.

SUMMARY: The Homeland Defense Institute (HDI), the Ted Stevens Center for Arctic Security Studies (TSC), and the University of Alaska Fairbanks (UAF) co-hosted this TTX in coordination with NORAD and U.S. Northern Command's exercise ARCTIC EDGE 26. The purpose was to explore how the United States and its partners can better detect and respond to UAS activity in the Arctic, where environmental conditions, large geographic distances, and fragmented authorities complicate homeland defense operations.

Day 1 (Arctic Operations Immersion): A field seminar exposed participants to Arctic infrastructure and environmental conditions (-40°F), providing a tactile understanding of permafrost and operational challenges.

Day 2 (UAS research and education): Observed laboratory work and discussed sensors and unmanned systems research to prepare for the TTX.

Day 3 (C-UAS TTX): Participated in dialogue with panels of UAS and Counter-UAS experts. UAF's Alaska Center for Unmanned Aircraft Systems Integration (ACUASI) developed a TTX to assess vulnerabilities and options for security against emerging UAS threats to military installations and critical infrastructure in Arctic conditions. NORAD and USNORTHCOM provided the following objectives:

- Objective 1 – Integrating Non-Traditional Sensors for Detection and Tracking
- Objective 2 – Operating With and Through Academia, State Assets, and Allied Partners as C-UAS Enablers
- Objective 3 – Accelerating Decision Advantage in the Counter-UAS Kill Chain

KEY FINDINGS:

Objective 1 – Integrating Non-Traditional Sensors for Detection and Tracking (Domain Awareness)

- Existing sensing infrastructure across Alaska and the Arctic could contribute to UAS detection, but remains unintegrated. Participants noted that Alaska already hosts a wide range of sensing systems, including environmental monitoring stations, seismic networks, maritime sensors, and academic research infrastructure. While these systems are not designed specifically for counter-UAS missions, they may be able to provide useful indicators of aerial activity if integrated into a broader sensing architecture.
- Environmental conditions in the Arctic significantly affect sensor performance. Extreme cold, ice accumulation, snow cover, and atmospheric inversions can degrade some sensing technologies while enhancing others. Participants emphasized the need for Arctic-specific testing of detection systems to inform research and development to better understand these effects and field advanced mitigation capabilities.

➢ **Recommendations to Improve Sensor Integration:**

- Map existing sensing infrastructure across the Arctic AOR, including academic and commercial networks.
- Conduct exercise experimentation and pilot programs for early to lates stage efforts aimed at integrating non-traditional sensors into domain awareness systems.
- Explore AI-enabled multi-sensor fusion to improve detection accuracy and algorithms to enable friend or foe identification.

Objective 2 – Operating With and Through Academia, State Assets, and Allied Partners as C-UAS Enablers

- Data sharing across government, academic, and commercial organizations remains inconsistent and fragmented. Participants identified legal, technical, and organizational barriers that limit the ability to share sensor data across agencies and institutions. Differences in data formats, privacy considerations, and institutional policies complicate efforts to build a unified operational picture.
- False alarms and data quality are a significant concern. As more sensing nodes are introduced, participants stressed the importance of filtering, validating, and prioritizing sensor inputs to avoid overwhelming operators with unreliable information. This will be exacerbated by a rising commercial sector use of autonomous systems in the Arctic.

- **Recommendations to Establish Data Standards and Sharing Frameworks to enhance information dominance:**
  - Develop standardized data formats for reporting UAS incidents.
  - Identify authorities and policy barriers that can enable the establishment of formal data-sharing agreements
  - Integrate relevant data streams into existing command-and-control and domain awareness systems.
  - Consider developing an Arctic FALCON PEAK experimentation to execute as part of ARCTIC EDGE.

Objective 3 – Accelerating Decision Advantage in the Counter-UAS Kill Chain

- The unique conditions in Alaska and the Arctic contribute to decision latency in the counter-UAS response chain**.** Participants observed that even when a drone is detected, delays associated with identifying the threat, confirming authorities, and coordinating responses can significantly reduce the effectiveness of defensive actions within the Arctic region. The speed of the attack in the scenarios and the uncertainty in what was happening led the teams to have limited communication across interagency.
- Authorities for counter-UAS mitigation can be fragmented across organizations. The legal authorities governing counter-UAS operations in the homeland are distributed across federal agencies, state, local, territorial, and tribal (FSLTT), which can complicate rapid response during time-sensitive incidents given the conditions and distance unique to the North American Arctic region.

