POST FX 2023
Final Report

“Seizing the Initiative via Decision Superiority, Innovation and Collaborative Partnerships”

March 9, 2023
Honolulu, Hawai‘i
Executive Summary

The Pacific Operational Science & Technology Conference (POST) is the United States Indo-Pacific Command’s (USINDOPACOM) annual Science and Technology (S&T) conference. The conference brings together policy, military, industry, and academic leadership from the US and its Pacific allies to focus on the emerging stability challenges in the Indo-Pacific region. The theme for POST 2023, “Seizing the Initiative via Decision Superiority, Innovation and Collaborative Partnerships,” inspired informed, collective action across the full span of S&T exploitation.

The conference underscored the importance of information sharing, technology development, and mission-focused cooperation to maintaining a free and open Indo-Pacific. The Field Experimentation (FX) component of the conference is designed to provide a stage for field demonstrations of technologies that engage USINDOPACOM’s allies and partners. Following a successful POST FX in 2022, the event was repeated in 2023 to offer a platform to vendors from small and local companies, larger corporations, and those employed by USINDOPACOM or other government agencies to present their technologies.

POST FX 2023 was conducted on March 9, 2023, at the Ke Kula Maka’i Honolulu Police Academy in Waipahu, Hawai’i and hosted 23 organizations, agencies, and technology vendors. Approximately 170 attendees from the US Government and Pacific Security Partners, industry, and academia from 10 countries were part of this event.

Feedback from POST FX 2023 technologists and attendees was positive and many indicated the event provided both useful information about technologies and excellent networking opportunities. From this feedback, this field demonstration will likely continue to be an important component of future POST conferences. This report connects interested readers with POST FX organizers and technology providers for appropriate discussion using the contact information provided.
## Contents

Executive Summary ................................................................................................... 2
Contents ................................................................................................................... 3
Acronyms ............................................................................................................... 4
Purpose and Objective ........................................................................................... 6
Location and Participants ....................................................................................... 7
Technologies Demonstrated
- Air Force Research Laboratory ........................................................................ 8
- Applied Research Laboratory at the University of Hawai‘i ................................ 10
- Booz Allen Hamilton .......................................................................................... 12
- Beamlink ............................................................................................................ 14
- BioMADE ........................................................................................................... 16
- BlueVoyant Government Solutions ................................................................. 18
- Caliola Engineering ............................................................................................ 20
- Dontec ................................................................................................................. 22
- EpiSci .................................................................................................................. 24
- FlightWave Aerospace Systems ....................................................................... 26
- Fornetix/General Dynamics Information Technology ...................................... 28
- Fourth State Communications .......................................................................... 30
- Northern Arizona University ............................................................................. 32
- QuSecure ............................................................................................................ 34
- Reveal Technology .............................................................................................. 36
- Silvus Technologies ............................................................................................ 38
- Synthetaic ............................................................................................................. 40
- TDA Research .................................................................................................... 42
- USACE ERDC (US Army Corps of Engineers, Engineer Research & Development Center) .................................................................................. 44
- Vermeer ............................................................................................................... 46
- Zepher Flight Labs .............................................................................................. 48
Conclusion .............................................................................................................. 50
<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2/AD</td>
<td>Anti-Access/Area Denial</td>
</tr>
<tr>
<td>ACE</td>
<td>Agile Combat Employment</td>
</tr>
<tr>
<td>AFCEC</td>
<td>Air Force Civil Engineer Center</td>
</tr>
<tr>
<td>AFRL</td>
<td>Air Force Research Laboratory</td>
</tr>
<tr>
<td>AFSOC</td>
<td>Air Force Special Operations Command</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>ARL at UH</td>
<td>Applied Research Laboratory at the University of Hawai‘i</td>
</tr>
<tr>
<td>ASV</td>
<td>Autonomous Surface Vehicle</td>
</tr>
<tr>
<td>ATAK</td>
<td>Android Tactical Awareness Kit</td>
</tr>
<tr>
<td>ATO</td>
<td>Authority to Operate</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BLOS</td>
<td>Beyond Line of Sight</td>
</tr>
<tr>
<td>BV</td>
<td>BlueVoyant</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOE</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>ERDC</td>
<td>Engineer Research &amp; Development Center</td>
</tr>
<tr>
<td>ETSS</td>
<td>Enhanced Thermo-Scatter System</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FOC</td>
<td>Full Operational Capability</td>
</tr>
<tr>
<td>FX</td>
<td>Field Experimentation</td>
</tr>
<tr>
<td>GDFS</td>
<td>Graphical Data Fusion System</td>
</tr>
<tr>
<td>GO</td>
<td>Graphene Oxide</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>HADR</td>
<td>Humanitarian Assistance and Disaster Relief</td>
</tr>
<tr>
<td>HF</td>
<td>High Frequency</td>
</tr>
<tr>
<td>HFD</td>
<td>Honolulu Fire Department</td>
</tr>
<tr>
<td>HPD</td>
<td>Honolulu Police Department</td>
</tr>
<tr>
<td>IL</td>
<td>Impact Level</td>
</tr>
<tr>
<td>INDOPACOM</td>
<td>Indo-Pacific Command</td>
</tr>
<tr>
<td>ISR</td>
<td>Intelligence, Surveillance, Reconnaissance</td>
</tr>
<tr>
<td>IW</td>
<td>Information Warfare</td>
</tr>
<tr>
<td>J85</td>
<td>Science and Technology Division</td>
</tr>
<tr>
<td>JADC2</td>
<td>Joint All-Domain Command and Control</td>
</tr>
<tr>
<td>LARS</td>
<td>Launch and Recovery System</td>
</tr>
<tr>
<td>LiDAR</td>
<td>Light Detection and Ranging</td>
</tr>
<tr>
<td>MDA</td>
<td>Maritime Domain Awareness</td>
</tr>
<tr>
<td>MiSo</td>
<td>Mini Sonde</td>
</tr>
<tr>
<td>MN-MIMO</td>
<td>Mobile Network Multiple Input Multiple Output</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>MR</td>
<td>Mixed Reality</td>
</tr>
<tr>
<td>MVP</td>
<td>Minimum Viable Product</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NDIA</td>
<td>National Defense Industrial Association</td>
</tr>
<tr>
<td>NUTR</td>
<td>Nearshore Unified Tactical Response</td>
</tr>
<tr>
<td>OTH</td>
<td>Over-the-horizon</td>
</tr>
<tr>
<td>OUSD</td>
<td>Office of the Under Secretary of Defense</td>
</tr>
<tr>
<td>PNT</td>
<td>Position, Navigation, and Timing</td>
</tr>
<tr>
<td>POST</td>
<td>Pacific Operational Science &amp; Technology Conference</td>
</tr>
<tr>
<td>POST FX</td>
<td>POST Field Experimentation</td>
</tr>
<tr>
<td>PPE</td>
<td>Personal Protective Equipment</td>
</tr>
<tr>
<td>R&amp;E</td>
<td>Research and Engineering</td>
</tr>
<tr>
<td>RAIC</td>
<td>Rapid Automatic Image Categorization</td>
</tr>
<tr>
<td>RES3</td>
<td>Rapid Expeditionary Security Surveillance Solution</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>S&amp;T</td>
<td>Science and Technology</td>
</tr>
<tr>
<td>SATCOM</td>
<td>Satellite Communications</td>
</tr>
<tr>
<td>SBIR</td>
<td>Small Business Innovation Research</td>
</tr>
<tr>
<td>SCC</td>
<td>Supply Chain Command</td>
</tr>
<tr>
<td>SCD</td>
<td>Supply Chain Defense</td>
</tr>
<tr>
<td>SCRM</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>SiaB</td>
<td>Sensor-in-a-Box</td>
</tr>
<tr>
<td>SIGINT</td>
<td>Signals Intelligence</td>
</tr>
<tr>
<td>SMART</td>
<td>Science Monitoring And Reliable Telecommunications</td>
</tr>
<tr>
<td>SW</td>
<td>System Software</td>
</tr>
<tr>
<td>SWaP</td>
<td>Size, Weight and Power</td>
</tr>
<tr>
<td>TRL</td>
<td>Technology Readiness Level</td>
</tr>
<tr>
<td>UAS</td>
<td>Uncrewed Aircraft System</td>
</tr>
<tr>
<td>UAV</td>
<td>Uncrewed Aerial Vehicle</td>
</tr>
<tr>
<td>UGV</td>
<td>Uncrewed Ground Vehicle</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra High Frequency</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USCENTCOM</td>
<td>United States Central Command</td>
</tr>
<tr>
<td>USINDOPACOM</td>
<td>United States Indo-Pacific Command</td>
</tr>
<tr>
<td>USV</td>
<td>Uncrewed Surface Vehicle</td>
</tr>
<tr>
<td>VHF</td>
<td>Very High Frequency</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VPS</td>
<td>Vision Positioning System</td>
</tr>
<tr>
<td>VTOL</td>
<td>Vertical Take-Off and Landing</td>
</tr>
</tbody>
</table>
Recent technology advancements have altered the region’s competitive landscape and security environment. As the United States (US) military engages with regional partners, our community must innovate with a sense of urgency to develop, experiment, and apply new technologies and capabilities to confront these more complex challenges. “Seizing the Initiative via Decision Superiority, Innovation and Collaborative Partnerships” was this year’s theme for POST and the event placed a special focus on expediting technology transition and transfer, multi-lateral information sharing, and all-domain battlespace awareness. The security challenges in this region require all of us to move forward together at a faster and smarter pace and work to collaborate, innovate and strengthen efforts to maintain peace and prosperity in the Indo-Pacific through science and technology. Developing solutions from different perspectives and rapidly transitioning scientific ideas to technology demonstrations to experiment in an iterative manner are crucial to enable us to advance greater capabilities to the joint and combined warfighting force.

POST hosts the Indo-Pacific’s foremost experts in science, technology, and security who gather to better understand and address the critical issues and challenges of the region and encourages academia, industry, and government leaders to align innovation priorities. The event also showcases prototyping and experimentation in support of joint fires, information advantage, contested logistics and other joint warfighting challenges. POST FX 2023 demonstrations, designed to promote collaboration, featured technology companies and agencies associated with Pacific security and humanitarian assistance and disaster relief (HADR) situations and generally focused on intelligence-gathering sensors, tactical communications, damage detection, and uncrewed aircraft systems (UAS). POST FX target participants are technology providers, including military agencies and academia, that are involved in supporting USINDOPACOM and allied partners.

