

Next Generation Space Defense

MilsatMagazine

October 2021



Cover image is courtesy of
Northrop Grumman

Beyond Secure Satcoms

SANTANDER
TELEPORT



PUBLISHING OPERATIONS

Silvano Payne, Publisher + Executive Writer
 Simon Payne, Chief Technical Officer
 Hartley G. Lesser, Editorial Director
 Pattie Lesser, Executive Editor
 Donald McGee, Production Manager
 Teresa Sanderson, Operations Director
 Sean Payne, Business Development Manager
 Dan Makinster, Technical Advisor

COLUMNISTS + CONTRIBUTORS

Chris Forrester, Broadgate Publications
 Karl Fuchs, iDirect Government
 Bob Gough, Goonhilly Earth Station
 Rebecca M. Cowen-Hirsch, Inmarsat
 Ken Peterman, Viasat
 Giles Peters, Track24 Defense
 Koen Willems, ST Engineering
 Mike Young, Envistacom

THIS ISSUE'S AUTHORS

John Gilroy
 Brendon McHugh
 David Presgraves
 Rafia Shabbir

DISPATCHES

Airbus + UK MOD	4
Northrop Grumman	6
Ovzon	6
Horizon Technologies	8
Space Systems Command + Sev1tech	10
EDJX + Cubic Corporation	12
L3Harris Technologies.....	5 + 14
Smartronix + Orbital Insight.....	14
U.S. Space Force.....	16
OQ Technology.....	18
Orbital Micro Systems + Thomas Keating, Ltd...	18
Collins Aerospace	20
Lockheed Martin.....	20
U.S. Department of Homeland Security	22
National Reconnaissance Office	22
Microsemi / Microchip	31
GSR Update: USSF Status Report	35

FEATURES

Space Access The Nation Can Rely On.....	24
Author: Space Systems Command (SSC)	
Space-Faring Nations Look to Cislunar.....	26
As Next Space Frontier	
Author: Space Systems Command (SSC)	
Government Satellite Report: EM&C	28
Author: Ryan Schradin, GSR	
A Constellations Conversation With.....	32
Justin Padilla, Kratos Defense	
SSA + SDS for Satellites	36
Authors: Brendon McHugh + Rafia Shabbir, Per Vices	

ADVERTISERS

Advantech Wireless	19
AirBorn Inc.....	9
AvL Technologies.....	11
Boeing Defense, Space and Security (BDS)	3
CPI SATCOM Products.....	13
EM Solutions, Inc. (EMS).....	15
iDirect Government.....	5
Leonardo DRS.....	17
Radeus Labs, Inc.	21
Santander Teleport.....	1
SatNews Digital.....	2
SpaceBridge	7
Wavestream.....	23

KNOW SATELLITES

FREE SatNews Subscription

www.satnews.com/reg



Cover image

Northrop Grumman's advanced, software-enabled positioning, navigation and timing payload has been developed to keep forces on target in difficult environments against advanced threats – even if the availability of existing satellite navigation systems are degraded or denied. Image is courtesy of Northrop Grumman.

MilsatMagazine is published 11 times per year by SatNews Publishers, 800 Siesta Way, Sonoma, California - 94576 - USA

Phone: (707) 939-9306 / Fax: (707) 939-9235

© 2021 SatNews Publishers

We reserve the right to edit all submitted materials to meet publication content guidelines, as well as for grammar and spelling errors, or to move articles to an alternative issue to accommodate publication space requirements, or remove content due to space restrictions or unacceptable content. Submission of articles does not constitute acceptance of said material by SatNews Publishers. Edited materials may, or may not, be returned to authors and/or companies for review, prior to publication. The views expressed in SatNews Publishers' various publications do not necessarily reflect the views opinions of SatNews Publishers. All rights reserved. All included imagery is courtesy of, and copyright to, the respective companies and/or named individuals. SatNews reserves the right to alter publication dates and print issue designations, based on industry event date changes and circumstances that are beyond the control of SatNews Publishers or the company's staff.



702X SATELLITES

**REPROGRAM
REALLOCATE
REIMAGINE**

Elevate your competitive edge with Boeing's family of software-defined satellites. With the ability to reallocate resources on the fly, the revolutionary 702X adapts to evolving market conditions, maximizes return on investment and is ready today.

boeing.com/satellites



THE UK MOD'S SKYNET 6A MILSATCOM SATELLITE PRODUCTION IS INITIATED BY AIRBUS



The UK's Minister for Defence Procurement, Jeremy Quin MP, visited [Airbus](#) in Stevenage and pushed the button to start production of the first panel skin for the UK MOD's next generation military communications satellite (MILSATCOM), Skynet 6A.



The Defence Minister started the high precision cutting machine to profile the first aluminum panels of the near six ton, Skynet 6A satellite, which is based on Airbus' Eurostar Neo telecommunications spacecraft and he also visited the extensive cleanroom facilities on site. Airbus was awarded the more than £500 million contract to design and build Skynet 6A in July of 2020 and the program achieved its Preliminary Design Review (PDR) in December of 2020.



Artistic rendition of the Skynet 6A MILSATCOM satellite, courtesy of Airbus UK.

Skynet 6A will extend and enhance the Skynet fleet. The contract signed with the UK involves the development, manufacture, cyber protection, assembly, integration, test and launch, of the military communications satellite, Skynet 6A. The contract also covers technology development programs, new secure telemetry, tracking and command systems, launch, on-orbit testing and ground segment updates.



Defence Minister Jeremy Quin MP (right) starts production of the UK MOD's Skynet 6A satellite. Photo is courtesy of Airbus.

Defence Minister **Jeremy Quin** said, "Secure military satellite communications are vital for our ability to conduct operations on a global scale. Seeing the first hardware for the next generation Skynet 6A satellite shows we are on track for launch in 2025 and ready to upgrade and enhance the UK's global military communications network."

Richard Franklin, Managing Director of Airbus Defence and Space, said, "Airbus in the UK is a world leader in the design and manufacture of military and commercial telecommunications satellites, and working hand in hand with the Defence Digital team we have overcome the challenges of Covid and are on track with the program. We also look to future export opportunities which will benefit the wider space ecosystem and are actively engaged with bringing on board a wider spread of UK SMEs to deliver this essential sovereign capability."

The Skynet 6A satellite will use more of the radio frequency (RF) spectrum available for satellite communications and the latest digital processing to provide more capacity and greater versatility than Skynet 5 satellites. The satellite will feature electric orbit raising propulsion as well as electric station keeping systems for maximum cost effectiveness.

Complete satellite integration will occur at Airbus facilities in the UK followed by testing using **National Satellite Test Facility (NSTF)** at **Harwell** in Oxfordshire supporting the [UK Space Agency](#) initiative for sovereign UK end-to-end satellite production and support.

The Skynet 5 program, provided by Airbus as a full service outsource contract, has provided the UK MOD with a suite of highly robust, reliable and secure MILSATCOM services, supporting global operations since 2003.

Airbus has been involved in all Skynet phases since 1974 and this phase builds on a strong UK commitment to space manufacturing in the UK. The program commenced by using the legacy Skynet 4 satellites and then augmenting them with a fully refurbished, ground network before launching the Skynet 5A, 5B, 5C and 5D satellites between 2007 and 2012.

The Skynet 5 program has reduced or removed many of the technical and service risks for the MOD, while ensuring unrivaled, secure MILSATCOM and innovation to UK forces.

1K FALCON IV COMPACT TEAM RADIOS ORDERED BY U.S. ARMY FROM L3HARRIS TECHNOLOGIES



The U.S. Army has ordered 1,000 new L3Harris Technologies (NYSE:LHX) Falcon® IV AN/PRC-171 Compact Team Radios to ensure soldiers at any tactical level can transmit

crucial information to command teams across an integrated network.

The Army placed its first delivery order of the Compact Team Radio, an easy-to-use and ruggedized solution leveraging robust technologies from fielded and emerging company products. This affordable radio allows voice and sensor data from all users to be shared in true Joint All-Domain Command and Control fashion, supporting the Army's connected-network vision.

The AN/PRC-171 COMPACT TEAM RADIO

continuous and reliable voice and data communications on a single battery and can seamlessly interface with other L3Harris solutions, including the Enhanced Night Vision—Binocular (ENVG-B).

The radio fully supports the Army's unified network strategy, offering a broad portfolio of waveforms that can survive through disadvantaged line-of-sight, with flexibility to upgrade waveforms as new technology emerges.



The radio's accessories are interchangeable with the rest of the L3Harris Falcon family of radios and supported with in-field upgrades to emerging wideband and narrowband resilient waveforms.

"The delivery of these single-channel radios furthers L3Harris' support of the U.S. Army's new Integrated Tactical Network by enabling all tactical operators to share situational awareness information across the entire network," said Bryant Henson, President, Tactical Communications, L3Harris. "These radios will field alongside our HMS Manpack and Leader Radios at the squad level—extending the network and warfighter effectiveness to all soldiers."

IT'S TIME TO CUT OUT THE INTERFERENCE

iDirect Government introduces CSIR™ (Communications Signal Interference Removal) NOW embedded in our 9-Series Satellite Modems, protecting your critical communications from jamming with INTERFERENCE MITIGATION.

www.idirectgov.com

iDIRECT
Government

NORTHROP GRUMMAN TO DESIGN SIGNALS INTELLIGENCE SENSOR PROTOTYPE FOR US AIR FORCE



The U.S. Air Force has awarded Northrop Grumman Corporation (NYSE: NOC) a contract to complete the design of a next-generation, open standards-based signals intelligence (SIGINT) sensor for high-altitude intelligence, surveillance, and reconnaissance (ISR) platforms.



Northrop Grumman will design an innovative, open standards-based signals intelligence (SIGINT) sensor prototype for the U.S. Air Force. Image is courtesy of Northrop Grumman.

Under the U.S. Air Force's **Global High-altitude Open-system Sensor Technology (GHOST)** program, the company will deliver a design of a prototype sensor — including airborne and ground components — with an innovative, open standards-based hardware and software architecture that can be scaled and configured to fly on multiple types of manned and unmanned Air Force aircraft.

Northrop Grumman's GHOST sensor will provide the Air Force with an agile architecture to meet today's ISR needs, while supporting rapid system enhancement, testing, accreditation and integration at the speed of relevance long into the future as the dynamic battlespace changes.

"Leveraging our SAGE technology and 45 years of SIGINT mission expertise, our platform agnostic GHOST sensor is a next-generation intelligence data collection and exploitation system," said **Ben Davies**, vice president and general manager, networked information solutions, Northrop Grumman.

OVZON T6 TERMINALS ORDERED FROM A NEW CUSTOMER WITHIN THE U.S. DOD ENVIRONS



Ovzon has received a direct order for the industry's smallest and most powerful satellite communications terminals from a new customer within the U.S. Department of Defense.



This order represents an expansion and the second new U.S. DoD customer for Ovzon in the last 90 days as the company continues to expand in its core customer base.

The order includes both the Ovzon T6 terminal for Communication-On-The-Pause (COTP) as well as the Ovzon Medium OTM terminal, an autonomously steered antenna for Communications-On-The-Move (COTM) from ground, maritime and aerial platforms.

The Ovzon T6 terminal is the latest addition to Ovzon's advanced mobility product offerings. Weighing just 13 pounds, the terminal is capable of being placed into operation by an untrained user within less than a minute.

The Ovzon T6 can send up to a minimum of 70 Mbps and receive 120 Mbps and provides an "early-entry" capability that can scale into a robust command and control node without follow-on systems or additional crew. The Ovzon Medium OTM terminals enable continuous connection to Ovzon's high-performance, global network while on the move. This integrated solution offers unprecedented agility to military and emergency organizations with no-fail missions.

"We are excited to continue our expansion with a prestigious new U.S. DoD customer. We continue our strong commitment to deliver unmatched, industry-leading performance and mobility to both government and commercial organizations with critical global communication requirements," said **Per Norén**, CEO of Ovzon.



CONNECTING OUR MILITARY TO ITS MISSIONS

ASAT II™
Tactical , BLoS
HTS System



For over 30 years, SpaceBridge has striven to provide C4I over SATCOM connectivity by being an innovator, leader, and trusted provider of bold tactical solutions in the military ground segment Satellite technologies.

We live on the cutting edge of what's possible, challenging ourselves to provide products and services that rise to the occasion. In a world of mounting unconventional threats, there is no room for failure or compromise.

We are dedicated to the exploration and implementation of new communication technologies that provide our armed forces with ultra high-performance satellite connectivity products that boast the best security, and highest availability.

Recognized by major players such DISA, SpaceBridge will continue to offer high-throughput solutions at exceptional value.

Contact us today to learn how we can connect you to your beyond line of sight missions.