- **Recommendations to Accelerate Decision Timelines:**
  - Develop AI enabled decision-support tools to help operators rapidly identify potential threats amidst increasing commercial and personal drone use.
  - Explore pre-delegated authorities for certain defensive actions across SLTT.
  - Design scenarios for exercises that specifically test response timelines and coordination procedures, in addition to training and analysis on identifying and respond to UAS incursions with potential infrastructure sabotage.

Cross-Cutting TTX Observations

- UAS threats alone created serious dilemmas for the homeland defense mission, but likely represent early indicators of broader adversary activity. Arctic conditions amplify the effects of infrastructure disruption, particularly in power systems, increasing the likelihood of cascading humanitarian and security crises. Participants noted that hostile drone activity could serve as reconnaissance or

shaping operations preceding more conventional attacks once first response is degraded.

- The proliferation of small UAS has revealed a new operational seam. Participants described the emergence of an "air littoral"—the low-altitude airspace below traditional air defense coverage where small drones operate. Framing the problem in this way helped identify how traditional airspace management fails to provide adequate security here.
- Passive and low-tech defenses likely play an important role in protecting infrastructure. Observations from recent conflicts suggest that relatively simple protective measures—such as hardened infrastructure, protective netting and barriers—may significantly reduce vulnerability to drone attacks.
- Payloads identification is important for C-UAS mitigation decisions. Other nefarious payloads such as explosives or fentanyl/drug delivery should be factored into the identification and mitigation decision process due to the potential consequences.

Recommendations for experimentation and mitigation via exercise ARCTIC EDGE:

- Integrate FIFA and Olympics lessons learned into ARCTIC EDGE 27C-UAS scenarios, objectives, and/or experiments.
- Reduce stovepipes of information across FSLTT, academia, and industry. Context from exercises makes it much easier to incorporate homeland defense mission solutions into research and SLTT exercises.
- Integrate and resource experts who have unique Arctic domain expertise and experience: Establish a consortium of researchers for ARCTIC EDGE to create a persistent presence of technical and Arctic specific expertise.
    - Enable tighter coupling with JIATF 401 and research organizations to combine C-UAS lessons learned with technical Arctic expertise.

CONCLUSION: Across all sessions, a consistent theme emerged: the challenge of countering UAS in the Arctic is not solely technological. While new sensing and mitigation capabilities are important, the most significant barriers lie in the integration of existing systems, the alignment of authorities, and the ability to make timely decisions in a complex and ambiguous environment. Improving data integration, clarifying authorities, and accelerating decision timelines offer the most immediate opportunities to enhance homeland defense over the next 12–24 months. The ARCTIC EDGE exercises series remains the ideal vehicle to incorporate emerging technology to advance Arctic capable force development as well develop Arctic war fighting standards.

EXSUM Drafted by: Wes Moerble/ TSC Arctic Operations Research Analyst / wesley.moerbe@us.af.mil
Reviewed by: Nicole Rumsey / TSC Associate Director for CCMD Programs / 719-554-4670
Larry Dobbs / Chief Engineer Homeland Defense Mission / JHU APL / 240-228-9731

Annex A: Summary of Proceedings

Day One – Arctic Environment, Capabilities, and Technology

The first day of the event focused on building a shared understanding of the Arctic operating environment and exposing participants to research and operational capabilities available in Alaska.

During the Welcome and Opening Remarks, speakers emphasized UAF's role as "America's Arctic University" and its commitment to supporting national defense priorities through long-term partnerships. These remarks framed the event as part of a broader effort to align academic research with Department of War mission requirements.

The Arctic Operating Environment and UAF Capabilities session, led by the Geophysical Institute, provided an overview of the physical and scientific characteristics of the Arctic. Participants were introduced to the Institute's operational capabilities, including seismic monitoring, volcanic observation, satellite tracking, and atmospheric research. This session highlighted that Alaska hosts a dense network of sensing infrastructure that could contribute to domain awareness, though it is not currently integrated into defense systems.