POST FX 2023 demonstrations aligned with one or more of the following innovation priorities:

- Biotechnology
- Quantum Science
- Future Generation Wireless Technology (FutureG)
- Advanced Materials
- Trusted Artificial Intelligence (AI) and Autonomy
- Integrated Network Systems-of-Systems
- Microelectronics
- Space Technology
- Renewable Energy Generation and Storage
- Advanced Computing and Software
- Human-Machine Interfaces
- Directed Energy
- Hypersonics
- Integrated Sensing and Cyber

The purpose of POST FX 2023, held on March 9, 2023, was to initiate a framework for field experimentation around these innovation priorities, promote collaboration among vendors, agencies, and the US and its allies and partners, and bring forth solutions as they emerge.
Location and Participants

Funding for POST FX 2023 was provided by USINDOPACOM J85. In-kind support was provided by the Honolulu Police Department (HPD). The National Defense Industrial Association (NDIA) provided transportation and marketing support. The Applied Research Laboratory at the University of Hawai‘i (ARL at UH) planned, arranged, organized, and executed the event.

The one-day demonstration event was held in an outdoor area at the Ke Kula Maka‘i Honolulu Police Academy in Waipahu. The location provided a convenient and secure venue to host the event with a covered area where technologists set up their demonstration equipment and an open-air area for the setup of large vehicles and where it was safe to fly UAS; the airspace is Federal Aviation Administration (FAA) Class G, enabling ARL at UH and contractor UAS operations under Code of Federal Regulations (CFR) 107, FAA Educational Interpretation, or Certificate of Authorization. Technology vendors arrived and set up their equipment one day prior to the demonstrations to ensure functionality and deconflict operations. There was also a period of time during the setup day dedicated to vendor cross-briefings to facilitate collective awareness of all of the capabilities brought to the event.

The event demonstrated 23 organizations, agencies, and technology vendors from across the Defense Industrial Base who showcased how their capabilities can assist in maintaining a free and open Indo-Pacific region. Visiting observers were split into small groups and rotated through each exhibit in a round-robin style where exhibitors made a short presentation on their capabilities and entertained questions from observers. About 170 attendees from the US Government and Pacific Security Partners, industry, and academia attended; of those, 54 participants were demonstrating their technology and the remaining 116 consisted of observers from 10 countries. One ‘demonstration’ area was reserved for the HPD and Honolulu Fire Department (HFD) to display equipment, videos, and engage in conversation with observers and with technology demonstrators. The success and interest generated by this second POST FX event suggest that this event should continue to be hosted in the future to foster the relationships between technology providers and users.
Graphene Oxide Fuel Filter for Biocontamination

**Technology Description / Product:**
- Graphene oxide (GO) nanofiltration media removes >99.97% of microbes present.
- Filtration is not dependent on small size pores.
- Electrostatic interaction between nanomaterial & microbes work synergistically to trap microorganisms.

**Technology Product**
- Integrated and validated microbial fuel filters
- Transition from TRL 5 to TRL 7

**Focus Areas:**
- Biotechnology
- Advanced Materials

**Where do we fit in?**
- Bilateral Secure Comms
- DIL
- Intel, Fusion, Threat Pacific Collaboration
- Deploy & Support
- Effector

**Company Information:**
- Dr. Mitchell Meade
  Air Force Research Laboratory
  937-255-6416
  mitchell.meade.1@us.af.mil

- Dr. Oscar Ruiz
  Air Force Research Laboratory
  Wright Patterson Air Force Base
  Oscar.ruiz@us.af.mil
  937-255-6237

**Deploy and Support:**
Can be used for maintaining and sustaining fuel systems by removing microbial growth that occurs in fuel storage tanks. This can result in biofouling of the fuel and impacts on vehicles.

Effective microbial filtration will reduce or even prevent biodeterioration in Air Force and DoD fuel systems.
Graphene Oxide Filter for Decontamination of Fuels

Biocontamination can deteriorate fuel and damage the performance of fuel systems. Thus, it is critical to develop effective methods to prevent and mitigate biocontamination in fuel. Filtration is an effective way to maintain fuel cleanliness. However, even the best aircraft filters cannot efficiently filter out particles smaller than 1 µm in size. Most bacteria have a diameter of less than 0.5µm thus it would require filter of ≤0.22 µm in pore diameter for effective filtration. Such filter would present a strong barrier to the flow of fuel and would lead to large pressure drops. If filtration is to be used for fuel biocontamination prevention and remediation, a new filtration technology not dependent on filter pore size is required. Previously, we demonstrated the development of a graphene oxide (GO) nanomaterial fuel filtration technology that was not dependent on particle size exclusion for filtration and provided 99.97% microbial filtration efficiency in laboratory testing. Here we show further development of the GO filtration technology into field-demonstrated microbial fuel filters for gas station fuel dispensers (diesel fuel pumps) and electrical power generators. We describe the engineering including filter geometries and configurations, laboratory validation, and field testing that was required to create a fuel filter capable of providing >90% (>99% actually achieved) microbial filtration efficiency at fuel flow rates of up to 20 GPM for at least 100,000 gallons of diesel fuel. The filter has a delta pressure of ≤4 psi, which is well below the maximum of 7 psi for current bulk gas station fuel filters. The filter is of modular design allowing easy scale up for applications such jet fuel filtration that require much larger volumes. The field demonstration not only showed the functionality and durability of the filter under real use conditions, it also helped mature and de-risk the technology one-step further to facilitate its implementation.
Applied Research Laboratory at the University of Hawaii (ARL at UH)

Research, Development, Testing & Evaluation in the Maritime Environment

- Leverage existing toolchains and command-and-control software to design and build new capabilities for near real-time maritime domain awareness (MDA).
- Design and rapid fabrication of resilient coral reefs to protect near-shore facilities and environments.

Technology Description / Product:

- The ARL at UH is leading a multidisciplinary team who is designing, testing and fielding a fringing-reef-inspired living coastal protection system that will attenuate wave energy and facilitate the growth of a climate-tolerant coral-reef ecosystem. The team is utilizing state-of-the-art rapid prototyping and manufacturing technology, computational fluid dynamics, and cutting-edge adaptive biology techniques to develop an engineered reef that will become a growing, self-healing coastal breakwater system.
- The ARL at UH is designing, building, and integrating an uncrewed system consisting of Mini Sondes (MiSos) and a seabed communications relay node that can be connected by single-mode fiber optic science monitoring and reliable telecommunications (SMART) cables. The MiSos can relay position, monitor water temperature and pressure, and measure sound velocity. Additional sensors can be integrated into the system according to parameter monitoring needs.

Where do we fit in?

Focus Areas:

- Demonstrate rapidly manufacturable, modular, and low-cost infrastructure, platforms and sensors that can be used in a variety of MDA operations.
- Establish information dominance in contested littoral zones where traditionally accessible radio or satellite communication pathways may be blocked or pose a risk to allied forces, should they utilize these pathways.
- Present alternative methods of communication that are resilient to natural hazards and denial-of-service attacks.
- Design and install structures that are compatible with the surrounding environment.

Contact Information:

Applied Research Laboratory at the University of Hawaii

www.hawaii.edu/arl

2800 Woodlawn Drive
Honolulu, HI 96822

Margo Edwards: margo@arl.hawaii.edu
Joshua Baghdady: baghdady@arl.hawaii.edu
The ARL at UH is one of five Navy-sponsored University Affiliated Research Centers (UARCs). The ARL at UH serves as a center of excellence for critical Navy and national defense needs, imagining and developing agile, innovative and cost-effective solutions to problems impacting our stakeholders, our community, and our planet. The ARL at UH efforts focus on Ocean Environmental Effects, Astronomical Research, Advanced Electro-Optical Systems, Detectors, Arrays and Instrumentation, Environmental Sensor Research and Remote Sensing, New Renewable Energy, and Mission-Related and Public-Services-Oriented Research and Development. During POST FX 2023, ARL at UH focused on two project areas: maritime domain awareness (MDA) and coastal protection through rapid fabrication of resilient reefs.

**Maritime Domain Awareness.** Establishing information pathways in damaged or contested littoral zones where communication tools may not be able to operate is crucial for making effective rapid response decisions; communication methods that are resilient to natural hazards and denial-of-service attacks can provide MDA data to decision makers. The ARL at UH developed capabilities to rapidly manufacture modular and low-cost platforms and sensors for MDA operations. Integrated uncrewed systems, both designed and built in-house and purchased from private industry, supplemented Mini Sondes (MiSos) and seabed-emplaced communication relay nodes connected by single-mode fiber optic SMART cables to transmit location and environmental data over broad spatial scales at high sampling rates in support of improved MDA requirements.

**Coastal Protection:** The Rapid Resilient Reefs for coastal Defense (R3D) project aims to re-design coastal breakwaters by developing engineered, living reefs that dissipate wave energy and protect coastal locations in the tropical Pacific. The ARL at UH is leading a multidisciplinary team that is designing, testing, and fielding a living coastal protection system, inspired by natural fringing reefs, that will attenuate wave energy and facilitate the growth of a climate-tolerant coral-reef ecosystem. The project includes development of additively manufactured, structurally complex habitats, acoustic enrichment of the site with healthy reef sounds, and development of natural chemical and biological cues to attract the settlement of coral and reef-supporting fishes and invertebrates. Collaborators in this five-year effort include five laboratories at the University of Hawai'i, the University of California San Diego / Scripps Institution of Oceanography, Florida Atlantic University and Makai Ocean Engineering.
Rapid Expeditionary Security Surveillance Solution (RES3)

Alan Kolackovsky, Booz Allen Hamilton, Kolackovsky_Alan@bah.com

Where do we fit in?

- **Focus Areas:**
  - Integrated Sensing and Cyber
  - Advanced Computing and Software

**Technology Description / Product:**

SiaB employs COTS technology, extending electromagnetic radio frequency, electro-optical/infrared (EO/IR), full motion video, and threat detection capability through an adaptable, Ground/Air/Surface/multi-platform capable design to resolve gaps in sensors and command and control (C2) for Joint and Partner Forces.

- Modular small form factor enables specialized platform configuration and integration.
- Scalable integrated edge processing, ML/AI application integration framework for resilience.
- Cyber offensive/defensive support options Modular open architecture approach enables integration with future and legacy government systems and programs of records.

**Company Information:**

Booz Allen Hamilton founded in 1914 with Headquarters McLean, VA provides management and technology consulting, engineering, analytics, digital solutions, mission operations, and cyber expertise to U.S. and international governments, major corporations, and not-for-profit organizations. Booz Allen has supported Information, Electronic and Cyber Warfare, Electromagnetic Spectrum Operations and Battlespace Management with direct hands-on and experience with DoD EM spectrum environments.