SpaceBridge.com | info@SpaceBridge.com | +1.514.420.0045
USA | CANADA | LATAM | BRAZIL | EMEA | APAC

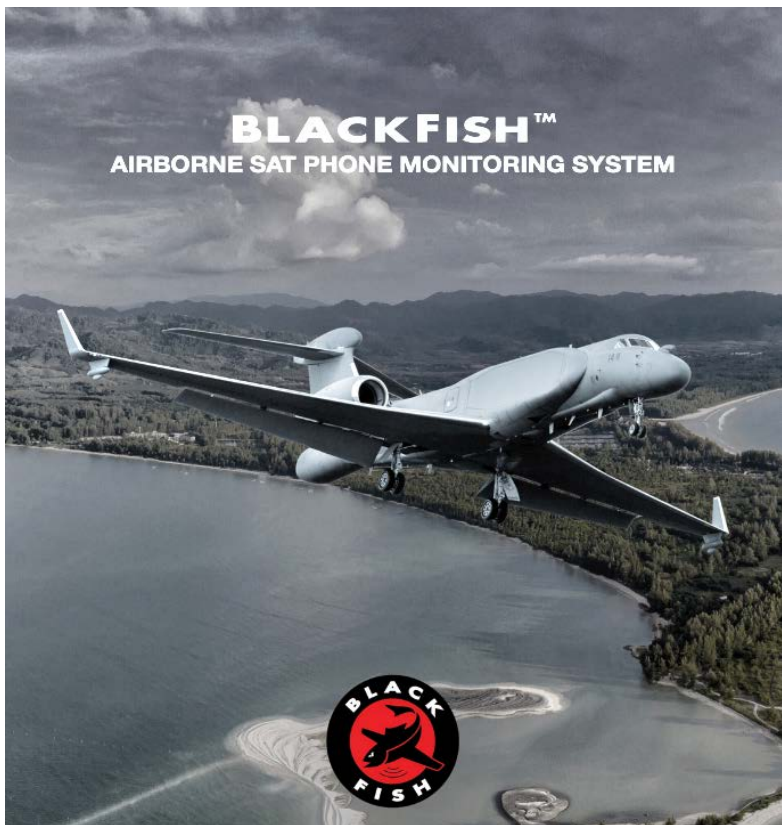


HORIZON TECHNOLOGIES CLOSES MILLION\$ SALE



Horizon Aerospace Technologies, a subsidiary of Horizon Technologies, has announced an approximately \$1 million sale of FlyingFish™ airborne SIGINT systems to a European prime contractor for a Southern European government end-user. The systems will be operated on manned ISR fixed-wing aircraft to support NATO and EU missions in the Mediterranean Sea and Northern Africa.

John Beckner, CEO, Horizon Technologies said, "We are happy to add another end-user to the list of countries who operate our FlyingFish™ and new BlackFish™ SIGINT systems. FlyingFish™ is in operation 24/7 around the globe saving refugees, combating illegal fishing, piracy, terrorism, and transshipments. There is also a great deal of interest in our upcoming Amber™ smallsat launch."



Recently, Horizon Technologies completed its Series A funding round with **Maven Capital Partners** and **Virgin Money**.

Horizon Aerospace Technologies is a leader in airborne Sat Phone monitoring systems for Intelligence, Surveillance, and Reconnaissance (ISR) applications, equipping governments worldwide by enhancing their SIGINT capabilities. The firm is the Original Equipment Manufacturer (OEM) for the FlyingFish™ BlackFish™ SIGINT systems that are in operation on numerous platforms across the globe. The company participates daily in SAR missions via NATO and FRONTEX in the Mediterranean Sea and are heavily involved in international operations around the globe. Horizon Space Technologies is the prime contractor for the UK Government's Amber™ program that will consist of Amber™ cubesats in multiple orbital planes, providing global **Maritime Domain Awareness (MDA)** data to NMIC (led by the Royal Navy).



John Beckner, CEO, Horizon Technologies, and **Bash Ahmed**, COO, Horizon Aerospace Technologies

Regarding the Amber™ satellite from Horizon Space Technologies, earlier this past summer, AAC Clyde Space (AAC) won a £4.6 million order for a full turnkey solution from Horizon Space Technologies, including two new satellite launches, operations and data delivery.





The satellites will become part of the **Horizon Space Technologies' Amber™** constellation dedicated to delivering MDA intelligence data.

The **EPIC-6U** smallsats will be able to locate and track vessels worldwide by geolocating and demodulating RF signals in a system that can be used to fight piracy, illegal trans-shipments, illegal fishing, and refugee smuggling, but can also be used for other purposes such as detecting and tracking a variety of RF emitters.

The mission delivers a commercial service and may be extended to include more than ten (10) additional Amber™ smallsats. Horizon Space Technologies' first customer is the [UK National Maritime Information Centre \(NMIC\)](#) in Portsmouth.

The two satellites in this order are scheduled for launch in the second half of 2022. This order is a follow-on order from the [Satellite Applications Catapult IOD program \(IOD-3 AMBER\)](#), for which AAC will also deliver a 6U cubesat to the **International Space Station (ISS)** in 2021 for deployment.

"We are looking forward to expanding our current partnership with AAC Clyde Space as we move forward with more launches and advanced versions of our mission payload. They are a key part of the Amber™ team," said Horizon Technologies CEO, **John Beckner**.

AirBorn



Micro D Connector Solutions

- AirBorn's M-Series Micro D connectors & cable/flex assemblies meet or exceed MIL-DTL-83513 performance specifications
- Ideal for down-hole, mil/aero, radar, communications, space applications & more
- 4 points-of-contact means ultra reliability no matter how rough the ride on Earth or space

a i r b o r n . c o m

SPACE SYSTEMS COMMAND AWARDS MILLION\$S CONTRACT TO SEV1TECH FOR DTAAS CAPABILITY



The **U.S. Space Force's Space Systems Command's (SSC) Cross-Mission Ground & Communications Enterprise (ECX)** has awarded a **cost-plus fixed fee contract totaling \$47.5 million to Sev1Tech LLC of Woodbridge, Virginia.**



The contract was awarded through the **Space Enterprise Consortium (SpEC)** Other Transaction Authority (OTA) agreement for **meshONE-T**. This prototype effort will deploy and demonstrate a **Data Transport as a Service (DTaaS)** capability for an initial set of Space Force mission partners, in support of national security objectives. It is intended to lay the groundwork for a modern, resilient, scalable, and secure data transport network able to accommodate a wide range of customers and facilitate the **Joint All-Domain Command and Control (JADC2)** vision into an operational reality.



Sev1Tech is a leading provider of IT modernization, cloud, cybersecurity, engineering, fielding, training, and program support services for U.S. government agencies and major commercial organizations and the company supports critical missions across the defense, intelligence, homeland security, health, space, and commercial markets.

Major activities associated with this award include data transport services development as well as the fielding and operations of a multi-node meshONE-T **Minimum Viable Product (MVP)**. Leveraging commercial innovation and employing industry based standards, this prototype will demonstrate secure enterprise communications, interoperability, and cloud connectivity for future multi-domain (terrestrial, air, and space) communications in support of the space warfighter.

With meshONE-T, the **ECX Data Transport** branch will assist in rapid growth of scalability and technology. When fully operational, the system will provide a high-bandwidth, intelligent, tactical-edge network connecting assets across **U.S. Space Force** and **U.S. Air Force** domains with reachability to other branches of military service, the Intelligence community, foreign mission partners, and **Advanced Battle Management System (ABMS)** and JADC2.

"Previous network architectures for weapon systems were designed to meet specific user and mission needs," explained Lt. Col. **Louis Aldini**, Materiel Leader for Data Transport. *"Future network architectures need to be integrated as well as provide enhanced capabilities and efficiencies for the enterprise. meshONE-T is focused on delivering a modernized common solution for all weapon systems."*

"Sev1Tech is excited to build on the success and continued partnership in delivering next-generation transport capabilities to operational space mission partners served by Space Systems Command," said **Bob Lohfeld**, CEO at Sev1Tech. *"We are honored to provide transformational engineering, design and implementation to Space Systems Command by delivering warfighters a modernized data transport capability to transmit and receive data securely and reliably, allowing robust Joint Command & Control across all phases of conflict."*

"meshONE-T is about the ability to get the right information to the right place at the right time. The key attributes are scalability, resiliency, and path diversity," said Col. **Rhet Turnbull**, director of SSC's Cross Mission Ground and Communications Enterprise. *"By leveraging the Space Enterprise Consortium we were able to reach a wide variety of both traditional and non-traditional vendors—and get on contract fast. A year from now we'll have an operational prototype."*

The Space Enterprise Consortium was created in 2017 through the Air Force's Space and Missile Systems Center, predecessor to today's Space Systems Command. SpEC was created to bridge the cultural gap between military buyers and commercial space startups and small businesses through Other Transaction Authorities. The OTA's innovative contracting process allows SpEC to solicit bids from a mix of member companies including companies that have not previously done work with the Department of Defense.

SSC, headquartered at Los Angeles Air Force Base in El Segundo, California, is a U.S. Space Force field command responsible for developing and acquiring lethal and resilient space capabilities for warfighters by rapidly identifying, prototyping, fielding and sustaining innovative, space-based solutions to meet the demands of the National Defense Strategy. SSC's functions include developmental testing, production, launch, on-orbit checkout, and maintenance of USSF space systems, as well as and oversight of USSF science and technology activities.

AvL TECHNOLOGIES

avltech.com



1.35M FIT

FLEXIBLE INTEGRATED TERMINAL

MANUAL POINT
OR AUTO-ACQUIRE FLYAWAY
TRI-BAND CONFIGURABLE

AvL's 1.35M FLEXIBLE INTEGRATED TERMINAL IS A FULL-FEATURED TRI-BAND (X, KU OR KA) TERMINAL WITH A COMPACT PACK-UP INTO 2 IATA CHECKABLE CASES.

Operated manually or motorized with auto-acquire, the terminal's optional AvL antenna control system automatically acquires and tracks satellite beacons with an internal receiver. The antenna is ODU and modem agnostic, and optionally provided with multiple modem options.

- ◆ Tri-band: X-, Ku- or Ka-band wideband
- ◆ Configurable with Ka-band certified modems
- ◆ Axisymmetric 1.35m 12-piece carbon fiber reflector
- ◆ AvL Cable Drive pedestal with integral base and tripod
- ◆ High-wind stability kit
- ◆ Quick band changes & multiple RF packages available
- ◆ Standard 2-port feeds & optional 3-port
- ◆ Pre-configured SSPA/LNB kits
- ◆ Optional AvL terminal power supply



Visit AvL @ IBC, December 3 - 6, Hall 5 - Stand 5.A63

STRATEGIC PARTNERSHIP FORGED BETWEEN EDJX + CUBIC CORPORATION TO LAUNCH IOMT

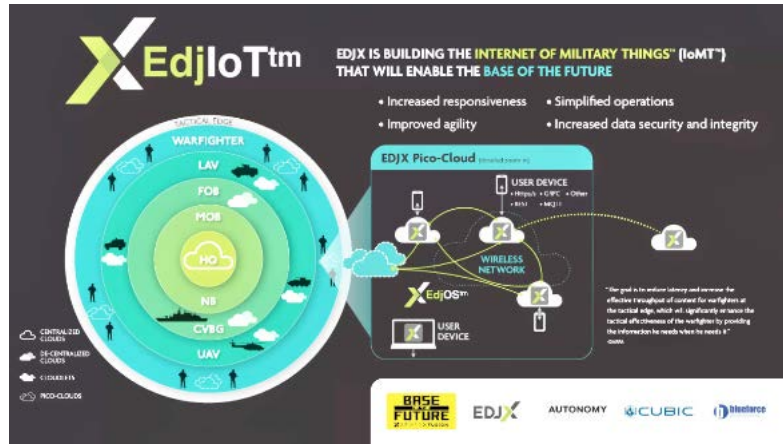


EDJX and Cubic Corporation have formed a strategic partnership to launch the world's first Internet of Military Things™ Edge Platform (IoMT).



The Internet of Military Things Edge Platform is a converged infrastructure solution consisting of **EDJX EdJOS** with Cubic Corporation's edge compute and networking hardware. **Blueforce Development** will become the first certified application developer on the IoMT Platform.

The IoMT, which has significant implications for IoT and advanced AI solutions at the far edge of the network, is the first major solution to be built on the **Autonomy Institute GRID** that includes **Public Infrastructure Network Node (PINN)**, announced earlier this year. The Autonomy Institute is the conduit for these technologies combining to form a transformational end-to-end IoT solution from base to battlefield, solving immediate challenges for the military and civilian first responders.



The IoMT Platform will launch on the **Autonomy Institute Alpha Lab** at **Texas Military Department's (TMD) Camp Mabry** in Austin, Texas, coinciding with the deployment of PINN infrastructure. The PINN is the first, unified, open standard to support 5G wireless, Edge Computing, Radar, LIDAR, enhanced GPS, and Intelligent Transportation Systems (ITS) and solves current infrastructure challenges.

THE INTELLIGENT & AUTONOMOUS INFRASTRUCTURE GRID
ACCELERATING INTELLIGENT AND AUTONOMOUS SYSTEMS NATIONAL R&D

24/7 LABS - ADVANCING INTELLIGENT & AUTONOMOUS SYSTEMS

- 5G/4G NETWORKS
- EDGE COMPUTING
- INTELLIGENT TRANSPORTATION SYSTEMS
- SITUATIONAL AWARENESS SENSORS
- NATIVE EDGE DEVELOPMENT
- ORCHESTRATED AUTONOMY
- CYBERSECURITY
- ASSURED POSITION, NAVIGATION, TIMING (APNT)
- SIMULATION & MODELING
- RESILIENT SYSTEMS & POWER (LEMP, HA)

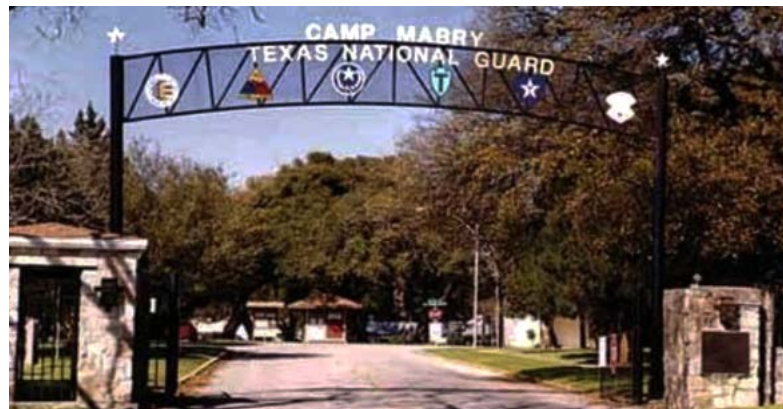
AI GRID **PUBLIC INFRASTRUCTURE NETWORK NODES** **EDGE** **EDGE DEVELOPMENT PLATFORM** **ASOCC** **24/7 OPERATIONS**

"ALL-UP" AUTONOMY REQUIRES GRIDS & CORRIDORS

Truck at the Edge

Sponsored by: **AUTONOMY INSTITUTE** 5G NR Radar Sensors E-GPS Compute Energy Microgrid Micro DC PINN

The Autonomy Institute Alpha Lab at Camp Mabry will be available to developers to build, test and deploy next generation IoT solutions providing the blueprint for public safety, military and civilian use cases. The Alpha Lab is part of operationalizing the PINN, which will have significant implications for public safety and disaster response. PINNs will enable first responders to accelerate emergency and disaster response with intelligent infrastructure and facilitate humanitarian assistance with disaster relief and domestic operations.