During the ACUASI Capabilities Briefing, participants examined the operational advantages of Alaska as a UAS test environment. The session emphasized the dual-use nature of unmanned systems and highlighted extensive flight testing conducted across the state. A key insight from this session was the complexity of counter-UAS operations in the United States, where unmanned aircraft are legally classified as aircraft and only a limited number of federal entities possess authority to conduct mitigation actions. Participants also noted that counter-UAS systems are inherently layered and imperfect, often described as a "swiss cheese" model in which multiple systems must be combined to reduce vulnerabilities.

The Arctic Technology and Research Presentations, including discussions on underwater gliders and icing effects, reinforced the importance of understanding environmental impacts on system performance. These sessions highlighted how Arctic conditions—such as extreme cold, ice formation, and atmospheric inversions—affect sensing technologies. At the same time, participants noted that these conditions may also provide opportunities to enhance certain detection methods, particularly optical and infrared sensing.

The Arctic Edge Exercise Overview session linked these technical discussions to operational applications. Presenters emphasized that Arctic Edge serves as a platform for experimentation, allowing participants to test emerging technologies and concepts in realistic conditions. A key takeaway was the importance of using exercises to "test and fail" in controlled environments, enabling rapid iteration and refinement of capabilities.

Day Two – Strategic Context and Tabletop Exercise

The second day of the event focused on strategic framing and a scenario-based tabletop exercise aligned to the three core objectives of the workshop.

During the Arctic Security Landscape and Emerging Threats session, speakers emphasized that UAS represent one of the most likely threats to homeland defense. Drawing on observations from recent conflicts, participants noted the rapid proliferation of UAS technologies and their potential use in reconnaissance, disruption, and attack. **This session also introduced the concept of the "air littoral," describing the low-altitude airspace below traditional air defense coverage that has become increasingly contested**.

The Arctic Edge Lessons Learned and C-UAS Operations sessions highlighted operational gaps observed in recent exercises and real-world incidents. Participants noted that while detection capabilities are improving, response remains constrained by fragmented authorities and coordination challenges. These discussions reinforced the importance of integrating multiple stakeholders, including federal agencies, state and local authorities, and private-sector partners.

During the Panel on Counter-UAS Technologies and Operations (Lab to Field), participants explored the transition of technologies from research to operational use. A key insight was that innovation cycles in academia and industry often outpace government procurement processes, creating challenges for fielding new capabilities. **The panel also emphasized that counter-UAS is not solely a technical problem but one that involves legal, policy, and organizational considerations**.

The Joint Interagency Task Force (JIATF-401) Discussion focused on the policy and legal frameworks governing counter-UAS operations in the homeland. Participants highlighted the complexity of coordinating across multiple agencies and the constraints imposed by privacy laws and communications regulations. **A recurring theme was that "capabilities without authority create operational paralysis," underscoring the need to align technological capabilities with legal authorities.**

The Scenario-Based Tabletop Exercise (TTX) formed the core of the second day. Participants were placed into a scenario involving coordinated UAS incursions targeting military installations and critical infrastructure in Alaska. The scenario was designed to include ambiguity, limited authorities, and compressed timelines.

As the scenario unfolded, participants identified several key challenges. Detection of UAS activity was often possible, but determining intent and responding effectively proved difficult. The process for escalating and authorizing mitigation actions was frequently too slow, particularly when incidents occurred outside installation boundaries. **Participants also struggled to distinguish between accidental and deliberate activity, complicating coordination with law enforcement and infrastructure operators**.

The exercise demonstrated how quickly a UAS incident could escalate into a multi-faceted crisis. Disruptions to power, communications, or transportation infrastructure could generate cascading effects impacting both military operations and civilian populations.

From the perspective of military and civilian infrastructure security, TTX Working Groups discussed sensor integration, data sharing, and kill chain decision-making. Discussions highlighted that the primary challenge is not the lack of sensors, but the inability to integrate data into a coherent operational picture. Participants also **emphasized the need for standardized data formats, improved information sharing, and the integration of academic and commercial sensing systems**.