Booz Allen is an industry leader providing rapid prototyping & systems of systems integration to support U.S. Navy, Marine Corps, Army, & Fleet Forces C5ISR solutions. Booz Allen brings extended reach-back into Warfare Centers, Research Facilities, & Program Offices to deliver solutions.
The Rapid Expeditionary Security Surveillance Solution (RES3) delivers a deployable, small form factor, self-contained conex box and a small human element supported with integrated sensors and payloads, autonomous platforms integrated into the Nearshore Unified Tactical Response (NUTR) system to support the U.S. Indo-Pacific operational strategy. Currently INDOPACOM expends significant resources securing and monitoring over-the-horizon sensing and targeting, tracking and locating of potential threats. INDOPACOM strategy consumes massive, manned resources and multidomain capabilities, such as:

- Lack of dedicated resources to monitor all facets within the region.
- Modern coastal gray water and port security lacks the rapid advance of technology and contains significant gaps, exposing critical vessels, manufacturing facilities, and shipyards vulnerable to exploitation and attacks from adversaries.
- Interagency cooperation is part of port and harbor security due to overlapping boundaries and adjacent jurisdictions. A lack of interoperability and commonality of systems is compounded by varying degrees of authority and enforcement, often requiring increased and redundant workloads to ensure adequate mission coverage and accomplishment.

**Sensor in a Box (SiaB)** (Figure 1) is a patent pending, multi-capable sensor and payload that is ruggedized for multiple platforms, to include manned and unmanned. SiaB is a stand-alone, self-contained, portable integrated unit, with onboard ML/AI capabilities embedded in a compact edge processing computer connected to a payload input/output communication suite. SiaB provides a platform-agnostic information warfare (IW) and signals intelligence (SIGINT) process with remote sensor fusion, integrated with the GOTS Nearshore Unified Tactical Response (NUTR) Graphical Data Fusion System (GDFS), which can control the SiaB remotely. SiaB has been deployed in fleet experiments and demonstrations; integrated into an unmanned surface vehicle (USV) and deployed in the northern Gulf of Mexico for 32-consecutive days performing environmental analysis. SiaB has five (5) variant form factors to support manned and unmanned platforms. SiaB provides the DoD, DHS, and DOE a sensor platform capable of redesigning to meet the users mission and operational needs, while providing a flexible payload that is easily integrated across multiple platforms to support various operational requirements.

Booz Allen Hamilton founded in 1914 with Headquarters McLean, VA provides management and technology consulting, engineering, analytics, digital solutions, mission operations, and cyber expertise to U.S. and international governments, major corporations, and not-for-profit organizations. Booz Allen has supported Information, Electronic and Cyber Warfare, Electromagnetic Spectrum Operations and Battlespace Management with direct hands-on and experience with DoD EM spectrum environments. Booz Allen Hamilton Navy and Marine Corps San Diego team provides rapid prototyping, engineering services, integration, and testing in support of Fleet Experimentation/ Demonstrations.
Beamlink

Technology Description / Product:
Beamlink’s portable cellular network technology enables first time to packet in less than 5 minutes.
- Full LTE and 5G-NR supported, as well as secure WiFi (WPA2)
- Mesh capability: Each device communicates to each other to enable greater range and decentralization
- Up to 2.0 miles (400 MHz) to 0.4 miles (6 GHz) range (line of sight) thanks to new low-cost amplification and filter technology.
- Compatible with any device that supports cellular or WiFi data connectivity
- SNOW-3G cipher (Radio security) and AES-256 (IP Security)
- Cellular and WiFi capability: TRL6, Mesh Capability: TRL4
- Interoperable with other IP systems

Private networks enable completely off-the-grid and secure networks, independent from foreign or domestic network providers.

Company Information:
Beamlink, Inc.
www.beamlink.io
arpad@beamlink.io
6060 Center Drive Suite 1000, Los Angeles CA 90045
The simplest & most adaptable network for austere contexts

On-base or off-the-grid

Maintaining communication across teams on-base or in the field is paramount to safety and effectiveness. When a disaster event hits, consistency and reliability in connectivity means emergency response networks need to be fully integrated with baseline systems. Private networks offer opportunity and efficiency in facilitating day-to-day operations and logistics, as well as long-term change and growth. They also free users from having to rely on external 3rd party providers, enabling them to build networks anywhere, in any way.

Enabling mission success with ease

We designed our secure portable cell towers and network architecture specifically for areas that have lost — or never had — consistent, reliable connectivity. Our towers are extremely low cost and auto-configure with the push of a button, so anyone can set up a network and fill in connectivity gaps quickly and easily.

Beamlink uses the standard SNOW-3G cipher for LTE and 5G-NR radio security and AES-256 for IP layer security, keeping all traffic fully encrypted end-to-end. All elements of the network can be hosted on site for additional control while easily communicating with those on the network.

Specifications

- **Protocols**: 4G LTE, 5G-NR, Wifi
- **Backhaul**: Satellite or Broadband Ethernet
- **Mesh**: Devices can share backhaul

**Range**: 0.5 – 2 mi a.o.n

**Weight**: 8 lbs

We want to hear from you

**Website**: beamlink.io

**Email**: hello@beamlink.io

**Twitter**: @beamlinkio

**Address**: 6060 Center Drive Suite 1000
Los Angeles, CA 90045
**Biocementation for Airfield Augmentation**

**Technology Description / Product:**
- Non-modified, naturally occurring bacterial spores applied to harden surfaces
- Leverages on-site resources (soil/water) to harden ground surfaces; cement produced ≤ 96 hours w/ significantly reduced manpower & heavy machinery requirements of traditional methods
- Uses affordable, locally sourced chemicals for growth; urea-fertilizer, CaCl₂-road salt
- Fieldable using multiple water types – fresh, salt, brackish and gray
- Accelerates construction of critical base infrastructure (i.e. parking aprons, roads, amphibious zones, foundations, LZs, and more)
- Creates 50% less greenhouse gas vs. Portland cement manufacturing

**Company Information:**

Dr. Maneesh Gupta
Air Force Research Laboratory
Maneesh.gupta.2@us.af.mil
937-255-9145

Dr. Mitchell Meade
Air Force Research Laboratory
Mitchell.Meade.1@us.af.mil
937-255-6416
Biocementation
AFRL is collaborating with a North Carolina-based small business to develop biomanufacturing processes to rapidly expand austere airfields using common agricultural chemicals and natural resources (soil and water) found at the location. These processes significantly reduce the need for heavy equipment, large teams of civil engineers and large quantities of cement and other materials to be shipped to the site. Instead, it allows bacteria to transform the local soil into hardened biocement by creating calcium carbonate crystals and binding the soil. This allows US forces to build infrastructure in otherwise resource-poor locations and operate from locations that were previously inaccessible. Once US forces have finished using the airfield, the hardened earth can easily be returned to its original state, lessening the ecological impact of overseas deployments of military personnel.

Naturally occurring bacteria, *S. pasteurii*, are grown on site and sprayed onto the soil where they are given a chance to percolate and grow. Feedstock chemicals, urea and calcium chloride, are then prepared and sprayed on the soil surface. The bacteria produce an enzyme called urease that reacts with urea to form ammonia and carbonate. In the presence of calcium, this forms calcium carbonate, which binds the soil particles together increasing the overall strength of the soil.

The biocement process can be used to treat and stabilize weak sandy soils and significantly improve the soil’s load-bearing capacity. The entire process can be carried out in less than 96 hours from initial setup to ready-to-use surface. AFRL and the Air Force Civil Engineer Center (AFCEC) are currently working to test the ability of biocement stabilized soils to support heavy ground vehicles and cargo aircraft for short-duration operations. Additional research and testing is currently being conducted to determine the feasibility of the material for use in operational environments and for various uses.

Biomanufacturing and biocement will enable tomorrow’s US Air Force to project power and realize their Global Power and Global Reach missions. This capability is made possible by the expertise of AFRL Materials & Manufacturing researchers working to translate the commercial developments to meet the special needs of the military.
BlueVoyant Supply Chain Defense

John Eubank, IV BlueVoyant, [443-717-2100], john@bluevoyantgov.com

Technology Description / Product:
Supply Chain Defense (SCD) provides global insight across supplier ecosystems for major weapon systems, US Federal Agencies, Commercial Industry, the Department of Defense, and International Partners.

SCD provides a comprehensive mapping of suppliers to programs down to the material level with context and analyst reporting on risks and vulnerabilities.

Through SCD users can Illuminate, Validate, and Remediate issues in the supply chain. SCD provides visibility to cyber threats and vulnerabilities along with business and operational risks (e.g. weather events and manufacturing trends).

SCD is available as a Managed Service in AWS GovCloud with immediate data access and analyst driven reporting in as little as 72 hours.

Company Information:
BlueVoyant is a Non-traditional Defense Contractor (NTDC). Our capabilities can be accessed under our SBIR Phase III contract vehicle.

BlueVoyant is a Cyber Defense Platform company that supports and enables cyber defense across the globe. Our portfolio is integrated across three lines of effort:
1. Illumination – Understanding and mapping of global supply chains using publicly and commercially available information (PAI/CAI)
2. Validation – Analyst curated reporting and cyber vulnerability analysis
3. Remediation – Alternative supplier recommendations and cyber vulnerability patching and mitigation

Focus Areas:
- Biotechnology
- Future Generation Wireless Technology (FutureG)
- Advanced Materials
- Microelectronics
- Space Technology
- Renewable Energy Generation and Storage
- Advanced Computing and Software
- Directed Energy
- Hypersonics
- Integrated Sensing and Cyber
**BlueVoyant’s Supply Chain Command (SCC)** provides visibility across global Government and Commercial supply chains. For the Department of Defense (DoD) we provide decision advantage across all Weapon Systems, Programs, Major Defense Acquisition Programs, and other systems. Our data informs decision making, identifies threats and vulnerabilities, brings understanding to risk and issues, and enables action to be taken to mitigate and avoid problems prior to their impact to the end users.

**Illuminate** ➔ we use non-Government data sets to identify the complete supplier ecosystem for all major defense programs covering over 2,000,000 unique global suppliers and over 3,000,000 unique facilities. Artificial Intelligence (AI) and Advanced Analytics process the data in real-time to derive situational awareness and understanding from over 50,000 data sets.

**Validate** ➔ Our Analyst-in-the-loop approach validates the data processing results, applies context to them, and validates risks alerts to reduce alert overload and data volumes to the users.

**Remediate** ➔ We don’t just identify the problem. We take action across the supply chain to improve cyber security postures, mitigate risks, provide alternative supplier recommendations, and inform decision makers before the risks become problems that block deliveries.