The IoMT Edge Platform is part of the broader future of AI at the edge and IoT story as a key proof point in an emerging market. IoT and 5G marks AI at the edge, the processing of AI algorithms on edge, on users' devices. IoMT is an emerging application of this technology, transforming military security and connectivity.

Service members and first responders make quick decisions for mission success and for the safety and security of others who depend on those decisions. These individuals operate under intermittent connectivity, weighty and complex gear, and with limited time to assess an environment before acting. The proliferation of sensors, unnamed vehicles, command posts, and mobile-enabled ground troops has resulted in a battle space that is increasingly complex and sophisticated. Edge computing enables data processing at the tactical edge by decentralizing decision-making changes, bringing the powers of data to the field, providing better information for the military and civilian first responders.

The tactical edge comprises the platforms, sites, and personnel (U.S. military, allied, coalition partners, first responders) operating at lethal risk in a battlespace or a crisis environment characterized by a dependence on information systems and connectivity for survival and mission success. Users are fully engaged, highly stressed, and dependent on their information systems' availability, integrity, and transparency.

"We are excited to support the launch of the Autonomy Institute Alpha Lab. Camp Mabry and the Texas National Guard have become a center of gravity for research and innovation. We are continually looking to leverage and accelerate the adoption of new commercial technology and novel architecture deployments like the PINNs. This Lab will help bring the concept of the Internet of Military Things to fruition by acting as a pathfinder for our systems to connect, share data, and learn. As a nation, we need to move faster if we are to meet the challenges of tomorrow," said Lt. Col. **Alex Goldberg**, Southwest Region Engagement Lead for the Defense Innovation Unit.

"The EDJX platform is a quantum leap in the field of edge computing because it enables our intelligent IoT and C2 application products to scale from base to battlefield, reducing cognitive lift while increasing the tempo of operations for members of the military and our first responders," said **Michael Helfrich**, Founder and CEO of Blueforce Development. *"Military and first responders need actionable intelligence for superior decision-making, where access to data and the fidelity of information is critical to decision-making in time-constrained decision environments."*

"Our innovative compute and networking platforms have been enabling allied forces around the world to benefit from the emerging Internet of Military Things over recent years. Our partnership with EDJX and Blueforce Development will greatly accelerate the proliferation of intelligent and autonomous solutions," said **Mike Barthlow**, SVP & GM, Cubic Mission Communications and Computing. *"We are excited to team up with EDJX, Blueforce, and the Autonomy Institute Alpha Lab at Camp Mabry to expand our vision for the safety and security for those operating at the tactical edge."*

"Launching the IoMT Edge Platform in partnership with Cubic ushers in the era of Industry 4.0 by bringing all of the key ingredients missing in the pursuit of mobile, intelligent, and autonomous systems development," said **John Cowan**, EDJX co-founder and CEO. *"Innovation will be at the heart of this project and we are excited to work with leading innovators like Blueforce and the Autonomy Institute in the effort to create the future."*



Download the CPI mobile app!

HPA RF calculator

Quickly access HPA data sheets

TWTA/SSPA product finder

Convenient contact info

Search: **CPI Satcom**



CPI Communications
& Power Industries

L3HARRIS RECEIVES U.S. ARMY HMS ADVANCED TACTICAL RADIOS FIRST FULL RATE PRODUCTION CONTRACTS



L3Harris Technologies (NYSE:LHX) has received full-rate production orders for the U.S. Army's HMS (Handheld, Manpack & Small Form-Fit) program providing advanced multi-channel, multi mission communications for the Integrated Tactical Network.



The Army awarded L3Harris more than \$200 million for the multi-channel, software-defined, **Falcon IV® AN/PRC-163 handheld Leader Radios** and **AN/PRC-158 manpack radios** that will increase warfighter effectiveness



by enabling and multi-mission networking capability. The radios also fully support the Army's unified network strategy, that will allow flexibility to upgrade waveforms as new technology emerges.

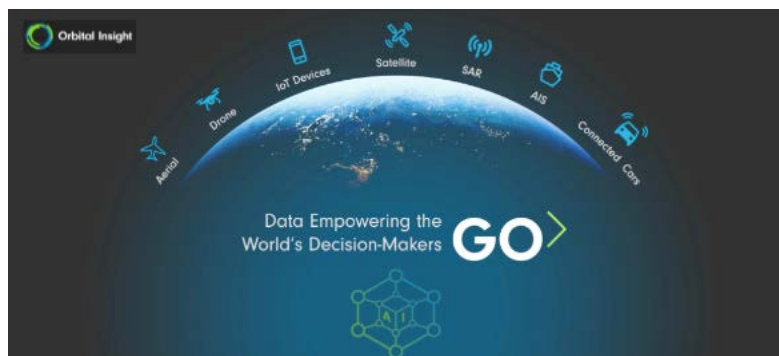
The Army's *Indefinite Delivery Indefinite Quantity* contracts for the handheld Leader and manpack radios include a 5-year base and an additional 5-year option, with a ceiling of more than \$16 billion. The Army expects to purchase approximately 100,000 two-channel Leader Radios and 65,000 HMS Manpack radios.

"The transition to full rate production is a major step forward for the U.S. Army in fielding their new Integrated Tactical Network and we are honored to support them with tactical radio solutions that make the ITN possible," said **Dana Mehnert**, President, Communication Systems, L3Harris. "Our continued performance on HMS and the ENVG-B program are the most recent examples of how L3Harris is supporting the U.S. Army's key priorities for its unified network and increasing situational awareness, mobility, survivability and lethality for our soldiers."

PARTNERSHIP BETWEEN SMARTRONIX + ORBITAL INSIGHT TO DRIVE SPACE + ISR INNOVATION ON AMAZON WEB SERVICES



Smartronix, LLC and **Orbital Insight** are partnering to accelerate mission outcomes through innovations in Space and Intelligence, Surveillance and Reconnaissance (ISR) powered by **Amazon Web Services (AWS)** cloud technologies.



Orbital Insight analyzes satellite, drone, balloon, and other unmanned aerial vehicle images, including cell phone, ship and vehicle geolocation data, to gain strategic insights from multiple sensor data. The Orbital Insight GO platform automates the most difficult steps of deriving insights allowing its customers to answer challenging geospatial questions.



Through this partnership, Orbital Insight will participate in Smartronix' Accreditation Accelerator Program, which is designed to help ISVs and solution providers achieve accreditation in a fraction of the time it might otherwise take them. This solution is built on AWS and will help Orbital Insight achieve DoD Impact Level 4/5 security controls required for data to be accessible and used by mission customers across Smartronix' C5ISR client base. Both Orbital Insight and Smartronix recognize the importance of leveraging AWS in this work.

SPACE MICRO TO DELIVER 10 NANOCOM SDRs TO LOCKHEED MARTIN FOR THE SDA'S TRANCHE 0 SATELLITE CONSTELLATION



Lockheed Martin (NYSE: LMT) has awarded **Space Micro Inc.** a contract to deliver ten, Ka-band, Nanocom™ Software Defined Radios (SDR) in support of the **Space Development Agency's** (SDA) **Tranche 0** satellite constellation — Nanocom recently passed **Critical Design Review (CDR)** and Space Micro will deliver flight models to Lockheed Martin by the close of this year.

Nanocom is a small form factor, quick-to-field, cost-effective, modular SDR designed to perform in hostile and extreme environmental conditions. Nanocom is programmable on-orbit and suitable for a variety of applications that include Telemetry, Tracking & Command (TT&C) transceiver, mission data transmitter, and Radio Frequency (RF) receiver with onboard signal processing. The flexible SDR uses **Xilinx's Zynq 7045 System on a Chip (SoC)** — [data sheet available](#)

[via this direct link...](#)), which combines dual ARM Cortex A9 cores with 350,000 programmable logic cells, capable of supporting a variety of complex wave forms and algorithms. Nanocom transmits and receives at 20 and 30 MHz, respectively, with a transmit data rate of up to 300 Mbps. Nanocom's modular design allows Space Micro to easily modify frequencies, data rates, interfaces and overall functionality to meet mission specific requirements.

Space Micro's product line of Software Defined Radios comprises several models: The **μSDR-C™** targets UHF, S-, L- and low C-band applications, while the more powerful Nanocom targets higher frequency, higher data rate and more processor intensive RF applications.

"Software-defined radios are key to offering the reprogrammability and mission flexibility our customers demand," said **Erik Daehler**, senior director of protected communications, Lockheed Martin Space. *"Space Micro's Nanocom SDR is an exciting addition to our diverse team of suppliers."*

"We are very pleased to be selected for the 10 vehicles Lockheed Martin is building for SDA's satellite constellation for their Ka-Band transceiver," said **David Czajkowski**, Space Micro CEO. *"Our decade of development of high data rate transceivers has led to the Nanocom product which supports the challenging SDA technical requirements with exceptional reliability, giving them a competitive advantage."*

EM Solutions

PROVEN, AGILE, TRUSTED TECHNOLOGY.

The trusted choice for **Government and Military Satcom-on-the-Move** on sea or land.



COBRA
MARITIME



SALAMANDER
LITTORAL



TAIPAN
LAND

TAIPAN – Type Approved for Inmarsat GX

www.emsolutions.com.au

EM Solutions is an innovative Australian company with a global focus that provides future-proof, next generation technologies.

Another First from



U.S. SPACE FORCE TO ACQUIRE U.S. ARMY + U.S. NAVY SATCOM MISSION AREAS



The Chief of Space Operations has announced the transfer of U.S. Army and U.S. Navy satellite communications billets, funding and mission responsibility to the U.S. Space Force.

Space Force General **John W. “Jay” Raymond** made the announcement at an **Air Force Association** meeting in Washington — the transfers are scheduled to be effective as of October 1, 2021, if the DoD budget is passed and signed.

“We’re one team with our sister services and over the last year-and-a-half we have worked with the Army and the Navy and the Air Force to determine which capabilities come over to the Space Force,” Raymond said. *“The intent was to consolidate (and) increase our operational capability; increase our readiness and do so in a more efficient manner.”* The changes are *“a first tranche,”* he said.

This is the latest step in building the new service. The idea behind the U.S. Space Force was *“to create a unity of effort around our space enterpris,”* said Space Force Lt. Gen. **B. Chance Saltzman**, the service’s deputy chief of space operations for operations, cyber and nuclear. Simply forming the service made the idea of looking for efficiencies possible.

“We need to create this unity of effort around our space missions, to ensure we’re up to those challenges that we face, because the space domain has rapidly become far more congested, and far more contested than ... when I was a lieutenant or a captain operating space capabilities,” Saltzman said.

The performance of satellite communications will be enhanced by this sort of unity of effort.

On the Navy side, the Navy’s narrow band satellite constellation will transfer 76 manpower authorizations to the Space Force, as well as 13 satellites — a mix of the new multi-user objective system and the UHF follow-on satellite constellation.

The U.S. Army will transfer roughly \$78 million of operations, maintenance and manpower authorizations. This will include five wideband SATCOM operations centers and four regional SATCOM support centers. This will affect about 500 manpower authorizations.



A Falcon 9 rocket launches on January 6, 2020, at Cape Canaveral Air Force Station. The rocket, carrying an installment of Starlink satellites, was the first official launch of the United States Space Force. Photo is courtesy of U.S. Air Force photo by Joshua Conti.

All told, 15 global units with 319 military and 259 civilian billets from the Army and Navy combined will transfer to the Space Force.

These are crucial defense capabilities. The units can’t stop just because the function is transferring to the Space Force. The capabilities are needed 24/7 and they will be, Saltzman said.

The move puts basically all of the DoD’s narrowband, wideband and protected SATCOM under control of U.S. Space Force. *“Now all of that— training, operations, acquisition and sustainment and follow-on activities, user allocations — all of that, will be consolidated under the Space Force to create that unity of effort, and hopefully gain the ability to be more resilient, more dynamic, and ultimately more efficient with that mission set,”* Saltzman said.

The soldiers, sailors and Army and Navy civilians are not obligated to move to Space Force. There is a process and those involved must volunteer to move. For civilians, the process is relatively easy — simply moving from an Army or Navy system to becoming Department of the Air Force employees. For soldiers and sailors, this requires release by their respective services and acceptance by the Space Force.