The Final Review and Synthesis Discussion focused on identifying actionable steps. Participants emphasized the **need to reduce decision latency through improved coordination, decision-support tools, and potential adjustments to authorities**. Additional recommendations included expanding partnerships, incorporating critical infrastructure operators into future exercises, and increasing experimentation under Arctic conditions.

Participants also highlighted the importance of preparing both the force and the public for UAS threats. While drones are often perceived as benign, their use in recent conflicts demonstrates their potential to create significant operational and psychological effects.

Annex B: Authorities Table

Organization	Primary Authority	Key Responsibilities	Limitations
Federal Aviation Administration (FAA)	Title 49 U.S.C.	Regulation of U.S. airspace and UAS operations	Cannot disable or destroy drones
Federal Aviation Administration (FAA)	Title 18 U.S.C.	Covers federal crimes against aircraft including sabotage, destruction, and fraud.	Prohibits interference with aircraft, aircraft sabotage, and aircraft destruction.
Department of War (DoW)	10 U.S.C. §130i	Detection and mitigation of UAS threats at designated military installations	Authorities limited to specific facilities and conditions
Department of Homeland Security (DHS)	6 U.S.C. §124n	Protection of federal facilities and national special security events	Limited operational scope
Department of Justice (DOJ) / FBI	Various criminal statutes	Investigation and enforcement related to illegal drone activity	Must operate within communications and privacy laws
Federal Communications Commission (FCC)	Communications Act of 1934	Regulation of spectrum use	Limits RF jamming and interference
State and Local Authorities	State laws	Enforcement of local regulations and criminal investigation	Generally lack mitigation authorities

Annex C: List of Significant Contributors and Organizations

- Dr. Cathy Cahill, Director, Alaska Center for Unmanned Aircraft Systems Integration (ACUASI), University of Alaska Fairbanks
- Joshua Beck, Administrative Professional, ACUASI, UAF
- John Robinson, Deputy Director, ACUASI, UAF
- Bremner Nickisch, Engineer, Northern Embedded Solutions (on contract with ACUASI, UAF)
- Larry Dobbs, Chief Engineer for Homeland Defense Mission, Johns Hopkins Applied Physical Laboratory
- Brittany Smart, Senior Advisor for Defense, Community, & Research, UAF Geophysical Institute
- Becky Lindsey, Director of Communications, UAF Geophysical Institute
- Kelly Eagan, Communications Manager, UAF Geophysical Institute
- Sara Wilbur, Communications Coordinator, UAF Geophysical Institute
- MAJ Chris Tunning, Director of Operations, Homeland Defense Institute
- Jesse “JJ” Johnson, Deputy Director, Homeland Defense Institute
- Laura McCutchen, Project Manager, Ted Stevens Center
- Wes Moerble, Arctic Operations Research Analyst, Ted Stevens Center