Supply Chain Command is ready for use and is currently being used for supply chain risk management (SCRM) and cyber defense of supply chains. The capability is operationally ready and is deployed within Amazon Web Services (AWS) GovCloud at Impact Level (IL) 4 with a roadmap for deployment to higher impact levels for National Security System (IL 5) and classified data (IL 6 and 11). As a Managed Service running in the cloud we can provide immediate scaling to meet new use cases and operational requirements.

Our offering supports the acquisition of tactical network systems and visibility into the supply chain ecosystem of the tactical networks. Our solution identifies supply chain business and operational risks along with cyber vulnerabilities to the vendors in the supplier ecosystem. With SCC we can show scalability issues, reliance on foreign suppliers, manufacturing risks, and potential cyber compromises that may reduce the integrity of what the supply chain delivers.

We enable readiness across the Joint Force with information advantage across weapon system and major defense system lifecycles. SCC brings visibility into the viable of new development efforts, the sustainment of existing systems, the maintenance ability to procure parts and spares, and the dependencies on global logistics networks. Our technology is cyber hardened and we continue to improve the security posture through on-going development efforts.

For technology innovation we have a multi-year roadmap to provide additional visibility and capabilities to improve cyber defenses across the entire DoD supplier ecosystem.

**Company description.** Founded in 2019, BlueVoyant (BV) is a Venture Capital backed startup with over 600 global employees. Our US subsidiary, BlueVoyant Government Solutions, operates under a Small Business Innovative Research (SBIR) Phase III contract with US Space Force, the US Navy, and several other US Federal organizations. BV is headquartered in New York City, NY and BVGS is headquartered in Washington D.C. We specialize in Cyber Defense solutions for the global marketplace.
Caliola Engineering - OverKey®

Where do we fit in?

OverKey
- Mesh VPN
- Secure overlay network management

Company Information:

Founded in 2019, Caliola builds solutions for resilient and secure communications in anti-access area denial (A2/AD) environments. We are experts in MILSATCOM, NC3, mission planning, HF modernization, assured PNT, and non-traditional cybersecurity architectures.

Caliola supports PMW/A-170 and the MIDS Program Office, as well as US Space Force and their Coalition & International Partners. The US Air Force is currently evaluating OverKey for use in swarming collaborative munitions networks.

Technology Description / Product:

- Caliola built OverKey to radically simplify the deployment of high-assurance encryption in austere environments.
- OverKey is the only mesh VPN that is designed specifically to meet the needs of the DoD and its coalition partners.
- OverKey builds on NSA-approved, quantum-resistant protocols. While competing mesh VPNs target point-to-point traffic patterns, OverKey can secure the peer-to-peer and group traffic that is required for Naval operations.
- OverKey can enable agile and resilient network architectures that securely connect Navy, Joint, and Coalition forces over 5G cellular, legacy MILSTACOM, modern pLEO SATCOM, and beyond.

Focus Areas:

- Advanced Computing and Software
  - OverKey provides a unique software-only solution for military-grade encryption
- Integrated Sensing and Cyber
  - OverKey provides secure cyber communications
- Future Generation Wireless Technology (FutureG)
  - OverKey enables peer-to-peer and group communications
OverKey is a mesh virtual private network (VPN) designed to simplify key management, network routing, and mission planning. OverKey is distinct from other commercial VPNs for two primary reasons, OverKey’s mesh network is designed to support peer-to-peer communications over heterogeneous networks rather than hub-and-spoke communications. Second, OverKey’s ability to create limitless secure communication channels in real-time and on-demand provides unmatched flexibility to its users. We envision OverKey will be used to establish secure communications in situations where dynamic key management or low-latency device-to-device communications are paramount.

OverKey’s core capabilities have been demonstrated and tested over multiple large-scale mesh networks, TRL 7. It has been the center of multiple small business innovation research topics providing funding to progress its TRL level. OverKey has operated over traditional ethernet and wireless networks as well as two commercial off-the-shelf radios, goTenna Pro-x, and the Trellisware TW-875. Caliola is seeking opportunities to work with government and commercial partners to beta-test OverKey in real-world operational environments.

OverKey was designed to be hardware agnostic and run over any routable network. This means that OverKey can operate over traditional LANs, wideband HF radio links, 5G cellular networks, and even hybrid space architectures. It has even been demonstrated over non-IP communications such as UART and Aspen Grove. To operate, OverKey only requires an operating system where it can be installed and information about the network connection. OverKey has been demonstrated on various flavors of Linux as well as Windows. We intend to expand OverKey’s capabilities to Android in the near future as well as embedded devices in the more distant future.

OverKey was designed to simplify the deployment of secure peer-to-peer communications and military-grade encryption. OverKey can form distinct virtualized LANs that segment communications while operating over the same network. This enables distinct organizations to share communication resources while guaranteeing that their communication remains separate and secure. We envision operational missions where distinct organizations meet to execute joint missions such as coalition Naval missions or local/state/national/international rescue missions. OverKey will be the mechanism that enables them to communicate securely while meeting secure and distinct communication requirements.

As part of the Space Force pitch day SBIR award, Caliola worked with AFRL to conduct a cyber vulnerability assessment. Based on AFRL’s recommendations we made updates to OverKey to continue to increase its security. Cyber security is central to OverKey’s operation and continuous research and refinements are critical to OverKey’s development.

OverKey’s next milestones include Android and embedded deployments as well as Network Address Translation (NAT) traversal. These developments will further OverKey’s ability to provide simple peer-to-peer secure communications.

Founded in 2019, Caliola builds solutions for resilient and secure communications in anti-access area denial (A2/AD) environments. We are experts in MILSATCOM, NC3, mission planning, HF modernization, assured PNT, and non-traditional cybersecurity architectures. Caliola supports PMW/A-170 and the MIDS Program Office, as well as US Space Force and their Coalition & International Partners. The US Air Force is currently evaluating OverKey for use in swarming collaborative munitions networks.
ARGOT and Roman Hydra

Technology Description / Product:

ARGOT
- Uncrackable, offline, airgap, text encryption tool
- Useful for unencrypted mediums such as the public internet or unencrypted HF TacChat
- Generation of key can occur at any echelon at any time

Roman Hydra
- Makes incompatible hardware and applications communicate
- E.g., devices on commercial internet, tactical satellites (Mobile User Objective System (MUOS)), and high-frequency radio

Focus Areas:

- Pacific Collaboration: ARGOT and Roman Hydra enable partners without common hardware and encryption resources to communicate securely with minimal pre-coordination.
- Integrated Network Systems-of-Systems: ARGOT and Roman Hydra allow current incompatible systems that have already been purchased and invested into to communicate with one another to form a resilient network.

Company Information:

Dontec creates simple solutions to complex problems. These solutions support interoperability and increase the value of existing investments.
ARGOT and Roman Hydra

ARGOT is an uncrackable, offline, airgap, text encryption tool. It is useful for unencrypted mediums such as public internet or unencrypted high-frequency TacChat. It produces encrypted messages that can be sent via any available means. It is interoperable and can be used with foreign partners reliant on cellular services like LINE and WhatsApp. Like execution checklists/proword definition documents, the messages aren't sensitive, but the codebook is. Sharing keys can be done as late as the day of the event via disk distribution. For short deployments, an hour of preparation time can be more than enough. No risk of messages being read (assuming proper use). It can encode any written message.

Tactical benefits include:
- increased survivability due to reduced need for identical equipment strings at each node
- use of local communications networks and devices without creating a military signature
- interoperability due to common encryption method across partner equipment sets
- no centrally controlled cryptographic material is needed
- users can generate keys locally

Roman Hydra allows incompatible hardware and applications to communicate. It is designed with a transport agnostic philosophy, and currently enables communications between high-frequency radios, tactical satellite radios, commercial internet, local wireless, cabled local-area network, and NIPR computers, with more channels being added all the time. It allows users to choose assets they’ll take to the field based on only range, weight, and power considerations, no longer needing to consider what equipment other participants in the network will have.

Tactical benefits include:
- increased survivability due to reduced need for identical equipment strings at each node
- allows changes of frequency range and waveform in response to battlefield conditions without loss of data and need to reconfigure network
- enables improved communications windows
- increased interoperability due to allowing currently-incompatible equipment to share data

Readiness: Initial builds for each are fully operational and can be put into use today, and further development is underway.

Integration: The technology can be easily integrated in a variety of tactical networks with minimal training and preparation.

Security: The capabilities are designed to be operated on secured or unsecured networks and will take full advantage of the network’s security measures. The Roman Hydra networks are also modular and compromised mediums can be revoked access quickly.

Further innovation: ARGOT will become easier to use in future updates, and Roman Hydra will continue to expand the number of hardware-software combinations it can bridge into the network.

Dontec was formed in 2023 and is a communications solution provider with a focus on providing simple and sustainable tools to fix real-world problems. You can reach us by email at ops@dontec.org.
**Tactical AI for (USV + UAV) Collaborative Autonomy**

Bo Ryu, EpiSci, [858-805-5608], bo.ryu@episci.com

**Technology Description / Product: Dockerized / Platform-Agnostic AI & Autonomy Algorithms**

- Autonomous Surface Vehicle (ASV) capable of hosting a UAS with autonomous Launch and Recovery System (LARS) capability for enabling mission-ready autonomy.
- Notional mission will autonomously find, fix, and track one or multiple vehicles within a predefined search area in a maritime environment.
- Manned-unmanned teaming with heterogeneous robotic systems that extend sensor and communication ranges will be provided, along with multiple eyes-on-target, earlier threat identification, improved accuracy of target fixing, and increased mission effectiveness.

**Company Information:**

- 50+ FT/PT employees and contractors
- 80+% of the team with advanced degrees in CS, EE, & AI/ML.
- Solving large-scale problems by bridging the gap between rapid advances in machine learning and prototyping, integrating, and deploying Tactical AI in next-generation autonomous systems.
- Creating cutting-edge technologies that enhance national security and growing a team built on a foundation of trust, innovation, and teamwork.

---

**Focus Area: Trusted AI and Autonomy**

Sim to Real
Maritime areas such as harbors, channels and straits require precise piloting of vehicles as they are typically congested with other surface vehicles and hazards such as docks, buoys, and bridges. Current harbor piloting systems use a human to integrate numerous inputs, including his or her sense of sight and hearing. Current ongoing research is focused on the ability to allow a pilot to perform this function while off-vessel. In both cases, a vessel is manually controlled to avoid contact with static obstacles and other moving vehicles based on the experience and estimation capability of a human pilot. To overcome the need for a human expert, an autonomous navigation solution is necessary.