OQ TECHNOLOGY + GOVSAT COLLABORATING ON IOT SOLUTIONS FOR DEFENCE + GOVERNMENT



OQ Technology and **GovSat** have signed a memorandum of understanding (MoU) to collaborate on developing and testing satellite-based IoT (Internet of things) and machine-to-machine (M2M) products aimed at defence and government sectors.

By combining OQ Technology's 5G products and services with GovSat's end-to-end SATCOM solutions, already supporting customers such as NATO, the UK's Ministry of Defence (MOD) and the Belgium Navy, the companies aim to offer highly scalable applications for air, land and maritime missions across the world. Customers of these future applications will benefit from access to real-time 5G IoT coverage, dedicated geostationary (GEO) capabilities, specialized frequencies and licenses, and a wider footprint of multiple beams.

Under the agreement, OQ Technology will provide user terminals, satellite hub equipment and remote management capabilities. The company will also re-design its satellite IoT user terminal to fit the GovSat frequency band, and this will also upgrade the antenna of the user terminal. In return, GovSat will give OQ Technology access to its satellite capacity, operate the satellite hub infrastructure and provide uplink services.

GovSat's coverage is critical for government customers and NATO operations with a reach that spreads Europe, the Middle East, Africa and South West Asia, with maritime coverage for the Atlantic, Baltic, Mediterranean and Indian Oceans. Their high-powered, fully-steerable spot beams in X- and Mil Ka-Band, plus a global X-Band beam, in addition to a secure service hub, assure secure operations and resilient SATCOM capabilities.

Since its successful demonstration of the technology in 2019, OQ Technology has been working on its patent pending technology to provide global 5G IoT coverage, initially using an LEO smallsat constellation. Following the launch of its Tiger-2 satellite onboard the SpaceX Transporter-2 mission in July, the company is now offering commercial 5G IoT services for a variety of IoT applications for environmental monitoring and agriculture, logistics, maritime, smart metering, mining and oil & gas.

Omar Qaise, founder and CEO of OQ Technology said, "To successfully provide 5G IoT and machine communication to critical SATCOM applications in the defence and the government sector, it became evident that we had to partner with a specialized GEO operator. GovSat, due to its application know-how and experience of delivering secure, non-preemptible, reliable and accessible satellite communication services, is the perfect partner to achieve this."

ADVANCED EO GEMS SMALLSATS CONSTELLATION TO BE DELIVERED BY ORBITAL MICRO SYSTEMS + PARTNER THOMAS KEATING LTD.



Orbital Micro Systems (OMS) has entered into a formal agreement with **Thomas Keating Ltd.**, a UK-based THz technology firm, to advance the development of millimeter-wave instruments for deployment in OMS' **Global Environmental Monitoring System (GEMS)** constellation of cubesats. As a part of the agreement, the companies will jointly fund related design, development, and test activities, leveraging the satellite technologies expertise of each firm.

Thomas Keating has a strong success record in the last 30 years in manufacturing and testing of quasi-optical antennas for science and weather forecasting missions. Based in Billingham, England, the company works with customers across the space, aviation and materials management industries.

OMS launched the first commercial microwave radiometer weather mission into orbit in 2019 and is leveraging its experience to expand the capabilities and precision of its current generation of instruments and satellites. As a result of its collaboration with Thomas Keating, OMS expects to provide unique, highly localized Earth Observation (EO) data that will enhance real-time weather forecasting. As commercially focused space markets continue to emerge, the companies are committed to dramatically increasing the accessibility and availability of timely all-weather earth observation data for commercial and government use.

Being readied for launch in early 2022, the next GEMS2 satellites carry state-of-the-art microwave radiometers designed and manufactured by OMS with support from the **U.S. Air Force**, **U.S. Space Force**, **U.S. Navy**, **Lockheed Martin**, and the **UK Space Agency** to gather temperature, humidity, and precipitation data across 24 sounding and imaging channels at 118 and 183 GHz. These uniquely capable instruments measure vertical temperature, humidity, and precipitation profiles 24/7 in nearly all weather conditions regardless of day or night. The sensor produces a cross-track scanned 2000-kilometer-wide swath as each satellite orbits the Earth.

"OMS worked with Thomas Keating to develop a hardware solution for our first GEMS payload and the collaboration just grew from there," said **Michael Hurowitz**, chief executive officer of OMS. "We anticipate that this partnership will help streamline the design-to-launch process and bring us closer to our goal of gathering and disseminating weather and climate observations for any point on the globe in fifteen-minute intervals."

"Our two organizations are well-matched to help shape the growing space-enabled weather forecasting marketplace," said Dr. **Richard Wylde**, managing director of Thomas Keating. "The move toward lower-cost satellite platforms using precision instrumentation that can cost-effectively increase observation-revisits and data integrity will fuel a data-starved market."

Advantech Wireless Technologies Military & Government Solutions



**X-Band SSPAs/BUcs
GaN & GaAs configurations**



**Engage Class Integrated
SATCOM Terminals**



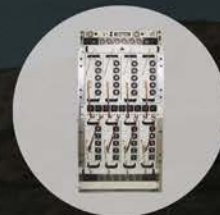
**X-Band / Ka-Band
Frequency Converters**



Troposcatter Products



LNAs / LNBs



**Solid State
Pulsed Amplifiers**

Faster & More Secure Communications for Military and Government Agencies

At Advantech Wireless Technologies, we have over 25 years of experience delivering cutting-edge innovations in communications that solve mission critical communications challenges.

We understand the challenges that government & military leaders face and our technologies empower them with the freedom to communicate quickly, reliably and securely.



COLLINS AEROSPACE RECEIVES 9TH DELIVERY ORDER FROM U.S. ARMY FOR HMS MANPACK RADIO MODERNIZATION PROGRAM



Collins Aerospace has received their ninth delivery order from the U.S. Army to provide **AN/PRC-162** ground radios for the Handheld, Manpack and Small Form Fit (HMS) program.



The AN/PRC-162 is a fully software-defined communications solution that features two, independent, channels across all frequencies for seamless voice, data, route and retransmission functionality. Additionally, the PRC-162 provides increased power output, longer battery life and improved signal sensitivity in one of the smallest form factors on the market.

The AN/PRC-162 allows the Army to maintain interoperability with legacy waveforms, such as Single Channel Ground and Airborne Radio System (SINCGARS), and next-gen waveforms, such as Trellisware's TSM® waveform and Warrior Robust Enhanced Network (WREN) waveform. Additionally, the AN/PRC-162 includes upgraded tactical SATCOM through implementation of the Mobile User Objective System (MUOS).

The AN/PRC-162 also brings high performance to the battlefield in dismantled and vehicular mounted solutions. The optional compact vehicle mounting kit can be retrofitted in the field in less than a day, providing lower life cycle costs and flexibility in deployment.

This ninth order was issued under a multiple award contract that the Army awarded to Collins Aerospace and two other companies in 2016. The contract has a \$12.7 billion ceiling with an ordering period ending March of 2026.

LOCKHEED MARTIN DELIVERS LONG RANGE HYPERSONIC WEAPON'S GROUND SYSTEM TO U.S. ARMY



Lockheed Martin (NYSE: LMT) has delivered critical ground equipment to the U.S. Army for the company's Long Range Hypersonic Weapon (LRHW) system, part of a rapid, multi-year hypersonic weapons development program supporting the service's focus on long-range precision fires.



In a ceremony held at **Joint Base Lewis-McChord**, the U.S. Army and industry team celebrated this delivery of ground equipment, including the battery operations center and four transporter erector launchers. The overall system is being developed in partnership with the U.S. Army's **Rapid Capabilities and Critical Technologies Office** and its **Hypersonic Project Office**. Led by Lockheed Martin, other industry teammates include Dynetics, **General Atomics**, **General Dynamics**, **i3**, **Moog**, **Northrop Grumman**, **Penta Research**, **Raytheon** and **Verity Integrated Systems**.

The Lockheed Martin LRHW contract was originally awarded in 2019. Future flight tests are slated for fiscal year 2022-2023, and the program remains on track. Earlier, Lockheed Martin opened an intelligent, advanced hypersonic production facility at its Courtland, Alabama location. Designed and constructed with the latest digital tools, factory work there will focus on producing much of the company's hypersonics portfolio, including LRHW.

Hypersonic weapons are a key aspect of the long-range precision fire modernization effort for the Army and the national security strategy to compete with and outpace potential adversaries. Lockheed Martin is an established industry leader in the development of hypersonic strike technology and our experience also serves as the cornerstone for hypersonic defense systems.



Enduring Performance

Purpose-Built Technology
that is simple, reliable & easy to use.

RL3430 Beacon Receiver

- Compact 1U design, purpose built for longevity
- Flexible interface options (Analog, 232, Ethernet)
- Analog summary fault output
- Available in L, C, Ku, X and Ka bands



See all of our reliable 3430 series Beacon Receivers at RadeusLabs.com

Contact Us

Contact us today for a site visit!

SALES (858) 602-1255 | Sales@RadeusLabs.com | Radeuslabs.com
(858) 391-1210 • 12720 Danielson Court • Poway, CA 92064 USA



U.S. DEPARTMENT OF HOMELAND SECURITY RELEASES GPS VULNERABILITY PROTECTION TOOLS



Science and Technology

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has published a [Global Positioning System \(GPS\) Receiver Whitelist Development Guide](#) and a new release of the [Positioning, Navigation, and Timing \(PNT\) Integrity Library](#) to protect against the spoofing, or deceiving, of GPS devices through false signals. These resources advance the design of PNT systems and increase resilience of critical infrastructure to PNT disruptions.

The [GPS Whitelist Development Guide](#) presents a software assurance approach to addressing potential vulnerabilities and increasing reliability of GPS receivers. The guide addresses data-related requirements in the [Resilient PNT Conformance Framework](#), which provides guidance for defining expected behaviors in resilient PNT equipment.

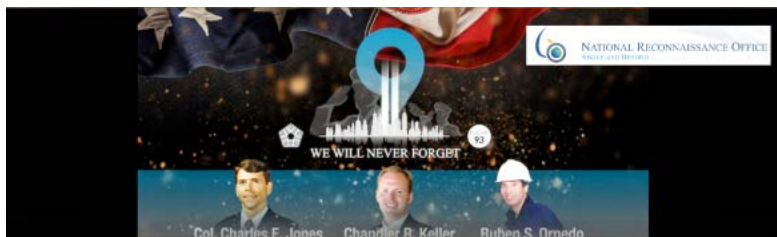
Originally released in March of 2021 as open source on [GitHub](#), the PNT Integrity Library provides users with a method to verify the integrity of the received GPS data. The update includes:

- A compliance check on Interface Control Document (ICD) IS-GPS-200, which is a formal means of establishing, defining, and controlling communication between the GPS space and other user systems
- A Do-It-Yourself (DIY) Toolkit, which describes how a perspective end-user of the PNT Integrity Library can assemble a demonstration toolkit with commercial-off-the-shelf (COTS) hardware.

“We hope this guide and related resources will help industry advance towards a cybersecurity-based approach to PNT resilience,” said S&T Technical Manager, [Ernest Wong](#).

“As GPS signals can be jammed or spoofed, critical infrastructure systems should not be designed with the assumption that GPS data will always be available or will always be accurate,” said S&T Project Manager, [Brannan Villee](#). “Application of these tools will provide increased security against GPS disruptions. However, DHS also recommends a holistic defense strategy that considers the integrity of the PNT data from its reception through its use in the supported system.”

NRO DIRECTOR REVEALS NEW COMMERCIAL ACQUISITION OPPORTUNITIES UPCOMING



The [National Reconnaissance Office \(NRO\)](#) has announced a new acquisition, the [Broad Agency Announcement \(BAA\) Framework for Strategic Commercial Enhancements](#), focused on new and emerging commercial capabilities.

Under the new [BAA Framework for Strategic Commercial Enhancements](#), the NRO plans to release independent focus areas multiple times per year. The BAA Framework and the first focus area, commercial radar capabilities, will be open to offerors across industry, including foreign-owned U.S. companies.

The NRO’s diversified architecture—comprised of national and commercial satellites, large and small constellations, working across multiple orbits—provides increased flexibility and capacity, greater responsiveness, and improved resiliency. Leveraging commercial capabilities to the maximum extent possible to meet mission requirements allows the NRO to reserve national assets for the most stressing and sensitive missions.

Focused on commercial imagery and data, this BAA builds on the success of the NRO’s Commercial Systems Program Office’s (CSPO) earlier study efforts and creates additional opportunities to expand NRO’s commitment to new and emerging commercial capabilities. It is specifically designed to explore and push forward new phenomenologies, including commercial radar, hyperspectral imagery, and radio frequency remote sensing, as well as emerging and evolving electro-optical capabilities. The Strategic Commercial Enhancements framework will reach across disciplines to drive innovation and explore new phenomenologies, while examining emerging and evolving capabilities.

“We’ve seen an explosion of innovation on the commercial side,” said Dr. [Chris Scolese](#), NRO director, who announced the BAA during his keynote remarks at the [United States Geospatial Intelligence Forum’s GEOINT Symposium](#). “This BAA Framework will allow the NRO to rapidly explore, assess, and leverage innovative industry capabilities to meet new intelligence challenges and inform operational requirements.”

“The breadth of this framework ensures we have access to the data and providers needed to deliver value today, assess mission utility with our mission partners, and inform the Intelligence Community and Department of Defense’s future needs,” said [Pete Muend](#), CSPO’s director.

The new BAA Framework and first focus area will be available at acq.westfields.net.



50W Ka-Band GaN Wideband BUC

Operates in all commercial and military Ka-Band frequencies

Supporting ARSTRAT-certified Ka-Band units 14 years after initial deployment.