Annex D: List of TTX Participants

Title	Last	First	Job Title	Organization
CAPT	Albert	Rebecca	Deputy Director of Operations	US NORTHERN COMMAND
Mr.	Aboudara	Brent	Special Agent	FBI
Mr.	Anderson	Mike	Arctic Campaign Planner	USNORTHCOM
First Lieutenant	Autrey	Luke	COMSEC OIC	354 Communications Squadron
Special Agent	Beihl	Travis	Special Investigator	OSI Det 632
Dr.	Bobda	Chrisophe	Professor	University of Florida
GS14	Bransford	Ryan	Global CUAS Lead	US Army Counter-UAS and Emerging Threat Solutions Division
Wing Cmdr	Butler	Paul	SO 1 Air	British Defence Staff US
Dr.	Cahill	Cathy	ACUASI Director	University of Alaska Fairbanks
Mr.	Chandler	Gerald	CUAS Program Analyst	NNC J3C CUAS Division
Lt Cmdr	Davies	Rhys	NORAD C-UAS Action Officer	NORAD
SSgt	Davis	Taylor	NCOIC C-sUAS/sUAS	673 ABW
Mr.	Dobbs	Larry	Chief Engineer for Homeland Defense	Johns Hopkins University Applied Physics Lab
Commander	Dudley	Brian	Joint Counter UAS Planner and Responder	USNORTHCOM J3C
Dr.	Falco	Gregory	Assistant Professor Mechanical & Aerospace Engineering	Cornell University
Ms.	Fantinato	Tricia	C-UAS Technical Program Analyst	FAA Office of Advanced Aviation Technologies
Dr.	Fee	David	WATC Director	UAF Geophysical Institute
Ms.	Findlay	Glenda	AHDC Senior Program Manager	University of Alaska Fairbanks Geophysical institute
CW3	Giauque	Mark	AMD Systems integrator	11th Airborne Division
CW2	Hahn	Nathan	Intel Integrator/CUXS Lead	SOCNORTH
CW4	Harms	Mike	Aviation Mission Survivability Officer	Arctic Aviation Command 11th Airborne Division
Dr.	Heckman	Chris	Associate Professor	University of Colorado Boulder
LTC	Hignight	Ryan	DARPA Service Chief	DARPA
WO1	Horak	MarkAnthony	AMD Systems Integrator	1 BCT 11th ABN DIV
Mr.	Huelskoetter	Mark	Special Agent	FAA
Mr.	Johnson	Jesse "JJ"	DEPUTY DIRECTOR HOMELAND DEFENSE INSTITUTE	NORAD/USNORTHCOM
SES II	Kang	David	J7 Director- Joint Training Exercises and Wargaming	NORAD & USNORTHCOM
Maj Gen (Ret)	Kee	Randy (Church)	Director	Ted Stevens Center for Arctic Security Studies
Ms.	Kesavan	Meera	Research Chemist	Johns Hopkins Applied Physics Laboratory
Dr	Klenz	Thilo	Research Assistant Professor	University of Alaska Fairbanks
Dr.	La Belle-Hamer	Nettie	Geophysical Institute Deputy Director	UAF
Mr.	Larsen	Robert	Engineering Program Manager	OAIRE
CWO3	Lilliott	Aaron	Service Fellow Chief	DARPA
Dr.	Loui	Jacques	Senior Scientist	Sandia National Laboratories
SSgt	Magalhaes-Pachico	Lemuel	NCOIC Visitor Center	354 SFS
Dr.	McCoy	Bob	Director	Geophysical Institute
MAJ	Miller	Zachary	J5	Alaska National Guard
LTC (R)	Moerbe	Wes	Arctic Operations Analyst	Ted Stevens Center
CW2	Paulo	Shane	BDE EW Tech	HHC 1/11 IBCT
Mr.	Peterson	Nolan	Subject Matter Expert	Irregular Warfare Center
CPT	Ponder	Marilynn	Division Air Missile Defense Chief	11th Airborne Division
Dr.	Redding	Robert	Deputy Regional Advisor / NORTHCOM & Homeland Defense	DoW Irregular Warfare Center
Ms.	Redmond	Elizabeth	Lead Research Associate	Cornell Tech Policy Institute
Major	Rockwell	Jennifer	commander	354 SFS
Mr.	Rooney	Sean	Deputy Associate Director	Ted Stevens Center for Arctic Security Studies
Ms.	Rumsey	Nicole	Associate Director for Combatant Command Programs	Ted Stevens Center
Ms.	Smart	Brittany	Senior Advisor for Defense Community & Research	University of Alaska Fairbanks
TSS-E	Sterner	Tim	Transportation Security Specialist-Explosives	TSA/DHS
Sr. MSgt	Stinnett	Seth	S5 Superintendent	268 Security Forces Squadron
Mr.	Stone	Will	Senior Scientist	JHU/APL
Mr.	Thomas	Levi	Agent	DOJ
Mr.	Tiffany	Jason	Principal Staff	Johns Hopkins Applied Physics Lab
Mr.	Tosh	Jeremy	Engineer	The Johns Hopkins University Applied Physics Laboratory
MAJ	Tunning	Christopher	Director of Operations	Homeland Defense Institute
COL	Vanderlugt	Russ	Commander	Arctic Aviation Commander
SSgt	Volpe	Frank	NCOIC ESS & C-sUAS	354 SFS
2nd Lt	Wallace	Spencer	OIC Plans and Programs	354 SFS
Mr.	Walsh	Andrew	R&D Engineer	Oklahoma State University
1st Lt	Yantis	Lucas	Drone Countermeasures Engineer	AFRL Directed Energy
Mr.	Yost	Zachary	Senior Technical Advsior	USAF Test Center
Mr.	Youngblood	Dylan	sUAS Program Coordinator	State of Alaska Department of Public Safety