EpiSci has developed a system that is able to plan a path through a harbor. The path avoids static objects that are typically found in these environments (e.g., land, decks, piers, etc.). During the execution of this behavior, the system’s sensor suite (LiDAR and cameras) detects and localizes pop-up obstacles (e.g., buoys, marine wildlife, other vessels). The system estimates the obstacle’s trajectory and plots a safe path around it, avoiding a collision. Our system is also capable of adhering to a number of maritime co-regulations, such as giving an unpowered boat the right of way and changing its trajectory to pass on the port side of a vessel that it is overtaking. In our testing, the start and/or end location was beside a dock, requiring the system to have a fast feedback loop and more careful navigation.

EpiSci is maturing our autonomy algorithms and transitioning the resulting algorithms and AlphaUSV system out of a high-fidelity simulation environment and into the real-world under various initiatives including Project Overmatch. This includes assembling a prototype of the sensor suite, integrating the sensors with an onboard computer on which the system software (SW) will run, interfacing with the navigation system of a real vessel, and evaluating its performance in a real-world environment. This effort includes the addition of a stereo camera to estimate the distance to obstacles that are not detected by the Light Detection and Ranging (LiDAR). We fuse this backup localization mechanism with the anomaly detection pipeline results. This transition also includes the collection of real-world data for the development, training, validating, and maturing of our algorithms. We are planning a series of demonstrations of the final system to be deployed on an OPT/MAR WAM-V 22 USV and to navigate in diverse real environments.

Founded in 2012, EpiSci is a cross-disciplinary AI-driven company that develops trusted, human-level autonomous technologies for defense, aerospace, and commercial applications. Its Tactical AI accelerates hardware-enabled, software-defined, human-commanded, and AI-controlled autonomy for the next generation.
**FlightWave Edge 130 Blue UAS: Long Range VTOL Drone**

**Larry Berkin COO, FlightWave, [650-204-1798], larry@flightwave.aero**

**Focus Areas:**
- Advanced Computing and Software
- Human-Machine Interfaces
- Integrated Sensing and Cyber

**Where do we fit in?**

<table>
<thead>
<tr>
<th>VEHICLE SIZE</th>
<th>VEHICLE MASS</th>
<th>COMM FREQUENCIES</th>
<th>ENCRYPTION</th>
<th>CRUISE ENDURANCE</th>
<th>HOVER ONLY ENDURANCE</th>
<th>MAX. ALTITUDE</th>
<th>MAX. PAYLOAD MASS</th>
<th>CRUISE SPEED</th>
<th>MIN. CRUISE SPEED</th>
<th>MAX. WIND SPEED</th>
<th>MAX. WIND GUST</th>
</tr>
</thead>
<tbody>
<tr>
<td>130 cm</td>
<td>1,200 g</td>
<td>900 MHz Telemetry I 2.4 GHz Data</td>
<td>128 I 256 AES</td>
<td>125 minutes</td>
<td>125 minutes</td>
<td>3,650 m</td>
<td>345 g</td>
<td>27 mis I 65 mph I 100 kph</td>
<td>11 mis I 24 mph I 40 kph</td>
<td>17 mis I 40 mph I 64 kph</td>
<td>6 mis I 13 mph I 21 kph</td>
</tr>
<tr>
<td>51 in</td>
<td>2.65 lb</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12,000 ft</td>
<td>0.76 lb</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2 ft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 ft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
- **VEHICLE SIZE:** 130 cm I 51 in I 4.2 ft W 77 cm I 30 in I 2.5 ft L
- **VEHICLE MASS:** 1,200 g I 2.65 lb
- **COMM FREQUENCIES:** 900 MHz Telemetry I 2.4 GHz Data
- **ENCRYPTION:** 128 I 256 AES
- **CRUISE ENDURANCE:** 125 minutes
- **MAX. ALTITUDE:** 3,650 m I 12,000 ft
- **MAX. PAYLOAD MASS:** 345 g I 0.76 lb
- **CRUISE SPEED:** 27 mis I 65 mph I 100 kph
- **MIN. CRUISE SPEED:** 11 mis I 24 mph I 40 kph
- **MAX. WIND SPEED:** 17 mis I 40 mph I 64 kph
- **MAX. WIND GUST:** 6 mis I 13 mph I 21 kph

**Company:** FlightWave
1617 Broadway, 3rd Floor Santa Monica, CA 90404

**Product:** Edge 130 VTOL and Payloads

**Website:** www.flightwave.aero

**Edge 20km Mission Timelapse Video:** https://vimeo.com/405239731/48e61c3bb3

**Contact info:** govsales@flightwave.aero/ (866) 359-5664
Edge 130 VTOL Long Range Drone
The FlightWave Edge 130 sUAS is a long-endurance VTOL aircraft designed for long-range mapping & ISR missions.

**2 Hour Flight Time.** FlightWave’s patented tilt-pod technology uses Thrust Vector Control to steer the aircraft without control surfaces (ie: no flaps or ailerons). This enables the Edge 130 to perform long-range, stable flights that allows the use of sensors and cameras once too sensitive for traditional drones.

**Swappable Payloads.** The Edge 130 features a swappable twist-lock payload bay that allows easy integration of different payloads - all within seconds, without the use of tools.

**Commercially Proven.** The Edge 130 is a proven commercial platform for remote aerial sensing and infrastructure inspection used by dozens of customers since 2017 that include: NOAA, FBI, Greenpeace, & Kansas City Southern (NYSE: KSU).

**Backpackable.** The Edge 130 can be taken apart or snapped together by one person with no tools in 90 seconds. Goes from case to sky in minutes.

**Blue sUAS Approved.** The NDAA-compliant Edge 130 Blue UAS has received an Authority To Operate (ATO) under the DoD Defense Innovation Unit’s Blue sUAS 2.0 Program and has been placed on the Blue UAS Cleared List for US Federal agencies to purchase. [https://www.diu.mil/blue-suas-2#Edge130](https://www.diu.mil/blue-suas-2#Edge130)

---

**About FlightWave**
FlightWave Aerospace Systems Corporation is a leading manufacturer of dual-use VTOL drones, sensors and software solutions located in Santa Monica, CA. FlightWave designs and manufactures the Edge 130 VTOL drone and payload cameras for the commercial, defense, security, and intelligence markets. The fully autonomous Edge 130 sUAS has the best flight endurance in the industry and with AI edge compute capabilities provides superior aerial data capture to both the commercial and defense markets. Contact: [govsales@flightwave.aero](mailto:govsales@flightwave.aero)

*FlightWave* 1617 Broadway, 3rd Floor Santa Monica, CA 90404 [www.flightwave.aero](http://www.flightwave.aero)
**Technology Description:**
- Platform supports integration and control of person and non-person identities
- Solution provides capability to determine if an entity is authorized to access a resource - granting authorized entities access while denying access to unauthorized entities.
- The ICAM architecture will support integration with other enterprise ICAM
- Supports OMB shift toward requiring identity-focused approach to privacy and security.

**Company Information:**
- Nav Singh, Fornetix, [808.220.1450], nsingh@fornetix.com
- Chris Ward
  Senior ICAM / ZT Growth Director
  General Dynamics Information Technology
  3150 Fairview Park Dr | Falls Church, VA 22042
  (m) 703.328.5566
  chris.ward@gdit.com
Edge ZT/ICAM Capabilities Powered by VaultCore®

The United States and Coalition allies operate in a diverse environment with numerous challenges, but creating a consistent systems infrastructure based on Zero Trust should not be one of those problems—and it no longer has to be. Fornetix has partnered with General Dynamics Information Technology (GDIT) to provide a consistent means of delivering secure, integrated data across networks and systems. In support of USARPAC’s efforts, Fornetix and GDIT provide their Edge ZT/ICAM platform.

The Edge ZT/ICAM platform is the identity foundation for implementation of full Zero Trust Architecture. The Fornetix Edge ZT/ICAM solution provides warfighters with the ability to share data securely with mission partners on the battlefield. It aggregates identities from disparate data environments and stores identity data using a standardized schema. With Edge ZT/ICAM, mission commanders have a common identity repository informing them and with whom to share mission critical data, even when the partners come from outside our own environment.

**Edge ZT/ICAM Platform:**

- Allows for enhanced integration of coalition mission partners by orders of magnitude compared to current siloed identity solutions
- Provides secure integration and control of both person and non-person identities
- Provides capability to determine if an entry is authorized to access a resource, granting authorized entities access while denying access to unauthorized entries (known as Attribute Based Access Control or ABAC)

Unique to the Edge ZT/ICAM solution, the ABAC Policy Decision Point is protected inside a FIPS 140-2/3 cryptographic boundary that ensures the highest levels of encryption and security— including quantum resistance. The FIPS crypto boundary provided by VaultCore provides a means to control device identity represented by keys, certificates, secrets, and other security objects. This control extends support into deployed applications, systems, and network services.

Fornetix Edge ZT/ICAM solution and VaultCore platform were designed from inception to support multiple deployment architectures that include both centralized deployments and remote deployments, while being able to scale accordingly with Small/Medium/Large/XL configurations that mix and match. Further, devices deployed away from the central repository can function when the link to the central repository is unavailable or degraded based on the last shared set of policies and configurations. When connectivity is restored, the remote units will update all policies and configurations and operate using those new parameters.

By enabling secure data sharing and access control of resources in the field, Edge ZT/ICAM and VaultCore support the warfighters’ need to access mission-relevant data and make data-driven decisions in the field to drive victory.

---

**Figure 1:** DOD Tactical ZT / ICAM with a Centralized Identity Platform

© 2023 Fornetix
BLOS Communications Through Control of the Sky

John Edwards, Fourth State Communications, [760-218-8302], jedwards@4thstatecommunications.com

Technology Description / Product:
Enhanced Thermo-Scatter System (ETSS): Resilient backbone that connects end-users in denied and degraded environments by conditioning the upper atmosphere resulting in BLOS HF, VHF, and UHF Communications Extension and Timing Dissemination
- HF, VHF, and UHF Communications Range Extension
- Timing Dissemination
- Minimal Infrastructure Required
- Data rate up to 200 Mbps
- Range up to 2000 miles

Where do we fit in?
- Integrated Network Systems-of-Systems
- Joint All-Domain Command and Control (JADC2) in a Satellite Denied Environment
- BLOS Communications Across Pacific Island Chains with Minimal Infrastructure

Company Information:
Fourth State Communications is headquartered in Cheyenne, WY with expertise in atmospheric modification and space weather monitoring via hardware and software solutions and associated data dissemination.