We're ready to support the most critical networks on the planet.

Amplifying Mission-Critical Satellite Communication

SPACE ACCESS THE NATION CAN RELY ON

SPACE SYSTEMS COMMAND LAUNCH ACQUISITION & OPERATIONS BRINGS BETTER SYNERGY TO USSF LAUNCHES

Space launches are about to become more efficient, cost-effective and digitally advanced, thanks in part to the reorganization of [Space Systems Command \(SSC\)](#), and its new assured access to space strategy.

Access to space cannot be taken for granted: everything from our country's national security, to the economy, to the safety and lethality of our warfighters across the **U.S. Department of Defense** depends on our continued ability to launch satellites when needed, and into the precise orbits required.



Brig. Gen. D. Jason Cothorn

To ensure this mission, SSC has brought together launch acquisition and operations, including Space Launch Deltas serving the East and West Coast ranges as part of its new **Assured Access to Space (AATS)** organization. Led by Program Executive Officer, Brig. Gen. **D. Jason Cothorn**, SSC deputy commander, AATS consists of three components: **Launch Enterprise** at the **Los Angeles Air Force Base**; **Space Launch Delta 45** at **Cape Canaveral Space Force Station** and **Patrick Space Force Base**, Florida; and **Space Launch Delta 30** at **Vandenberg Space Force Base**, California.

"We're probably in a better place now than we've ever been in terms of assured access to space," said Col. **Robert Bongiovi**, director of SSC's Launch Enterprise, which manages the **National Security Space Launch (NSSL)** and **Rocket Systems Launch Programs (RSLP)**.

NSSL provides assured access for the nation's most critical warfighting space assets, launches that often have demanding orbits and complex payloads. These launches cannot fail and the program currently has a record of 87 consecutive successful launches. The RSLP is focused mainly on smaller launches: suborbital, experimental, and demonstration, but also can operational launches, such as a recent launch for the National Reconnaissance Office.

Partnership with commercial space industry partners such as **SpaceX** and **United Launch Alliance** has helped SSC harness new technological discoveries to improve launch reliability and success and has also made launches more cost-effective, Bongiovi said. Since 2013, SSC has been able to reduce its lifecycle costs by \$22 billion, and has returned \$7 billion in budgeted funds for other warfighting capabilities.

"As defined by law, 'Assured Access to Space' means making sure there are multiple ways to get any of our payloads into orbit at any given time, but it's broader than that," **Bongiovi** said. "Some of our payloads have really robust demands on what mass needs to go into what orbits, and that makes it hard to be affordable unless you take advantage of what industry is doing on the commercial side and partner with them on the harder missions we need to fulfill. The U.S. commercial launch industry is the envy of the world, and the two launch deltas were working to strengthen their partnerships with industry even before the standup of SSC and the subsequent reorganization."

"One of the most significant advantages of the SSC stand-up is the alignment of the East and West Coast ranges and the Launch Enterprise under the Assured Access to Space Corps," said Col. **Robert Long**, commander, Space Launch Delta 30. "We had built solid partnerships over decades, but until we merged under one organization, we existed in two very different chains of command. Now, the entire team that focuses on launch and test is all sitting at the same table working for a single person. This is going to accelerate and improve upon our already strong relationships. It represents a tangible example of the benefits of the flatter organizational model the USSF is now operating under."



Col. Robert Long

Bongiovi added, "Bringing the launch ranges and Launch Enterprise together enables us to be more synergetic in our activities and allows us to have a single, two-star general officer-led organization where we can work together to solve problems, plan for the future and implement some of the critical innovation that's needed as we move to a more demanding and responsive capacity. It really removes red tape – there's been about two echelons of leadership removed, and certainly a lot more coordination is able to happen this way."

"From the perspective of national security, we see the growth in commercial space as a strategic benefit to the nation, so we work hard to meet the needs of both industry and the DoD," **Long** added. "We work closely with our commercial launch service providers to offer them equal access to the Ranges and the full spectrum of services that we offer to all of our customers. As a result, we have seen innovation and competition in the launch services market create new opportunities for National Security Space at lower costs than ever before. Additionally, we are modernizing our Range services through technology and infrastructure investments that enhance our flexibility and capacity. These investments are already yielding more launch availability, and reducing schedule conflicts, allowing both industry and the DoD to coexist rather than compete for Range time."

"We're successful because of our industry and it's important that we keep that in mind," **Bongiovi** said. "Every time they do a launch, every time they develop or upgrade their systems, it's benefiting the national security of the United States as well. This is a true partnership, whether it's because we can use those systems as the starting point for a more complex launch that we need to do, or whether we can count on their expertise to allow us to move more rapidly down a learning curve to reduce the cost of mission assurance."

Space Launch Delta 30 operates the Western Range and provides range and spaceport capabilities for National Security, civil and various private industry contractors as well as missile testing, aircraft testing and ground- and sea-force exercises.

"We support the Missile Defense Agency, Air Force Global Strike Command, the National Reconnaissance Office, the Combined Force Space Component Command, Delta 5, Delta 1, and many, many others," **Long** said. "In addition to providing world class range services, we are a strategic platform providing world-class installation support to enable global power projection. Our footprint covers more than 118,000 acres of land and we support approximately 11,000 military, civilians, contractors, dependents and retirees."



"We see Vandenberg as the 'Range of Choice' for launching satellites into polar orbit, conducting ICBM test launches, supporting missile interceptor tests, collecting critical data for aeronautical operations and military exercises in the broad ocean off our coasts, and a host of other unique services relevant to both the DoD and industry," Long said. "These are all growth areas. The demand for test mission support is at an all-time high. ICBM testing only occurs at Vandenberg."

He continued, "For example, the Ground Based Strategic Deterrent program is a huge growth area for us in this domain. Also, our established spacelift partners, like United Launch Alliance and SpaceX, are projecting significantly more launches than they have in the past. Additionally, we are working closely with a number of emerging commercial launch service providers — like Firefly, Relativity and ABL, just to name a few — and we continue to explore new ways leveraging Vandenberg's unique location for space launch and test activities. Each of these companies bring unique capabilities and potential for even higher launch rates. The next decade and beyond will be very exciting for our mission, our base and our local community."

Space Launch Delta 45 operates the Eastern Range and provides services and support for National Security, civil and commercial missions and typically launches payloads into GEO orbits.

The USSF "Range of the Future" initiative over the next decade will include infrastructure enhancements, scheduling overhauls and other improvements to bring in a new era of U.S. spaceports. One major change will be adopting **Automated Flight Safety Systems (AFSS)** by 2023.

"Traditional flight safety systems require a vast array of ground-based assets to ensure that we know where the rocket or missile is at all times, and that we have the capability to terminate it in flight if it presents a risk to the public," Long explained. "Through tremendous innovation by both government and industry, we have collapsed the functionality of that network of sensors and transmitters on the ground into a system on-board the rocket itself. AFSS maintains the same extremely high standards of public safety protection, while eliminating many dependencies on the ground. AFSS is the one of the most significant enablers to transforming the ranges into national spaceports."



"Ideally, a national spaceport will provide launch opportunities similar to how an airport provides flight opportunities. The vision is that launch service providers and the DoD test community will be able to launch on-demand with policies and norms in place that facilitate safe, flexible, repeatable and simultaneous operations. To make this vision a reality, we anticipate a whole-of-government approach with representatives from not only the DoD, but also the Federal Aviation Administration, the Department of Commerce, the Department of Transportation and many others. This transformational operating model will promote orbital and suborbital launches for multiple customers with diverse business goals or mission requirements."

"The rest of the world is copying what our launch industrial partners are doing," Bongiovi said. "And we're going to make sure that we continue to provide the best launch capability in the world, and do it in a way that's affordable and meets the needs of the upcoming threats in the changing world."

Space Systems Command is the **U.S. Space Force** field command responsible for rapidly identifying, prototyping and fielding resilient space capabilities for joint warfighters. SSC delivers sustainable joint space warfighting capabilities to defend the nation and its allies while disrupting adversaries in the contested space domain.

SSC mission areas include launch acquisition and operations; space domain awareness; positioning, navigation and timing; missile warning; satellite communication; and cross-mission ground, command and control and data.

Contact Space Systems Command at SSC@spaceforce.mil — follow on [LinkedIn](#).



Vandenberg SFB, California



Cape Canaveral SFS, Florida

Merely decades ago, just getting from Earth to the Moon and back was enough.

Today, many space-faring nations have set their sights on exploring and developing the area of space in between – cislunar space – as a possible stepping stone to future space exploration and development.

“Cislunar” refers to the volume of space influenced by the Earth and/or Moon. Geosynchronous orbit – typically the highest orbit for satellites – is approximately 22,236 miles above Earth’s equator. The moon lies approximately nine times that distance – 238,900 miles – from Earth.

The National Aeronautics and Space Administration’s (NASA) Artemis program is planning to return humans to the moon by 2024, and to build an orbital outpost, known as the Gateway, in the vicinity of the moon during this decade. The Gateway could enable human-crewed missions in cislunar space and missions on the surface of the moon, as well as demonstration projects for technology to be used for Mars and other deep space missions.

At the same time, China and Russia are working together on plans for a joint International Lunar Research Station, a planned lunar base.



George Pollock

“There are a number of factors which are driving the marked increase of interest in cislunar,” said **George Pollock**, director of the astrodynamics center at the Aerospace Corporation, the only federally funded research and development center dedicated to serving the entire U.S. space enterprise.

“First, you have the scientific interests. The Apollo missions answered many questions about the moon and its origins, but also posed other questions,” Pollock said. “Perhaps the most tantalizing of those questions is the indication from orbital sensors that there could be substantial volumes of water ice in various locations on the moon and that’s one of several potential resources that could be used for expanding humanity’s exploration of the solar system. If you’ve got water, you’ve got hydrogen and oxygen, which could be used as rocket propellant.”

“One objective that NASA has in mind, is that going back to the moon is a stepping stone to getting to Mars with humans,” Pollock added. “It serves as a test bed for key technologies that will be needed for those longer-duration human spaceflight missions to Mars and beyond.”

“And then there is an interest globally, motivated by international prominence or prestige – the presence of robotic spacecraft and human activities on and near the moon stand to represent the culmination of human ingenuity and technological supremacy and serve as foundational evidence that a nation is a space-faring leader,” Pollock said.

“Then there’s national security. As a nation’s interests expand beyond GEO, there are national security motivations for understanding the earth-moon system and ensuring that they can secure their interests,” Pollock said.

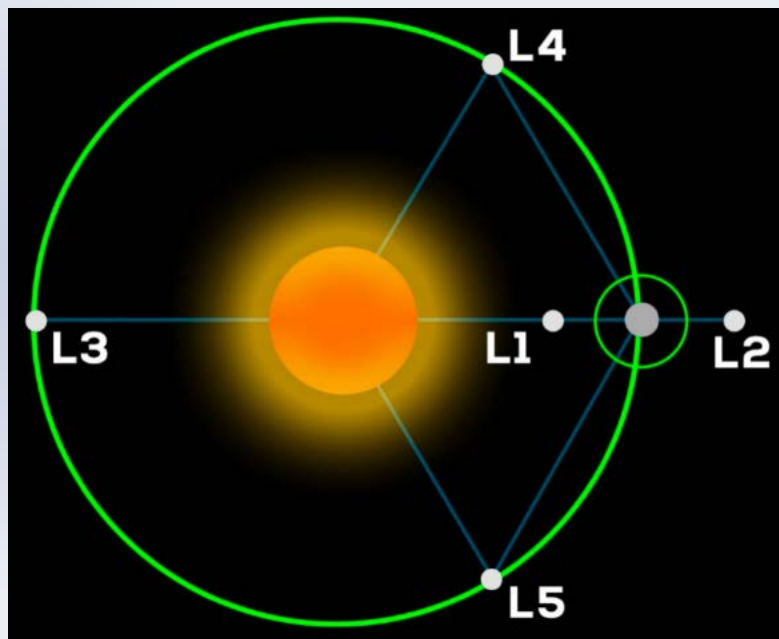
“Another factor driving the interest in cislunar is the fact that technology has finally advanced enough to make it practical,” said **Bruce McClintock**, lead for the RAND Corporation’s Space Enterprise Initiative and senior policy analyst.



Bruce McClintock

In cislunar space, any space object must contend not only with the effects of Earth’s gravity, but also that of the moon’s, which affects everything from a rocket’s trajectory to the kind of orbit it might have around the moon – and how those orbits change over time. Scientists have known for centuries about some of the unique orbital mechanics of cislunar space – including the five Lagrange points, positions in space where gravitational forces create a sort of “parking space” for objects where they tend to stay put – but it’s only been in the last 50 years that humanity has been able to use them for space operations.

As examples of using similar Lagrange point locations in the Earth-Sun system, L1 is where the Solar and Heliospheric Observatory Satellite is located, and the L2 point will be the future home of the James Webb Space Telescope, according to NASA.



“Over the past several years, there has been a significant change in capabilities, as far as reliable, low-cost space launch is concerned,” said **Jan Osburg**, senior engineer with RAND, a nonprofit research organization. “For the longest time, there was no point in the United States and the DoD worrying about what should or could we do on or around the moon, because there was no way to get there for any sort of reasonable amount of money and risk. Humanity was pretty much stuck in Earth orbit up to the GEO belt.”



Jan Osburg

“One of the under-appreciated realities of beyond-GEO spaceflight is that the orbital dynamics become much more rich,” Pollock explained. “Once you get out there with your spacecraft, you’re able to do maneuvers that would be unthinkable expensive in a direct Earth orbit. There are halo orbits on, say, the far side

of the moon and the near side of the moon and one can transfer between those for a very small amount of propellant.”