Annex E: Geophysical Institute EXSUM/AAR

ALASKA STATEWIDE COUNTER-UAS PROGRAM

Arctic Edge '26 · C-UAS Table-Top Exercise · UAF Geophysical Institute

NORTHCOM · NORAD · Multi-Agency · Fairbanks, Alaska · March 2026

DATE:	March 2026
TO:	NORTHCOM / NORAD Command Staff · Alaska DHSEM Leadership · JFHQ-AK · Arctic Edge '26 Participants
FROM:	Arctic Edge '26 C-UAS Table-Top Exercise — Program Coordination Team
SUBJECT:	Executive Summary — After Action Review, Arctic Edge '26 C-UAS TTX
CLASSIFICATION:	UNCLASSIFIED // FOR OFFICIAL USE ONLY (FOUO)

The Arctic Edge '26 Counter-Unmanned Aircraft System (C-UAS) Academic Table-Top Exercise convened a multi-agency, multi-tier cohort of professionals at the University of Alaska Fairbanks Geophysical Institute to examine the most urgent defense challenge facing Alaska's critical infrastructure: the coordinated, adversarial use of unmanned systems against assets that 47 million Americans depend on for energy, national missile defense, and Arctic sovereignty. Six scenario-driven teams independently interrogated three NORAD-NORTHCOM crucial output questions across simultaneous attacks against Fort Greely, Eielson Air Force Base, Fort Wainwright, Clear Space Force Station, Fairbanks International Airport and the Interior Alaska Infrastructure.

This summary presents the principal findings of the After-Action Review (AAR) that follows. The AAR addresses in full what was intended, what the participants produced, which pre-program assumptions the groups validated or left unaddressed, and what should happen next. This cover letter is written for decision-makers who require the bottom line before they reach the analysis.

PRINCIPAL FINDINGS

1.	**The strategic diagnosis was confirmed.** — Every team, independently, arrived at the same conclusion: Alaska's C-UAS vulnerability is a legal and organizational architecture problem, not a technology problem. Sensors exist. Partners exist. Legal frameworks exist. What does not exist is an integration spine connecting them to a NORTHCOM common operating picture. This is the most robust finding of the exercise. It was not prompted — it emerged from six independent teams working six different scenarios.
2.	**Four of nine assumptions were fully validated.** — The assumptions that UAF acoustic and atmospheric sensor networks can supplement low-altitude detection (A1.2), that a DoW-UAF research partnership under 10 USC 4001 is executable (A2.2), that pre-designated UAS exclusion zones with tiered defeat authority represent the correct kill

	chain solution (A3.1), and that AI-assisted threat classification with Human-in-the-Loop defeat authority is the right operational architecture (A3.2) — all four were independently arrived at by multiple teams without prompting. These assumptions should be treated as practitioner-validated program priorities.
3.	**Two critical assumptions were entirely absent from the group record.** — No team proposed a formal utility-to-NORTHCOM attack-indicator channel — the precise mechanism that would have routed the GVEA sabotage warning to military installations before the LRDR was destroyed. No team proposed formalizing the Alaska State Trooper and VPSO community observation network as a structured AK-Counter-UAS Fusion Center (AK-CFC) feed — despite the fact that the AST trooper's observation at Fort Greely was a 15–20 minute pre-warning that never reached the installation. These two omissions represent the most actionable and least expensive gaps in the entire program, and they were invisible to the exercise.
4.	**An Arctic Joint Interagency Task Force has practitioner legitimacy.** — Five of six teams independently recommended an Arctic JIATF — a permanently staffed, multi-domain, multi-tier task force with its own authorities and budget — as the appropriate interagency architecture for Alaska C-UAS. This is a meaningful upward scope expansion from the program's current AK-CFC concept. The groups are not wrong. A staffed desk within JFHQ-AK is a starting point, not a solution. The A-JIATF concept must be formally evaluated in the next program design cycle.
5.	**The human dimension of the kill chain is not ready.** — Multiple teams and the common friction record identified that the humans currently in the C-UAS kill chain do not understand the systems and processes they are responsible for. Training was named as a standalone priority by three teams. IFF ('Identify Friend or Foe') and 'Shoot, Don't Shoot' scenarios were named as non-existent. An exclusion zone with pre-delegated defeat authority means nothing if the duty officer does not know when and how to act within it. No program investment in technology or legal architecture will close this gap.
6.	**Rural Alaska was invisible.** — The six government tiers that underpin the critical infrastructure and key resource (CIKR) analysis include Territory and Tribal as the most vulnerable — 230+ villages, zero defeat authority, no direct federal link, Alaska Village Electric Cooperative (AVEC) micro-grids with no backup, and bulk fuel storage that represents a 72-hour survival window for entire communities. No team mentioned VPSOs. No team mentioned AVEC. No team addressed the statutory authority void for boroughs and tribal entities. The Interior Alaska military scenario focus biased participants away from the dimension of Alaska's C-UAS problem that has no institutional advocate.