Fourth State Communications
750 Road 138, Cheyenne, WY 82007
John Edwards, CEO, jedwards@4thstatecommunications.com
Levi Kunkel, CTO, lkunkel@4thstatecommunications.com
Enhanced Thermo-Scatter System (ETSS)
BLOS Communications Through Control of the Sky

The ETSS is the high-speed, omnidirectional, low-cost, resilient over-the-horizon (OTH) Beyond Line of Sight (BLOS) communications solution that will allow the United States Navy and Department of Defense to have complete backhaul link ownership with limited infrastructure investment in support of Joint All-Domain Command and Control (JADC2) in a Satellite Denied Environment across USINDOPACOM and beyond.

The ETSS consists of a High-Frequency (HF) Pump able to manipulate the Thermosphere in order to make it more reflective to HF, Very-High Frequency (VHF), and Ultra-High Frequency (UHF) communications signals. Due to the altitude of this reflective layer, the ETSS has the ability to transmit and receive communications over 2,000 miles.

The ETSS is currently being developed to meet its Minimum Viable Product (MVP) stage corresponding with TRL7 under a SBIR Phase II sponsored by AFWERX and Air Force Special Operations Command (AFSOC). Previous RTD&E has been supported by the US Air Force through several rounds of SBIR funding taking it from Proof of Concept, to Prototype, to MVP over a three-year period. Once the MVP has been established the ETSS can be quickly reproduced anywhere in the world.

Integration of the ETSS into existing tactical and strategic networks can be accomplished via Fourth State Points of Presence or through slight modifications to existing radio equipment in the form of directional antennas and increased power output. There is no need to replace existing assets already in use by the DoD.

The next stage in development is to get the ETSS to a full operational capability (FOC) where it will offer 24/7 backhaul capability while reducing its Size, Weight, and Power (SWaP). We envision the ETSS being deployed across USINDOPACOM and all other strategic DoD sties.

Fourth State Communications is a Service-Disabled Veteran-Owned Small Business headquartered in Cheyenne, WY. We specialize in atmospheric weather monitoring, worldwide reporting, and modification.

POC: John Edwards, CEO
jedwards@4thstatecommunications.com
760-218-8302

CAGE Code: 8AYQ1
UEI: NFT8U57QWUL5
Open-Source Supply Chain Intelligence with FEWSION

Where do we fit in?

FEWSION is a supply chain intelligence data fusion tool providing decision advantage for both planning and response.

This tool is a visualization dashboard providing real-time awareness and decision making in operational planning. It helps operators visualize multiple data supply chains fused into a meaningful operational picture.

This tool will enable operators to visualize logistics patterns, vulnerabilities, and better plan and respond to operational challenges and missions. It will also equip operators to build partnership capacity across regions by identifying the supply chain stakeholders and locations that are most critical for each operation and those that might be affected by a given scenario.

Current System Capabilities:
- Fuses multi-sourced supply chain data to show global supply chains and infrastructure, including sources, storage, routing, mode of transport for all kinds of goods, including fuel, food, equipment
- Incorporates pre-assembled data for immediate real-time visualization and analysis
- Built-in analysis of network hotspots, hubs, vulnerabilities, concentrations, on the supply chain network
- Both strategic “mesoscale” and tactical “last mile” data for multiple countries are available; US mesoscale data is in the public viewer “FEW-View”
FEWSION: Purple Team Technologies + Northern Arizona University

Technology Overview:
The FEWSION system is a supply chain and critical infrastructure data science platform that fuses many open-source and private data to create the world’s first complete “top-down” picture of how goods and services are flowing between facilities, cities, and nations. This data platform and the associated visualization and analysis capabilities provide a basis for both protecting and attacking supply chains, and for solving the problem of resilient supply and infrastructure networks. This is a dual-use technology that has already enabled significant breakthroughs in network science and supply chain resilience engineering.

Technology Description:
FEWSION employs a scientific workflow and the largest civilian supercomputers to bring together 50+ open-source datasets into a supply chain and critical infrastructure data model that describes the world’s flows of supplies, including energy and water. A visual analysis engine then makes this information accessible to non-experts to create situational awareness for their tactical and strategic decision making. Nothing like it existed before the 2019 prototype was launched; see the public version at https://fewsion.us.

Logisticians in the military and the private sector have visibility (at best) into their own immediate network of push and pull supply, and into their own localized infrastructure dependencies (e.g. power). But, as we have experienced in 2020-2022, resilience requires that we consider our place in the complete global network, because problems and vulnerabilities often lie elsewhere in the system. FEWSION is building the first complete picture of that global system from the “top down”, with both tactical and strategic applications.

FEWSION Offers Top-Down Strategic Supply Chain Data Science Developed Through Research Grants at NAU

<table>
<thead>
<tr>
<th>Aggregate and Correlate SCM Data</th>
<th>Comprehensive Data Model</th>
<th>Open-Source Datasets</th>
<th>Advanced Supply Chain Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current Capabilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Advanced analytics of supply chain resilience, dependency, vulnerability, environmental dependency</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Infrastructure Analysis: Analysis of infrastructure that support supply chains</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Comprehensive supply chain data model and data fusion workflow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Supply chains represented at three levels of granularity in space and by category</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Open Source: Incorporation of more than 50 open-source datasets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Automated report and supply chain data output for power users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• &quot;FAR&quot; (FEWSION for Resiliency) user training course that teaches supply chain concepts and tools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• API for data query</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• High Performance Computing (HPC) computation on university clusters and Pittsburgh Supercomputing Center Bridges-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Al/ML employed for gap filling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Proof of concept on &quot;last mile&quot; facility level supply chain modeling in foreign countries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Funded by NSF, USDA, JARPA as a basic science capability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Routine enterprise data security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Validation of methods and findings in peer-reviewed journal articles</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Technology Readiness Level (TRL)**

- Current State
- Future State
- TRL 7 for all capabilities: ready-to-deploy at scale and in full-funded operations

**50+ Open-Source Datasets Modeled**

- County Data
- U.S. Census Population Data
- U.S. Department of Commerce
- Bureau of Labor Statistics
- U.S. Department of Agriculture
- U.S. Department of Agriculture National Agriculture Statistics
- U.S. Department of Agriculture Agricultural Research Service
- U.S. Energy Information Administration
- U.S. Environmental Protection Agency
- U.S. Department of Homeland Security
- U.S. Department of Energy

**Future State: 12-24 Months**

- Implementation of certified data security
- Incorporation of controlled and classified data
- API integration with Priority5 interface
- Implementation of "last mile" supply chain models for as many countries as funded
- Proto两类ing of near-real time supply chain estimates and departure-from-baseline analysis
- Prototyping of Al/ML near-term predictive forecasting
- Government license TBD
- Veracity and precision ratings using the DoD’s own methods framework
- Field demonstration in partnership with DoD operations

TRL 1-2: Basic Research | TRL 3-4: Research to Province Feasibility | TRL 5-5: Tech Development | TRL 6-6: Tech Demo | TRL 7-8: System Development | TRL 9-9: System Test, Launch, Ops
QuSecure

Include Picture(s) / OV-1

Technology Description / Product:

1. QuProtect
QuProtect is an enterprise SaaS for managed cryptography. It is optimized for compatibility with today’s and yesterday’s technologies and easily deployed across servers to all end devices. QuProtect allows for easy, safe, low risk post-quantum transition, crypto-agility and active defense.

2. Quark & QSL
The foundational core of our SaaS solution, the Quark is a central, post-quantum secure orchestration hub that enables secure connections and control over those connections. This is the only piece of hardware in our QuProtect solution.

Company Information:
- Year of incorporation: 2019
- State of incorporation: Delaware
- Funding: Series A
- Corporation type: 2X-For Profit Organization
- D-U-N-S Number: 117366288
- CAGE Code: 8GGT0
- Headquarters: San Mateo, CA

Staff Credentials
- Top Secret Clearance (renewal pending)
- CISSP, CRISC, PMO, PMP, CompTIA, CSM
- MPA, MBA, MS, JD, PhD degrees
Scalable security
For the postquantum organization.

Protect data in motion or at rest from quantum and other emerging cyber threats on any system, anywhere. QuSecure’s comprehensive enterprise quantum security management suite, QuProtect, allows you to orchestrate postquantum secure communications end-to-end, on any device, using proprietary quantum and classical technologies. QuSecure is engaged to deliver post-quantum protections to the organization’s new secure portal.

Core Competencies
- Quantum resilience
- Quantum computing
- Cybersecurity
- Cryptography

NAICS Codes
- Primary NAICS Code: 511210
- Software Publishers
- NAICS Code: 423430 – Computer and Computer Peripheral Equipment and Software Merchant Wholesalers
- NAICS Code: 541511 – Computer software analysis and design services, custom

Staff Credentials
- Top Secret Clearance (renewal pending)
- CISSP, CRISC, PMO, PMP, CompTIA, CSM
- MPA, MS, JD, PhD degrees

Company Information
- Year of incorporation: 2019
- State of incorporation: Delaware
- Corporation type: 2X – For Profit Organization
- D-U-N-S Number: 117366288
- CAGE Code: 8GGT0

QuSecure Differentiators:

- Standardization

- Sole-source supplier
  QuSecure’s quantum security management suite, QuProtect, is the world’s only comprehensive quantum enterprise security suite that orchestrates ultra-secure communications end-to-end using a combination of proprietary software-based quantum and classical technologies in combination with NIST standards.

- Flexible access
  The only quantum-resilient products that can be accessed from the government or enterprise cloud, hybrid cloud or on-premises behind the firewall. Achieve self-aware, lightweight cryptographic protection of all legacy and new systems.

- Speed
  Hyper-fast and secure post-quantum channel drives faster throughput than Transport Layer Security (TLS).

- Maximum security
  Generate up to 60,000 randomized quantum keys per second with variable length to secure your enterprise networks with maximum post-quantum protection.
Reveal Technology: “Farsight” Edge 3D Mapping

Trevor Howard, Reveal Technology, [814-203-2662], trevor@revealtech.ai

Technology Description / Product: Farsight is a software platform that gives disconnected and distributed teams access to actionable ISR, rapid modeling, & advanced analytics at the tactical edge.

-Farsight builds maneuver-quality real-time 2D maps and near real-time 3D models. Models are available for post-processing analysis in as little as 2 minutes.
-All processing is done with no network connection required.
-Farsight is platform agnostic and interoperable with the DoD's legacy, current, and future UAS arsenal. All Farsight-produced modeling and analytics can be integrated into Android Tactical Assault Kit (ATAK) via plug-ins and shared across the tactical network.
-Analytics include: Line of Sight Analysis / AI Route Planning / Digital Elevation Mapping / HLZ Surveying / AI Measurement Tool / Terrain Analysis & Graphing

Company: Reveal Technology, Inc.
Product: Farsight
Website: https://www.revealtech.ai/
Product Overview: https://vimeo.com/598449203
Contact info: trevor@revealtech.ai / [814-203-2662]
Farsight is a software platform that gives disconnected and distributed teams access to actionable ISR, rapid modeling, & advanced analytics at the tactical edge

Farsight by Reveal Technology, Inc. (Reveal) is a software solution that provides disconnected and distributed teams access to actionable ISR, rapid modeling, and advanced analytics at the edge. By automatically processing sensor video data, Farsight builds maneuver-quality real-time 2D mapping and near real-time 3D models. Models are available for post-processing analysis in as little as 2 minutes. All processing is completed at the edge with no network connection required making it unlike any other commercial-off-the-shelf or government-off-the-shelf solution on the market.