Cislunar orbits could be used for multi-purpose orbiting platforms, propellant storage depots, research outposts, places to extract and process extraterrestrial minerals, Pollock said.

The role Space Systems Command and the USSF will play as humanity expands into cislunar space is still evolving. A recent memorandum of understanding between the NASA and the U.S. Space Force noted that USSF’s “sphere of interest” extends beyond GEO – “more than a tenfold increase in range and 1,000-fold expansion in service volume. USSF now has an even greater surveillance task for space domain awareness (SDA) in that region...” “



Frederick Palkovic

“You can think about cislunar space in a similar way as we view other domains,” said **Frederick Palkovic**, deputy chief of SSC’s space domain awareness division.

“For example, in the sea domain we don’t need to know everything going on, everywhere, in all the oceans. What is important to know is the right things at the right times and right locations necessary to support our national interests including the protection and defense of our sea lines of communication. To know everything, everywhere, in our oceans might be nice but it is simply unaffordable.”

“Today in the space domain, we have systems of systems which work together to gain and maintain space situational awareness in the critical orbits around the Earth,” Palkovic said. “In general, we use radars to illuminate objects in near earth orbit to track satellites and debris close to the earth and use optical systems using the energy from the sun reflected off satellites to track objects in the geosynchronous belt.”

“While our current systems have provided us with domain awareness in the past, the expansion of our national interests into cislunar space is a 1,000 times increase in the volume of space to maintain awareness of,” Palkovic said. “The key here remains the same as our needs in near earth space and in other domains: to know the right things at the right times.”

What are our national interests in cislunar space? Palkovic explained, “Well, there will be much debate before that is settled, but, the guiding principles are fundamental and not likely to be changed. We need to know enough to protect our national interests in space and ensure potential adversaries do not use the sanctuary of the dark of deep space to threaten our national interests there, closer to earth, or in the other domains.”

“SSC’s anticipated future role is to deliver systems capable of providing cislunar domain awareness, commensurate to U.S. national interests,” Palkovic said. *Already, SSC participates with a broad team looking at the challenges of cislunar space, including SSC’s federally funded research and development centers and laboratory partners, USSF, U.S. Space Command, NASA, the intelligence community as well as international and commercial space industry partners.*

In addition to expanding space domain awareness into cislunar, space-faring nations also will be dealing with another issue: there is no GPS in cislunar space.

“The current situation is that our globally position-navigation-and-timing systems are space utilities,” Pollock noted. “For operations that go beyond GEO, it’s typically been incumbent on the operator of the system to provide their own navigation solution, usually by leveraging their two-way communications link to do so. We don’t have a globally available utility like we enjoy with GPS today. As activity increases beyond GEO, it may well become worth the investment to provide an interoperable user service such that spacecraft operators can get PNT on demand at a lower cost.”

Further defining space norms and “best practices” is another policy challenge to be sorted. The 1967 Outer Space Treaty, with more than 100 signatory nations, is a foundational set of international agreements about the use of space, Pollock said, but it will be necessary to add more specificity as to what exactly constitutes good or bad behavior in space.

NASA’s Artemis Accords, which 12 countries - Australia, Brazil, Canada, Italy, Japan, Luxembourg, New Zealand, the Republic of Korea, Ukraine, the United Arab Emirates, the United Kingdom and the United States - have signed, covers such principles as peaceful exploration, registration of space objects, release of scientific data, extracting and using space resources and the deconfliction of activities.

For example, while no nation can lay claim to a celestial body, what happens when different nations want to start mining rare minerals from the moon? How do countries make sure space debris doesn’t become an issue around the moon, as it has in Low Earth Orbit (LEO)? While Pollock said the “preferred” cislunar orbits are large enough that it will be a long time before crowding becomes an issue, there may be problems with inadvertent communications interference that will need to be worked out.

“Cislunar is not something that’s going to dramatically escalate overnight,” McClintock said. “We’ve been operating in space since the 70s with a small number of platforms – it’s going to take time to expand to the point where it’s something that’s considered a common occurrence. But we are starting to see more activity there, and we need to take note. The United States can’t just wait until things are fully mature there – otherwise we will have fallen too far behind to catch up.”

Want to learn more? Check out these resources:

[Aerospace: Cislunar Stewardship: Planning For Sustainability and International Cooperation](#)

[Aerospace: Cislunar Development: What to Build—and Why](#)

[Air Force Research Laboratory: “A Primer on Cislunar Space”](#)

[NASA: The Artemis Accords](#)

[The Outer Space Treaty](#)

[RAND Corporation: “A Clean Sheet Approach to Space Acquisition in Light of the New Space Force.”](#)

[Space Force Journal: Cislunar Mission Concepts for the Department of Defense](#)

GOVERNMENT SATELLITE REPORT (GSR)

EM&C — OPENING THE DOOR TO AN INTEGRATED SATELLITE ARCHITECTURE FOR THE MILITARY

Author: Ryan Schradin, Editor,
Government Satellite Report

Rapidly growing information requirements and the increasing unpredictability of the location, nature, and types of conflicts make satellite communications systems more important every day. Using commercial bandwidth to augment the military's dedicated capabilities is essential to providing global coverage.

The goal is a future military SATCOM enterprise that will leverage all available satellite capability in a way that is transparent to the user, much like turning on a cell phone. Several key government programs will help enable this vision, with the linchpin being **enterprise management and control (EM&C)**.

Kratos Defense & Security Solutions, Inc. is one of the companies playing a key role in achieving both the broader strategy, and EM&C in particular. GSR recently spoke with **Frank Backes**, senior vice president for Federal Space at Kratos, to discuss EM&C and how it will open the door for the military to embrace next-generation satellite solutions, including the **SES O3b mPOWER** satellite service.

Government Satellite Report (GSR)
Good day, Mr. Backes. Please explain what EM&C is and why is it something the military needs?





Frank Backes

FRANK BACKES

EM&C supports the military's strategic goal to operate an integrated SATCOM enterprise and increases assured SATCOM access for the warfighter with legacy and next-generation terminals. It seeks to improve the effectiveness of the DoD's critical SATCOM infrastructure by enhancing resilience.

Among the goals of EM&C are giving more satellite link choices, reducing resource allocation times, improving bandwidth efficiency, and providing situational awareness to SATCOM. It allows

military and commercial satellite communications systems to be tied seamlessly into the terrestrial infrastructure.

For example, Kratos' *Global Sensor Network* helps the government detect and resolve RF spectrum challenges. With EM&C, data collected through this network and other sensor networks, such as the SES satellite network, is fused and pulled into the *Unified Data Library (UDL)* and accessed by our military.

EM&C gathers data from sensors into one accessible, cloud-based environment that can be viewed through a common operating picture. Its success rides on providing clear, concise, and actionable data to decision-makers in an operationally relevant timeframe.

"...multiple organizations independently pursuing their own mission needs have produced a number of ground-based proprietary satellite communication solutions, which have created a lack of interoperability between different commercial services and the armed forces." — Frank Backes

GSR

What benefits would an integrated commercial and military satellite architecture deliver to the military?

FRANK BACKES

We believe an integrated architecture allows the military to leverage the investments the commercial sector have made in innovative technologies. Advanced commercial technologies have added benefits, including increased resilience to interference, jamming, or environmental effects, far more rapid resource allocation, improved situational awareness, and increased bandwidth utilization efficiencies.

The military can benefit from commercial innovation if they can switch seamlessly between government and commercial satellites – regardless of ownership. Operating as a seamless network enterprise gives the military more options allowing flexibility, scalability, and resiliency.

GSR

What are the current technological impediments to this being a possibility? What interoperability challenges exist?

FRANK BACKES

Unfortunately, multiple organizations independently pursuing their own mission needs have produced a number of ground-based proprietary satellite communication solutions, which have created a lack of interoperability between different commercial services and the armed forces. Those same proprietary solutions remain roadblocks to a dynamic SATCOM infrastructure supporting communication for an evolving military theater.

Currently, terminals cannot automatically switch between different satellites, and warfighters are challenged to communicate to networks outside of their domain. If terminals are jammed, it can be time-consuming to execute the current system to locate and help switch to reliable communication links. If redundant terminals or gateways

"Right now, terminals cannot automatically switch between different satellites, and warfighters are challenged to communicate to networks outside of their domain." — Frank Backes

are not available, alternative waveforms may not be automatically accessible

These challenges go beyond our own military and answers must include a holistic approach that ties in our allies.

GSR

What is the Flexible Terminal Interface (FTI) and what role will this play in enabling an integrated satellite architecture?

FRANK BACKES

FTI is an interface standard that has been defined by our government. It can be added to existing terminals as either a software or lightweight hardware-based interface upgrade. It provides management and communication functions, plus, it allows roaming between terminals that would not normally communicate with each other.

EM&C determines why, when, and how the system should roam and transition utilizing flexible terminals to access diverse SATCOM resources. EM&C enables the terminal to have awareness of other network options operating on alternate satellites and automatically switch to new networks to avoid interference. By monitoring the RF environment and impacts to performance, its system logic determines best available SATCOM resources, coordinating and connecting users on each end as needed.

Think of it as being like a roaming cell phone capability. It doesn't matter if you have AT&T or Verizon or Sprint, you can talk to anyone regardless of the provider.

GSR

What pilot programs and testing programs is the military conducting regarding the FTI and

EM&C? What work is Kratos doing on these programs?

FRANK BACKES

The U.S. Air Force has continued to define details of the EM&C architecture over the past several years. These efforts have included funding a Pilot Phase 1 study, which solicited feedback from Industry on possible solutions and recommended architectures, followed by a Pilot Phase 2 effort, which funded several companies to demonstrate prototypes of the EM&C architecture. Both of which Kratos was a participant.

Successful demonstrations were then carried out in December of 2018 and January of 2019, showing the ability to roam among heterogeneous networks, enabling secure SATCOM across multiple operator networks. These demonstrations used a U.S. government multi-band satellite communication terminal and gateway equipment representative of a current deployed infrastructure.

In March of 2021, a successful demonstration was hosted by U.S. European Command (EUCOM) and funded by the Advanced Battle Management System (ABMS) program. SATCOM situational awareness was demonstrated to an operationally secure environment utilizing commercial resources.

EM&C capabilities highlighted a means for providing real-time satellite communication end-to-end connectivity status and operational readiness. It also showed the ability to restore satellite service in response to interference and the capability to gather and fuse information into the UDL from sensors and satellites that included coalition partner sources. Kratos' partner SES provided the SATCOM capacity for this demonstration.

“Among the goals of EM&C are giving more satellite link choices, reducing resource allocation times, improving bandwidth efficiency, and providing situational awareness to SATCOM.” – Frank Backes

GSR

SES is poised to launch their next-generation Medium-Earth Orbit (MEO) satellite solution in the coming months which is part of a larger industry trend of launching High Throughput Satellites (HTS) in orbits closer to Earth. What do these new satellite constellations offer that the existing Wideband Global SATCOM (WGS) satellites don't? Why should the military be excited for this next generation of satellite constellation?

FRANK BACKES

WGS is a MILSATCOM Geostationary Orbit (GEO) constellation that provides wideband communication to the U.S. military and our allies. The satellites are far away from earth, extremely expensive, and take a long time to build. Also, there are not many satellites in the constellation, and some consider them easy targets to peer adversaries.

This does not mean that WGS no longer serves a purpose. WGS is still a central element of the DoD's SATCOM infrastructure. However, the newer constellations can offer higher capacity, lower latency and more diverse communication paths that enhance resiliency.

Right now, if you look at the terminals supporting fixed U.S. Army or Air Force command posts, the DoD has to coordinate for the channel days or months in advance if using military channels or pay a lot for the throughput for a specific channel. With the commercial SATCOM in Low-Earth Orbit (LEO) and MEO, you pay just for the service being used and it can be consumed almost immediately. EM&C offers a means to have situational awareness on this complex network and potentially enable active roaming.

GSR: Are FTI and EM&C necessary for the government to utilize satellite constellations like the O3b mPOWER satellite service? How could EM&C and FTI make it easier and more seamless for the military to use satellite constellations like these?

FRANK BACKES

We believe the DoD would benefit from compatible terminals that the FTI would support. Terminals would be available in different sizes for different users but all equally capable of talking to LEO, MEO, and GEO satellites.

In a complicated network that includes many satellites in multiple domains, EM&C would control the operation for deployed warfighters. It would do the work and automatically choose the best satellite based on

“In a complicated network that includes many satellites in multiple domains, EM&C would control the operation for deployed warfighters. It would do the work and automatically choose the best satellite based on relevance, availability, and capability.” – Frank Backes

relevance, availability, and capability.

GSR: Beyond terminals, are today's ground systems ready for such broad operational vision? What commercial approaches can augment and perhaps support future Joint All Domain Operations (JADO)?

FRANK BACKES

Ground systems are not completely ready and that is why we announced the OpenSpace Platform this year. The OpenSpace Platform is a commercial, virtualized software solution with advanced networking capabilities. Virtualized processes can remove dependence on proprietary and expensive hardware. Features available through the platform increase security, offer just-in-time deployments, reduce hardware footprints, and enable cloud-based solutions. Commercial approaches such as the OpenSpace Platform can indirectly

augment and support JADO. For example, Kratos' Global Sensor Network provides Space Domain Awareness (SDA) which is essential to JADO. The network uses the OpenSpace Platform to configure RF hardware such as antennas, digitizers, and software to collect, process, and disseminate data.