RECOMMENDED NEXT STEPS — TOP FIVE BY CIKR CONSEQUENCE		
1	Stand up AK-CFC as a staffed 24/7 fusion desk within JFHQ-AK — connecting utility Supervisory Control and Data Acquisition (SCADA), borough Emergency Operations Centers (EOCs), UAF sensors, and the Alaska State Troopers and Village Public Safety Officer (AST/VPSO) observation network into a single NORTHCOM common operating picture. This is the prerequisite for every other action on this list.	**[PROGRAM] 0–8 months**
2	Execute pre-signed UAS Exclusion Zone orders with tiered defeat authority for Fort Greely GMD, Clear SFS LRDR, Eielson F-35A hangars, Fort Wainwright, and TAPS Pump Station 1. The legal framework exists. The gap is unsigned execute orders.	**[PROGRAM] 0–6 months**
3	Execute NORTHCOM–borough EOC data-sharing MOUs (bidirectional, FOUO level) with the FNSB, NSB, Mat-Su, Kenai, and Kodiak borough EOCs. These nodes are 24/7 staffed	**[PROGRAM] 6–9 months**

	and adjacent to every high-risk federal installation. They currently have no formal pathway to military threat data.	
4	Establish a formal DHS-brokered utility attack-indicator agreement with GVEA, MEA, Chugach, and AVEC routing SCADA anomaly events to AK-CFC. This provides 15–30 minutes of pre-attack warning on infrastructure sabotage and requires no new hardware — only a signed agreement.	**[PROGRAM] 0–12 months**
5	Formalize the AST/VPSO community observation network as a structured UAS sighting report feed to AK-CFC via existing HF/VHF radio. Zero new equipment. Six months to operational. The fastest, cheapest, and most consistently overlooked C-UAS capability in the state.	**[PROGRAM] 0–6 months**

The Arctic Edge '26 TTX confirmed that Alaska's C-UAS problem is solvable within the existing legal and organizational architecture. The sensors are there. The partners are there. The frameworks are there. Eight of the thirteen recommended next steps in the full AAR are achievable within the 24-month program strategy window without new legislation or new procurement.

What the exercise also confirmed is that time is the one resource the program does not have. The adversary does not wait for MOUs to be signed or task forces to be chartered. The C-UAS capabilities proposed by the six teams — exclusion zones, fusion cells, sensor agreements, observation networks — are not aspirational. They are executable. The five steps above can be operationally in place within twelve months of a decision to act.

The full After Action Review that follows this letter documents the evidence behind each finding and the rationale for each next step. It is the record of what a diverse, experienced, multi-agency cohort of Alaskans determined, in one room, about the most urgent infrastructure defense challenge their state has ever faced. That record deserves a response proportional to its urgency.

Submitted by:

Arctic Edge '26 C-UAS TTX Program Coordination Team

UAF Geophysical Institute · Fairbanks, Alaska

March 2026

Enclosure:

After Action Review — Arctic Edge '26 C-UAS TTX

10 pages · 7 sections · UNCLASSIFIED // FOUO

ArcticEdge26_CUAS_TTX_AfterActionReview.docx