Users can perform real-time analysis on models using Farsight’s artificial intelligence (AI) toolkit. Available analytics include:

- Line of Sight Analysis
- AI Route Planning
- Digital Elevation Mapping
- HLZ Surveying
- AI Measurement Tool
- Terrain Analysis & Graphing

Farsight is platform agnostic and interoperable with the DoD’s legacy, current, and future UAS arsenal. All Farsight-produced modeling and analytics can be integrated into Android Tactical Assault Kit (ATAK) via plug-ins and shared across the tactical network.

Through research and development alongside the DoD, Farsight is designed to have an easy to learn interface, require minimal integration, and be customizable depending on mission requirements.
Silvus Technologies is committed to providing the most technically advanced, easy to use Mobile Ad Hoc Network solutions on the market.

Leveraging its roots in cutting-edge DARPA-funded research, Silvus Technologies developed StreamCaster, the world’s first family of Multiple Input Multiple Output (MIMO) enabled Mobile Ad Hoc Networking (MANET) radios.

Unlike legacy MANET systems which are based on the 802.11 (WiFi) waveform, StreamCaster radios utilize Silvus’ proprietary Mobile Networked MIMO (MN-MIMO) waveform which was developed specifically to deliver unprecedented range, throughput, and robustness in harsh tactical conditions characterized by long range, unpredictable terrain, high mobility, and electromagnetic interference.

Where do we fit in?

Today, StreamCaster radios are enabling a multitude of use cases across military, law enforcement, unmanned systems, airborne ISR, maritime, broadcasting, firefighting, commercial services and more.

Company Information:

- Founded in 2004 by UCLA Professor Babak Falsafi
- 18 years of experience performing more than 3 dozen government R&D contracts with over $75M in R&D contracts
- Proprietary waveform not based on Wi-Fi protocols
- Secure solution including AES 256 / FIPS 140-2, Level 2
- Los Angeles HQ and production, San Diego RF design lab
- Rapidly becoming the mesh radio of choice for wide range of organizations across the globe
SILVUS TECHNOLOGIES, INC.

Silvus Technologies is proud to introduce its Mobile Networked MIMO (MN-MIMO) technology to the Unmanned Systems Market. MN-MIMO is the result of more than 15 years and $55M of Research and Development, funded by the US Government. MN-MIMO utilizes the latest advances in military technology to provide wireless video and data communications in the harshest of environments where traditional systems fail. Touting COFDM modulation, up to 4x4 MIMO, and mesh networking capability, MN-MIMO has been proven to provide longer range, better reliability, and higher data rates than any commercial or military wireless standard available today. Silvus has developed a versatile datalink that delivers unprecedented throughput, range and robustness to UGV and UAV communication scenarios, from air to ground to sea and everywhere in-between.

StreamCaster radios feature MN-MIMO at the core. 2 radios join to form a robust, long-range, bidirectional datalink, supporting video, C2, telemetry and any other form of IP data. When a 3rd radio is powered to the same frequency, they join to form a fluid, self-healing, self-forming mesh network. Each radio can act as a repeater for its neighbors, enabling advanced swarm and relay missions.

UNMANNED AERIAL SYSTEMS

StreamCaster radios equip your teams with reliable bi-directional UAV communication for highspeed data and high-resolution video transfers in unpredictable environments. Traditional Tier 1 and 2 systems use separate line-of-sight communications links for video and C2. These systems often have trouble maintaining connectivity when flying at lower altitude in high scatter or non-line-of-sight environments. Silvus' robust RF and proprietary networking protocols provide a self-healing, self-forming mesh network that self-optimizes, requiring no operator involvement.

UNMANNED GROUND SYSTEMS

Robotics missions require dependable communications that perform reliably in scenarios where operator involvement ranges from impractical to impossible. Silvus StreamCaster radios excel in non line-of-sight tele-robotics missions in harsh urban environments and remote locations. Penetrate deep into buildings, culverts and other complex structures at a safe distance with a bi-directional signal that automatically shifts between 15+ discreet operating modes to adapt dynamically to changing channel conditions.

UNMANNED SURFACE SYSTEMS

StreamCaster radios are able to harness signals reflected on the water to increase the reliability and robustness of surface communications. What was previously a cause for interference is now an asset that increases range, throughput and reliability for real-time transmission of video and data. With self-healing self-forming mesh network capability, Silvus radios are a flexible solution for multi-vessel operations.
**Synthetaic RAIC**

Technology Description / Product:
RAIC (Rapid Automatic Image Categorization) leverages cloud architecture to provision computational resources required to handle and execute: a data ingestion pipeline, low-latency queries, and automated AI model training. First, a data ingestion pipeline executes the following processes: 1) ingests all available (unlabeled) data, 2) trains a domain-specific generative AI in an unsupervised manner using available data and adversarial machine learning techniques, 3) builds out a searchable RAIC-space using the resulting generative AI and 4) projects all (real) datasets of interest into RAIC-space. Then, RAIC-space is built out for the data domain, which enables the user to carry out graph queries. Lastly, through a “human nudge,” AI models can be trained on the fly (across multiple objects in additional applications), using the image projections in RAIC-space.

Company Information:
Synthetaic, Inc. — 505 Wells, Street, Suite 2A, Delafield, WI 53018
Duns: 117484388 Cage: 8KKV6 UEI: KYPYWS21A6B6

Founded in 2019 out of Wisconsin, Synthetaic’s vision is to fast-track the world’s transition to practical AI where human labeling is no longer a time and budgetary barrier to AI development. We build high-performing AI solutions in minutes, not months. Synthetaic combines unsupervised and generative techniques with our end-to-end AI pipeline to rapidly train and deploy AI models that outperform the speed and accuracy of traditional approaches. Our solutions have been applied to critical use cases across industries, including healthcare, geospatial AI, security, and conservation.
HOW RAIC WORKS - RAPID AUTOMATIC IMAGE CATEGORIZATION

AI in 60 seconds.

RAIC enables users to build an AI from scratch in minutes without requiring labeled data. Users can simply provide a single object image to begin the process. RAIC then finds other similar objects in an unlabeled dataset and the results from this search are then contextually associated to the original starting image so that the user can improve the AI by identifying the best results through an intuitive human nudge tool. From this, RAIC learns the dataset and can build an AI to perform detection, classification, or even export labeled data.

SYNTHETAIC.COM/CONTACT
Cooling Shirts for Navy Shipyard Welders (CoolAire™)

Girish Srinivas, PhD, MBA | CEO, TDA Research Inc | 303-940-2321 | gsrinivas@tda.com

Technology Description / Product:
TDA's patented cooling shirt technology (CoolAire™) drastically improves sweat evaporation efficiency to cool the wearer, even in hot and humid environments. TDA’s cooling shirt is worn under personal protective equipment (PPE) and uses a lightweight fan to blow air through small channels sewn into the shirt (improving the mass transfer coefficient).

The CoolAire™ shirts are lightweight (< 3 lbs including all electronics), durable, have long lasting batteries (>4 hours) that are swappable for long term use. TDA’s shirts don’t restrict mobility in any way, and they are intrinsically self regulating, so they never over cool the wearer.

TDA’s cooling shirt works in all temperature / humidity conditions found on earth and has been shown to significantly reduce core body temperature over long periods of time. TDA tested its shirts at the National Personal Protection Technology Laboratory (NPPTL) and showed core body temperature reductions of up to 2.3°F during a 90-minute test (a huge reduction that can be the difference between someone suffering heat stroke vs. merely being uncomfortable).

Where do we fit in?

Focus Area: Personal Cooling and Personal Protective Equipment (PPE)
- Many DoD jobs require personnel to wear personal protective equipment (PPE) for safety reasons
- Unfortunately, PPE introduces a new risk the wearer, heat related illness
- TDA’s cooling garments are worn beneath the PPE and significantly reduce the risk of heat related illness
- These cooling garments improve worker comfort and safety

Company Information:
TDA Research Inc. was founded in 1987 and is based out of Golden Colorado. The company has a ~120 employees (about 1/3 of whom have PhDs) with a diverse set of backgrounds including Chemists, Chemical Engineers, Mechanical Engineers, Physicists, Electrical Engineers, and Material Scientists.

TDA develops and manufactures advanced materials, chemical processes, sensors, personal protective equipment, and advanced aerospace and military hardware. With our diverse team and wide range of experiences, we can develop technology in nearly any field.
TDA Research Inc—CoolAire™ cooling garment for workers in hot environments

Girish Srinivas, PhD, MBA
CEO (gsrinivas@tda.com)

TDA Research has developed a cooling shirt (CoolAire™) for naval shipyard welders to protect them from heat related illness and improve worker safety and efficiency. Shipyard welders are extremely susceptible to heat related illness (caused by excessively high core body temperature) since they are frequently in hot / humid environments. The welders must wear heavy personal protective equipment (PPE) to meet welding safety standards, which prevents sweat evaporation from cooling them down. Thus, heat related illness (such as heat exhaustion or heat stroke) can quickly set in if the welder stays in that environment for any significant amount of time. So, naval welders take frequent breaks to prevent heat related illness. They need an active cooling system inside the welders PPE that will prevent the welder from overheating and that allows them to work for longer periods of time, improving worker comfort, safety, and efficiency.

- TDA’s cooling shirt was successfully tested on a sweating thermal manikin at the National Personal Protective Technology Laboratory (NPPTL) but needs additional testing with potential end users. We are currently in the process of setting up a garment manufacturing line to expand production.
- TDA’s cooling shirts will help improve safety, comfort, and efficiency during maintenance and training. There is considerable danger in maintenance and training in very hot / humid environment with risk of heat related illness. TDA’s cooling shirt reduces this risk.
- There is no micro-controller and no internet access, so TDA’s cooling garment is completely cyber hardened.
- TDA is investigating methods for improving air flow distribution across the body.