Advanced SATCOM capabilities available from O3b mPOWER's constellation can also augment and support JADO. In turn, mPOWER's constellation could benefit from SDA capabilities provided by Kratos' Global Sensor Network.

For additional information about how Ob3 mPOWER can enable next-generation technologies on the battlefield, [select this direct link](#) to download a complimentary copy of the whitepaper, “High Throughput Satellites for U.S. Government Applications.”

This article first appeared on GovSat and is republished with permission of SES and GSR.



Ryan Schradin is the Executive Editor of GovSat Report. A communications expert and journalist

with more than a decade of experience, Ryan has edited and contributed to multiple, popular, online trade publications that

are focused on government technology, satellite, unified communications and network infrastructure. His work includes editing and writing for the GovSat Report, The Modern Network, Public Sector View, and Cloud Sprawl. His work for the GovSat Report includes editing content, establishing editorial direction, contributing articles about satellite news and trends, and conducting both written and podcast interviews. Ryan also contributes to the publication's industry event and conference coverage, providing in-depth reporting from leading satellite shows.



MICROCHIP'S LOW POWER FPGAS TO ACCELERATE DARPA TECH INNOVATIONS



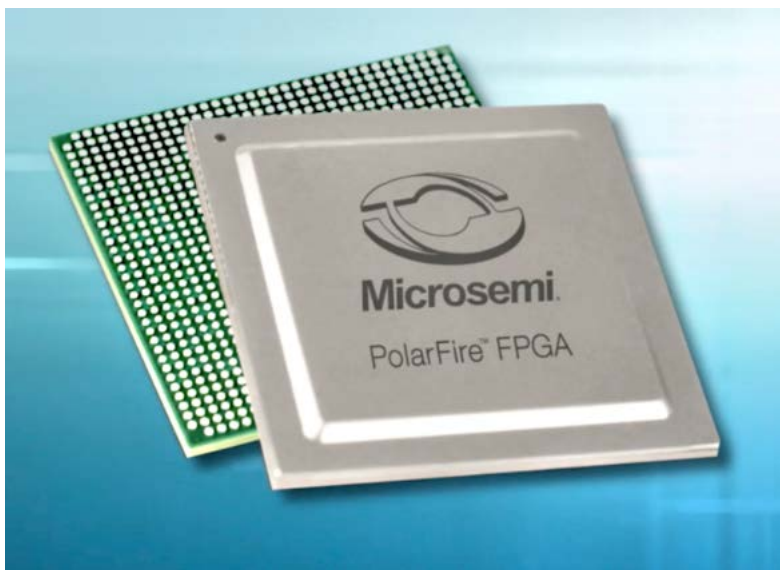
Recently, Microchip Technology Inc. (Nasdaq: MCHP) joined the Defense Advanced Research Projects Agency (DARPA) Toolbox initiative that gives the organization's researchers simplified open licensing opportunities with commercial technology vendors.

DARPA Toolbox Initiative -  Microchip



Microchip's participation will speed innovation across a variety of defense and aerospace development programs by giving qualified DARPA researchers zero-cost access to the company's Libero® design software suite and associated intellectual property (IP) for developing systems based on its low-power FPGA product families.

Microchip is the only technology company in the DARPA program to offer radiation-tolerant FPGAs, MOSFETs, zenor diodes, transistors, ASICs, linear regulators, microcontrollers, oscillators, atomic clocks, power supplies, relays, switches and other microelectronic solutions that can survive conditions in space and other harsh military and defense environments.



The PolarFire® product family includes PolarFire, PolarFire System on Chip (SoC) and Radiation Tolerant (RT) PolarFire devices, all offering up to 50 percent lower power, best-in-class security and a side channel resistant CRI pass-through license on data security devices and FPGA configuration cell upset immunity.

The PolarFire product family gives DARPA researchers new tools to solve complex problems where high levels of operating performance and density must be combined with low heat dissipation, power consumption and system-level costs.

"Partnering with Microchip through our DARPA Toolbox initiative gives our award-winning innovators streamlined access to the industry's most advanced commercial technologies for solving such difficult aerospace and defense challenges as onboard satellite payload processing," said **Serge Leef**, the Microsystems Technology Office (MTO) program manager at DARPA and leader of the DARPA Toolbox initiative. *"Microchip's portfolio of soft IP cores provides our researchers with a powerful option for implementing designs ranging from high-resolution passive and active imaging systems to precision remote scientific measurement equipment, multi-spectral and hyper-spectral imaging solutions, and object detection and recognition systems using neural networks."*

"As the industry's largest microelectronics suppliers to the military and aerospace markets, Microchip is committed to enabling DARPA researchers to reach higher and solve complex problems with our low-power and secure FPGA product families," said **Bruce Weyer**, vice president of Microchip's FPGA business unit. *"We are among the few semiconductor suppliers that are capable of completing the rigorous device qualification process for military and spaceflight microelectronics products, and this expertise is embedded in the FPGA design software and IP that we are delivering through our streamlined DARPA Toolkit acquisition license."*

A CONSTELLATIONS CONVERSATION WITH... JUSTIN PADILLA, DIRECTOR, CYBERSECURITY SERVICE, KRATOS DEFENSE

WHAT YOU NEED TO KNOW ABOUT CMCC...
CRITICAL INFORMATION PROTECTION AND
CONTRACTING WITH DoD

In light of the data breaches that have hit government and commercial organizations, the U.S. Department of Defense is enacting CMMC, the Cybersecurity Maturity Model Certification. This new unified security standard and certification process is designed to significantly enhance cybersecurity and protect critical information across the DoD supply chain. It will also impact contractors in the satellite industry, requiring them to achieve certification in order to do business with the DoD.

The interview was conducted by Kratos' podcast host, John Gilroy.

John Gilroy:

This is a space and satellite podcast, however, the Department of Defense is a key component in this discussion. The DoD does not manufacture anything. Instead, it relies on more than 300,000 suppliers for its goods and services. While the Pentagon is a hardened target, our adversaries understand that DoD's suppliers are not. To improve the security for the defense industrial base, a relatively new concept called CMMC, or Cybersecurity Maturity Model Certification, is being put into place that will affect companies looking to do business with the DoD, which of course, includes the satellite industry.

To break this all down is Justin Padilla, the Director of Cybersecurity Services at Kratos. Kratos was recently named as one of the first two authorized CMMC Third-Party Assessment Organizations, or C3PAOs. Justin is going to walk us through what CMMC is and how it will impact your organization. Justin, to start this conversation, what's the crux of CMMC?



Justin Padilla

John Gilroy

What precipitated this whole move to CMMC?

JUSTIN PADILLA

It seems as though every week we hear about major data breaches, ransomware and other targeted attacks on organizations that have become integral components, not just for DoD, but our daily lives, as well. The troubling thing is those are just a small portion of the cyber threats and attacks that we actually hear about.

There are more than 300,000 companies that now comprise the defense industrial base. For years, organizations doing business with the DoD have been self-attesting that they meet the majority of the requirements that are within the CMMC. This evolutionary step is now moving away from that self-attestation model to a third-party assessment model that provides greater assurance that organizations holding this critical DoD data are doing what they say they're doing and protecting it.

John Gilroy

What is the role of the assessment organization, the C3PAO, which Kratos has been authorized to do?

JUSTIN PADILLA

A C3PAO is a CMMC third-party assessment organization. It's a trusted, vetted organization that specializes in assessing compliance of companies against a specific framework, in this case, the CMMC security practices and processes.

John Gilroy: Instead of relying on a company's own self-examination, which have been found wanting, they decided to bring in a trusted third party, to assess their security, their maturity in cybersecurity, correct? Plus, to be one of these trusted organizations, there must be significant requirements to be authorized as a C3PAO?

JUSTIN PADILLA

Exactly and, yes, there are. There are a number of things that aligned for us. Kratos is a substantial contributor to the defense industrial base, which means that as an organization, the delta

or difference between what we were previously attesting to and what we had to obtain from CMMC was rather minimal.

For many companies that have been doing business with the DoD, they should really be in that same boat, where they've been working towards or have already implemented the NIST SP 800-171 requirements that were part of the DFARS, and now they're doing that delta to get CMMC compliance.

A C3PAO itself has to meet whatever level that they're going to be assessing against. In this case, it was level three, so we had to validate that our organization, as a whole, was a level three.

Another main factor was that Kratos was an early adopter of CMMC, not only from the requirements but also as part of the program itself, working with the accreditation body and helping the community understand CMMC. There are also requirements around the company and staff being vetted from a security standpoint, all playing key factors in becoming a C3PAO.

John Gilroy

We're tackling this topic because companies doing business with the DoD are going to be directly impacted by CMMC.

Can you explain how this process works?

JUSTIN PADILLA

It is fairly straightforward. If you go to the cmmcab.org, there's a marketplace that identifies different people and resources that help organizations get prepared. It also points you back to the Office of the Undersecretary of Defense's website, which has documentation that leads people through the process for getting certified or meeting the requirements to get certified. But in order for an organization to get certified, there's a number of steps that they have to take, including making sure that they actually implement the requirements, and then working with the C3PAO to undergo that process.

John Gilroy

Is the process the same for everyone or are there different levels for certification?



JUSTIN PADILLA

CMMC has five levels of maturity that have increasing security requirements commensurate with the level of data that's associated with the contract. Levels 1 and 2 focus on federal contract information, and that information is provided by or generated from the government under contracts that's not intended for public release. Levels 3, 4, and 5 is Controlled Unclassified Information. The [National Archives and Records Administration](#) goes into great detail defining those various categories. From a definition standpoint, there's very specific information that would be better looked up than for me to explain here.

However, levels 1 through 3 are the only ones that can be assessed right now. Levels 2 and 4 are eventually going to be steppingstones from what I've heard from CMMC-AB. That will allow organizations to not necessarily make that big jump from 1 to 3, because there's a big difference in security requirements between those levels. Level 2 is there as a steppingstone. Level 4 and 5 are not fully finalized yet as far as the requirements. It's expected that's going to focus on specific types of Controlled Unclassified Information (CUI), that is deemed sensitive to a certain level — CUI has very military or space applications.

John Gilroy

There there any tips that you can share with companies going through the assessment process? Like what to prepare for, and how long the process takes?

JUSTIN PADILLA

From a tip perspective, I would say that if you haven't started getting your organization ready, start now, even if you don't plan on bidding on contracts or getting assessed next year or three years from now. The longer the runway that you have, the easier it's going to be. Whenever

time is constrained and you need to do something in a shorter period of time, it makes it much more difficult for an organization to implement.

As for what's involved, there's essentially four phases involved with the actual assessment. There's a **planning** phase, which outlines the scope of the environment and your work with your C3PAO. That includes identifying points of contact, documentation, or demonstrations of what would be needed during an assessment. The C3PAO works with an organization and helps them confirm that they are ready before actually entering into phase two.

Phase two is when we actually **conduct the assessment** and that requires both an on-site visit to physical locations, where CUI might be stored or what's defined in your scope or your boundary. It incorporates in-depth interviews and reviews of documentation and technical testing, things of that nature. The result of that is basically a pass or fail for each security practice and process, which ultimately determines the successful or unsuccessful certification recommendation.

For phase three, there's **reporting the assessment results** and whether you passed or failed. Note that with CMMC, it is all-or-nothing. An organization has to pass all of the given levels, security practices and processes in order to be recommended for certification. Any one control failure can and will result in a C3PAO not recommending you for certification, which sounds really scary.

There is a phase four, which is **remediation of outstanding assessment items**. That gives organizations up to 90 days to resolve any minor issues that might have been found during the assessment.

John Gilroy

Regarding costs, will CMMC put an undue burden on small companies that will need certification?

JUSTIN PADILLA

Organizations should have been meeting or close to meeting the previous DFARS requirements that incorporated the **National Institute of Standards and Technology (NIST) SP 800-171** (an NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled, unclassified information (CUI)). Realistically, there should only be around a delta of approximately 20 security controls in order for organizations to get to a CMMC level 3 requirement.

Companies are going to have to invest some money to tie up potential loose ends or **Plan of Action and Milestones (POA&M)** items that they had on their lists. But from an assessment perspective, I don't see CMMC assessment costs being drastically different from other certifications that organizations would normally go through. The DoD has also said that it may be reimbursable at some point, although I'm not the one to speak on that, but I do think that's a possibility.

John Gilroy

I understand that there are CMMC assessment services, but also advisory services. What's the difference? Does a company do one or both?

JUSTIN PADILLA

Organizations can do both. An RPO is a **Registered Provider Organization**, and they provide various consulting or advising services to organizations to get them prepared to undergo a CMMC assessment. That can be anything from helping an organization interpret security controls to integrating security solutions, conducting gap assessments, anything of that nature. The intent is to get them to the point that they can pass a CMMC assessment. When it comes to a C3PAO, that function is solely reserved for assessment, period. And that can be readiness assessments or even the full-on certification assessments. The key element is that a C3PAO, when performing in the role as an assessor, cannot provide guidance or recommendations. They're only there to assess whether or not you are meeting or not meeting a given requirement. And so for organizations that are both a C3PAO and an RPO, they cannot serve in both capacities for the same. It's either one or the other.

John Gilroy: What are some of the top challenges here for CMMC compliance?

JUSTIN PADILLA

CMMC will continue to evolve over the next few years as things get more flushed out. However, as we've been working with companies, CUI handling and the protections both from a physical and an electronic standpoint has areas of challenges. In large part, because many times organizations should be receiving information from the government that identify specifically whether it is or it is not CUI. In many cases, that's not happened and so organizations have a really difficult time with making sure that they are properly handling and marking information that would be classified as CUI.