TDA Research Inc (tda.com) is a technology development company based in Golden Colorado with approximately 120 full time employees, primarily mechanical, electrical, and chemical engineers, and chemists (34 of whom have PhDs). We’ve been in business for 35 years and specialize in a huge range of technical fields including catalysts, sorbents, chemical processes, personal protective equipment, medical equipment, military devices, and sensors.
Our mission is to further the use of small unmanned aircraft systems (sUAS) technologies to serve the civil and military missions of the Corps of Engineers. sUAS technology = cheaper, faster, safer. Data include both active and passive systems. Environmental characterization for remote sensing, geospatial analyses, and innovate sensor integration. Miniaturization of sensors, autonomous aerial imagery, the capability to access difficult or hazardous areas, and the optimization of data processing algorithms. Geospatial Research and Engineering: analytical support using emerging technologies for USACE military installations with respect to geospatial analysis, such as for assessing climate change impacts and ISR. USACE R&D: geospatial data development, analysis, management, and integration to support work units in EMRRP, EWN, DOER, NRDAR, APCRP, RSM, DOTS/DIGS, WOTS, FRM, HQ. Includes advanced data collection, processing, and analysis techniques, such as manned airborne and UAS LIDAR data, multispectral imagery, and hyperspectral imagery for modeling/visualization, site characterization, surface analysis, change detection, and monitoring assessment.

Where do we fit in?

Focus Areas:
- SUAS Standards, Training, and Oversight
- Military Engineering/Warfighter Support
- Disaster Response/FEMA
- Civil Works/levees/dams
- Rapid deployment of SUAS for environmental characterization
- Integration of COTS and custom payloads
- 35+ SUAS in operations
- Ability to fly on installations, CONUS, OCONUS
- Multi-modal Data Collections
- Infrastructure Inspections
- Data collection, extrapolation, interpretation, analysis

Company Information:

- Jenny Laird, ERDC UAS PM
- EL UAS Team Lead, ATPM
- US Army Corps of Engineers
- US Army Corps of Engineers (USACE)
- Mobile: (804) 928-5595
- mark.p.wetsel@usace.army.mil

UNCLASSIFIED
Using unmanned aircraft systems to map installation assets, maximize efficiency of time and cost, as well as minimize risks associated with employee safety.

The U.S. Army Engineer Research and Development Center’s Environmental Laboratory, utilized unmanned aircraft systems (UAS) to conduct an infrastructure assessment of the ERDC-Vicksburg installation, part of a collaborative effort with ERDC’s Directorate of Public Works (DPW), Installation Support Directorate and Army Geospatial Command. The project was initiated to fulfill a requirement for the BUILDER™ facility condition assessment of roof inspections. This involved the need to update GIS data for the entire installation and also the awareness of other Operations Orders and Directives.

For this facility application, the UAS will collect high resolution photographs to create an overall orthomosaic image of the entire installation along with thermal imagery for energy assessments – such as detecting excessive heat loss in buildings. The team is collecting high-quality geospatial data on all real property assets within the ERDC’s 700 acres.

This is a major USACE strategic and tactical application for the facility maintenance program. As funds become available other ERDC facility locations can utilizes and benefit from it.

Data Product Utilization:
• Contour Line for Elevation Uses
• Digital Surface Models (DSMs)
• Digital Elevation Models (DEMs)
• 3D Models of Buildings
• Utilities Locations
• Future Construction Support

Team Members:
Kenneth Matthieson, Shyla Hammond, Barry Barnett, Scott Bourne, Sam Jackson, Robby Boyd, Justin Wilkens

POC:
Jenny Laird
Jennifer.G.Laird@usace.army.mil
502-234-2014
Visual Positioning System (VPS) w/ Targeting

Technology Description / Product:
Visual Positioning System (VPS) - Gives manned and unmanned systems the ability to navigate and target areas where GPS is denied or spoofed. VPS does this with on-the-edge computing using a global geo-rectified 3D map database that feature-matches the platform’s FMV feed. The result is navigational accuracy of less than 5 meters and a targeting accuracy less than 2 meters. Others say they can operate in a denied GPS environment, but they lack accuracy, targeting, and automation and require operator control resulting in a very degraded capability.

- No degradation Swap-C
- Can be applied to an existing fleet with little to no hardware modifications
- Day/night operations
- Target tracking and geolocation in GPS-denied environments
- VPS Software is Sensor & System Agnostic

Where do we fit in?

Focus Areas: Trusted Artificial Intelligence (AI) and Autonomy
- Fully autonomous with navigation and targeting
- Can not be Jammed / Spoofed or Detected
- Ground to air platforms
- Autonomous ISR
- Autonomous Logistics delivery

Company Information:
CAGE Code: 8D6Y0 NAICS: 54171

Chris Pickett Director of BD, cpickett@getvermeer.com, 931-249-6789
Vermeer’s Vision Positioning System (VPS) is a payload module that allows manned and unmanned systems, from ground to air, to operate in contested environments. The vulnerability of GPS technology poses a significant challenge to the use of drones and unmanned systems in anti-access and area denial (A2/AD) environments. VPS could be used with Armed VTOL for autonomous strikes and with autonomous logistics, ship to shore. Our VPS payload offers a solution by enabling any platform to determine its absolute location in contested, spoofed and GPS-denied environments. Furthermore, our system allows for targeting in compromised GPS conditions. Our system does this in real-time by comparing the video feed from our VPS Payload with pre-mapped 3D terrain stored locally on the platform for unparalleled navigation capabilities. The system is totally passive and cannot be exploited.

VPS Air (day) can be purchased today and has been tested on Group 1-3 UAS with over 70 flights to date. Currently testing on Group 4 fixed wings at > 10000 ft AGL.

- VPS for aerial platforms, is at a TRL 8 for daytime operations. Night operations are expected to be ready by the Fall of 2023. Complete VPS TRL9 is expected by the end of the year.
- Current production quantities are 10 per month. A ramp-up period of 60-90 days could increase volumes to 100+ a month
- VPS can be used on ground vehicles and on Soldiers’ End-user Devices
- VPS is ATAK compatible
- VPS works like a GPS puck providing coordinates seamlessly in the background to systems that need it. Training would require less than 4 hours
- VPS does not connect to the internet. Map database loaded onto the hard drive would need to come from a trusted source. All components to VPS are NDAA compliant.

Vermeer’s HQs is in Jackson Heights, NY. Vermeer has its roots as a successful commercial drone cinematography solution company, Aerocine Ventures, from about 2016 supporting major Hollywood productions. We have expanded in the last 4 years to a DOD Company after winning the USAF TechStars Program for UAS and Multiple SBIR phase 2. We have a team of 25+ building Mixed Reality (MR) and AI tools to support the Defense, Space, and Multiple Commercial industry sectors. Looking to advance and participate in the autonomy effort.
Hydrogen Powered Group 2 VTOL Tactical UAS

Technology Description / Product: The Z1 hydrogen-powered group 2 tactical UAS provides advanced tactical utility for users focused on expanding sensor fusion, mission utility, Agile Combat Employment (ACE), and on-station affordability.
- 12+ hr endurance w/ 5kg, 100W payload
- 20+ hr endurance w/ min mission payload
- 5 kg mission payload/releasable package while remaining 55lb GTOW
- Hydrogen electric powered, toolless < 1-minute H2 refuel
- 1000+ hr system Time Between Overhaul
- Toolless < 5-minute assembly time, < 1-minute payload swap, < 1-minute CG config.
- Multiple payload locations, each compliant to USSOCOM MOD Payload
- Fully autonomous flight ready
- Less than 200m expected acoustic detection range
- CANbus architecture reports onboard system diagnostics and faults real-time
- AS9100 certified production ready
- Configurable in the field with no tools or software modifications required
- Significantly better endurance & payload capacity than other electric aircraft & significantly better acoustics and reliability than engine-powered aircraft.

Where do we fit in?
Focus Areas:
- Renewable Energy Generation and Storage
  - Next Generation Hydrogen-Powered Tactical VTOL UAS providing superior endurance capabilities in a tactically sustainable solution based upon renewable energy strategy.
- Integrated Sensing and Cyber
  - Modular Open Systems Approach (MOSA) equipped aircraft, providing advanced sensor fusion capabilities for future battlespace sensor integration

Company Information:
Zepher Flight Laboratories, Inc
www.zepherflight.com
adam.stolz@zepherflight.com
310 South Larch Street
Bingen, WA 98605

Ryan Cross, Zepher Flight Labs, 602-391-9298, ryanc@crossaero.com
Introduction
The Z1, developed by Zepher Flight Labs (ZFL) under contract with the US Government, is a hydrogen-powered Group 2 tactical UAS providing advanced tactical utility for users focused on expanding sensor fusion, mission utility, Agile Combat Employment (ACE), and on-station affordability. The cutting-edge 12-hr mission-capable UAS features a reduced acoustic signature, extended endurance and reliability, improved life-cycle costs, and increased operability for austere environments.

Z1 Characteristics
- Maximum Takeoff mass: 25kg
- Maximum Payload mass: 5kg
- Wingspan: 4m
- Ideal Loiter Speed: 40-50 kts
- Endurance: 12+ hours
- Combat Range: 480-640nm
- Propulsion System: 1,000W+ hydrogen fuel cell
- STANAG 4586 compliant GCS

VTOL Capability
Variable-pitch propeller combined with widely-spaced VTOL motors will enhance controllability while landing in challenging conditions and on moving platforms.

Additional Payloads
Mechanical, electrical, and signal connections are located around the aircraft for additional mission payload integration. The Z1 is designed to US SOCOM Mod Payload standards.

Modularity
Airframe and payload modules will be quick-releasable for changing system configuration and performing maintenance. The Z1 is modular in mechanical and avionics architectures.

Zepher Flight Labs
Zepher Flight Laboratories, Inc. (ZFL) is an engineering and manufacturing company focused on developing uncrewed and autonomous aerial vehicles (UAVs). ZFL’s mission is to enable the widespread use of drones by creating products that can scale in both manufacturing and operations. ZFL is developing the “Z1”, a 55 pound, 14-foot span VTOL drone that is powered by hydrogen fuel cells. ZFL received a government contract in 2020 to create the Z1 prototype and a second contract in 2022 to productize and deliver test articles to the U.S. Military.
Conclusion

Once again, holding the POST FX 2023 event in conjunction with the annual POST conference proved to be useful and beneficial to technology participants and visiting observers from USINDOPACOM and its allies, supporting industry, and academia.

The organizers of POST FX 2023 hope that, in publishing this report, positive interactions will continue between participants to promote innovation and build collaborative connections and experimentation to provide solutions that strengthen efforts to maintain peace and prosperity in the Indo-Pacific region.

“Mahalo” to the Honolulu Police Department, sponsors, supporters, participants, and attendees of POST FX 2023.