From a technical standpoint, there are aspects that have proven to be difficult. Multifactor authentication is one. Whitelisting and blacklisting of applications are two others. Surprisingly, being able to gather a complete and comprehensive inventory of an organization's assets has proven to be challenging for many organizations. Then there's also the aspects of documentation, which in itself isn't hard, as you're really documenting what you do as an organization.

John Gilroy

Any advice for companies seeking a C3PAO for an assessment?

JUSTIN PADILLA

As I mentioned, there's a standard process that all C3PAOs are using so, you shouldn't see that much variance between one organization or another. I think where it really comes into play is the organization's experience with the type of business they're working with. A services organization is very much different than one that manufactures equipment. Working with a C3PAO to make sure you get all of your questions answered, that you feel comfortable with that organization, and that they have relevant experience in assessing environments such as your own, is important.

John Gilroy

Are there any special CMMC considerations that companies in this sector should be aware of?

JUSTIN PADILLA

Yes, I touched on specialized CUI, specifically designating that as **Control Technical Information**. As I mentioned, that is applicable to military and space applications. While I don't think that everyone is going to have to meet a higher level CMMC requirement level four and five, I would imagine that many organizations that support the space industry are working on stuff that is highly sensitive, that may not be classified but is pretty close. If you're in that situation, as you're working toward your level three certification right now, you should also be planning for those higher level of requirements just to kind of extend that runway, as I mentioned before, so that you have better planning and better options for implementing the solution that'll get you to where you need to be.

Want to hear from more thought-leaders? Listen to Constellations podcasts as they become available. See the full list of interviews and subscribe at www.constellationspodcast.com



www.kratosdefense.com

GOVERNMENT SATELLITE REPORT (GSR) UPDATE

GENERAL THOMPSON PROVIDES A STATUS REPORT FOR THE U.S. SPACE FORCE



Gen.
Thompson

Recently, General David “DT” Thompson from the U.S. Space Force joined the Mitchell Institute for a special Spacepower Forum event to give a status update on the buildout of Space Force, as well as discuss how the service is preparing to defend U.S. space architecture against potential attacks.



David
Presgraves

Author: David Presgraves, Staff Writer, Government Satellite Report

As **Vice Chief of Space Operations**, General Thompson is responsible for assisting the Chief of Space Operations, and organizing, training, and equipping space forces in the U.S. and overseas, integrating space policy guidance and coordinating space-related activities. Thompson opened the forum by expressing his excitement over the recent confirmations of **U.S. Air Force Secretary Frank Kendall** and **Under Secretary Gina Ortiz Jones**. According to Thompson, both Secretary Kendall and Under Secretary Jones have hit the ground running and are quickly facilitating the next phase of Space Force.

Thompson then gave an update on where Space Force currently stands. He explained that year one of Space Force was focused on inventing the force, designing it, and getting it in place. Though there will be several more years of fully building out the force, Thompson proudly announced that the design and resourcing phase of establishing Space Force is complete.

Year two’s primary focus has been on the integration of the force. “We’ve taken some pretty aggressive and significant steps thus far,” said Thompson. He explained that “*integration*” includes integration of the force with the services, the combatant commands, and with partners and allies. “They’re trailblazing the path for large-scale interservice transfer from those services into the Space Force. They’ve already begun that activity. And even as we speak, we are selecting up to about 350 others from that group, who will follow behind them once they trailblaze the path to that inter-service transfer,” General Thompson said.

The first step of the force’s integration is interservice transfer. The Space Force began with a large transfer of individuals from the U.S. Air Force, resulting in about 5,800 individuals in uniforms. In addition to bringing in candidates from the Air Force Academy, Space Force is also looking to bring in 50 interservice transfers from the U.S. Army, Marine Corps, and the Navy. “They’re kind of our beta test,” said Thompson. “They’re trailblazing the path for large-scale interservice transfer from those services into the Space Force. They’ve already begun that activity. And even as we speak, we are selecting up to about 350 others from that group, who will follow behind them once they trailblaze the path to that inter-service transfer.” In addition to manpower transfers, Thompson stated that Space Force is currently finalizing transfers of SATCOM, missions and functions from the Army and the Navy.

Another recent and important milestone that Thompson highlighted was U.S. Space Force and U.S. Space Command sending elements to the **United States Pacific Command’s (USPACOM) Pacific Sentry** exercise. This step was key to understanding how the U.S. Space Force as a service, and U.S. Space Command as a combatant command, integrate, provide capabilities, and contribute to combatant commander operations and objectives. Both Space Force and Space Command sent one-star officers to the exercise to lead teams. According to Thompson, “*I think it was incredibly productive, not just for our two organizations, but helping to inform the other combatant commands how we should proceed.*”

Thompson also explained that Space Force is already deep into mil-to-mil connections with a host of countries. “They’ve reached out to us to look at how we develop and expand relationships, and how we better do in space, what the nation – and our allies and partners – have known how to do for decades in the air, on land, and at sea,” said Thompson. He further explained that these countries are not just “our tried-and-true and well-understood partners.” Space Force has had countries from South America and others in the Indo-Pacific who are interested in establishing some sort of a mil-to-mil relationship as it pertains to security in space.

To preface his update on Space Force’s proposed 2022 budget, Thompson explained that the main catalysts that drove the force’s creation were “*the threats that we face, the fact that we now have to defend and protect those capabilities we provide, and to look at how we deny those capabilities to others.*” He went on to say that Space Force brings “*coherence, consistency, and unity to those activities inside of the Department of Defense. In addition to protecting what we have today, we’re going to pivot toward architectures in the future that are designed to be resilient, robust, and deliver capabilities under attack.*,” the general said.

Thompson detailed Space Force’s priorities for the 2022 budget. “Our priorities for that budget were to ensure that we can continue to provide the capabilities we already have. That includes everything from GPS to missile warning to satellite communications to supporting the National Reconnaissance Office (NRO) and others with intelligence, surveillance, and reconnaissance (ISR) in space. We’re really focusing on defending and protecting those capabilities so that they can continue to provide what they need under attack.” He discussed how Space Force is pivoting toward designs, systems, architectures, and forces that are designed to operate under threat. Thompson explained, “*In addition to protecting what we have today, we’re going to pivot toward architectures in the future that are designed to be resilient, robust, and deliver capabilities under attack.*”

Thompson said that Space Force must look at a host of ways to deny adverse use of space capabilities. He used the Indo-Pacific region as a prime example. “*Left to its own devices, our forces in that part of the world – maritime, air, land, and others – will be under constant surveillance and monitoring by China over its space constellation,*” said Thompson. “*That poses a great threat to our joint forces and to our potential operations. We have to have a means by which to address them.*”

According to Thompson, up until now, Space Force’s test and evaluation enterprise was focused on ensuring that its satellites operated effectively in the space domain. He said there now must be a shift to create a test and evaluation enterprise that tests and confirms that these capabilities operate under attack — similar to combat aircraft, combat action groups at sea, etc.

“*We now have to build the enterprise that does that,*” said Thompson. “*We have to have more effective and detailed management of an entire suite of space professionals...we need all those enablers that need to support what is truly a military service, and more importantly, military forces in the domain.*”

SSA + SDS FOR SATELLITES

SPACE SITUATIONAL AWARENESS (SSA) AND SPACE DOMAIN AWARENESS (SDA) SERVE AN IMPORTANT ROLE IN PROTECTING SATELLITES FROM HAZARDS AND COLLISIONS. SOFTWARE DEFINED RADIO (SDR) CAN BE INTEGRATED INTO SSA AND SDA SYSTEMS TO GREAT EFFECT.

*Authors: Brendon McHugh,
Field Application Engineer and Technical Writer,
Per Vices
and
Rafia Shabbir,
Technical Writer and Educational Content Developer*

What is space situational awareness (SSA) and space domain awareness (SDA)?

Space Situational Awareness (SSA) and **Space Domain Awareness (SDA)** refer to the detection of any potential hazard in a satellite's orbit, whether active or passive, by analyzing and forecasting the kinematic state and other attributes of space objects.

The main objective of SSA/SDA is to provide continuous and accurate tracking and surveillance of such potential hazards and to inform satellite operators of such conditions when they occur, thereby providing greater safety and success of the space missions.

Certain factors such as space/spacecraft debris, other satellites in space, frequency interference, and space weather phenomenon pose some serious risks to satellite systems in space. SSA/SDA monitors and minimizes these risks and also helps to manage space traffic by ensuring that the satellite orbit is not obstructed. In short, SDA helps in the decision-making process by providing timely and measurable evidence related to space threats.

A BRIEF HISTORY OF SSA/SDA

Missile warning systems during the cold war led to the birth of SSA/SDA information. At that time, the *U.S. Department of Defense (DoD)* was the only player who was actively involved in providing crucial information to satellite operators.

However, today that scenario has changed, with many commercial and state entities capable of SSA/SDA. This is largely due to the satellites orbiting in space increasing dramatically over the last, few decades. It is estimated that there are currently 2,787 satellites actively orbiting in space. For these reasons, the DoD SSA system and service is unable to continuously monitor all of the threats to each of these satellites all of the time.

Satellite operators also feel that the DoD SSA system and service cannot meet their demands for safer operations. Moreover, *NORAD's* two-line element set which has been used for decades for orbital determination is now considered inaccurate.

The increase in space debris due to human-caused disasters highlighted the need for a system that can precisely track space objects. One such disaster occurred when a Chinese retired weather satellite *FY-1C (Fengyun-1C)* was struck by a Chinese anti-ballistic missile test in January of 2007. The FY-1C spacecraft was completely destroyed in this collision which led to the creation of a cloud of more than 3,000 pieces of space debris.

A second major incident occurred in February of 2009, when a functioning U.S. *Iridium* communications satellite (*Iridium 33*) and a derelict Russian *Cosmos 2251* communications satellite (orbital altitude 800 km) collided. This collision resulted in 2,000 pieces of space debris into LEO. It is estimated that most of this space debris will remain in orbit for decades to come and that will pose a significant collision threat to satellites in **Low Earth Orbit** (LEO).

REASONS WHY SSA/SDA IS DEEDED

The increasing amount of space debris and satellites orbiting the Earth makes it clear that SSA/SDA is greatly needed, as 95 percent of currently tracked objects in space are dead payloads, stray hardware, rocket boosters, and other inert bodies. Usually, these objects are larger than 10 cm; however, it is known that there are millions of untracked objects smaller than that size in space. The need to continuously keep satellites operational is due to their fundamental role in monitoring infrastructure, GPS, communications, and national security.

The number of satellite operators/companies is also increasing, which demands a centralized SSA/SDA. Each year, hundreds of millions of dollars are spent to navigate the satellites and spacecraft safely in space. According to *Joint Space Operations Centre (JSpOC)*, in the past few years, there have been hundreds of thousands of satellite collision warnings.

Some of these warnings even indicated a collision probability of 44 percent and that misled satellite operators into making inaccurate decisions, such as propelling satellites into different orbits unnecessarily and consuming valuable resources, all the while potentially causing even greater risks.

CHALLENGES TO BE ADDRESSED IN SSA/SDA SYSTEMS

It is essential to address the challenges in the modern SSA/SDA system for effective space surveillance. The primary challenge is that some satellites do unpredictably change their orbits. During the past few years, many countries and companies have sought to increase their space mission capabilities. Certain activities such as electronic thrusting and automation alter the orbit of the satellite. These activities can cause the orbits to become non-Keplerian and difficult to predict.

Moreover, smallsats in LEO can change their orbits by positioning themselves in such a way that atmospheric drag is increased. These satellites significantly change their trajectory in such a way that is difficult to predict their new orbits.

Other challenges are related to the smaller size of electronics. Advancements in technology are making electronics smaller and more power-efficient and that entails the use of fewer solar panels and decreasing the size of satellites. The smaller the satellite is, the more difficult that unit becomes to detect with instruments such as telescopes or radar, or by other means. Such satellites include cubesats, which are becoming increasingly widespread in use. They are 10 cm cubed and difficult to track.

INTEGRATED OF SDRS INTO SSA/SDA SYSTEMS

What is an SDR? That acronym represents *Software Defined Radio (SDR)*, a radio communication system that employs software to implement the many functions that are required to receive and transmit radio signals.

The front end of an SDR contains the receive (**Rx**) and transmit (**Tx**) functions, such as those shown in *Figure 1*, to receive signals over a varying tuning range. These radio chains provide extremely high bandwidths of up to 3 GHz and independent ADCs/DACs for each channel. One of the highest bandwidth SDRs is **Cyan by Per Vices** which has 16 independent TX and RX chains and a tuning range from 0-18 GHz (upgradeable to 40 GHz). The digital back end of the SDRs contains an FPGA with on-board DSP capabilities. such as modulation, demodulation, upconverting, and down-converting, along with additional capabilities for DSP algorithms and radio protocols. (*See Figure 1 on the following page...*)

WHAT IS THE STATE-OF-THE-ART IN SSA/SDA?

In today's environment, where a large number of man-made satellites are already orbiting in space, it has become essential to have a complete, operational picture of SSA/SDA. Many companies are offering actionable insights by analyzing and combining the relevant data to support accurate decisions.

One such commercial SSA, offered by **Kratos Defense and Space**, has a global network of RF monitoring sites and sensors with more than 80 antennas. Other systems, such as the **Space Fence System (SFS)**, employ a considerable radar array to monitor space debris. Shown in *Figure 2*, SFS is the most recent program operated by the **U.S. Space Force**, becoming operational in March 2020. SFS will replace the aging U.S. based **AFSSS (Air Force Space Surveillance System)** which was installed in 1961.

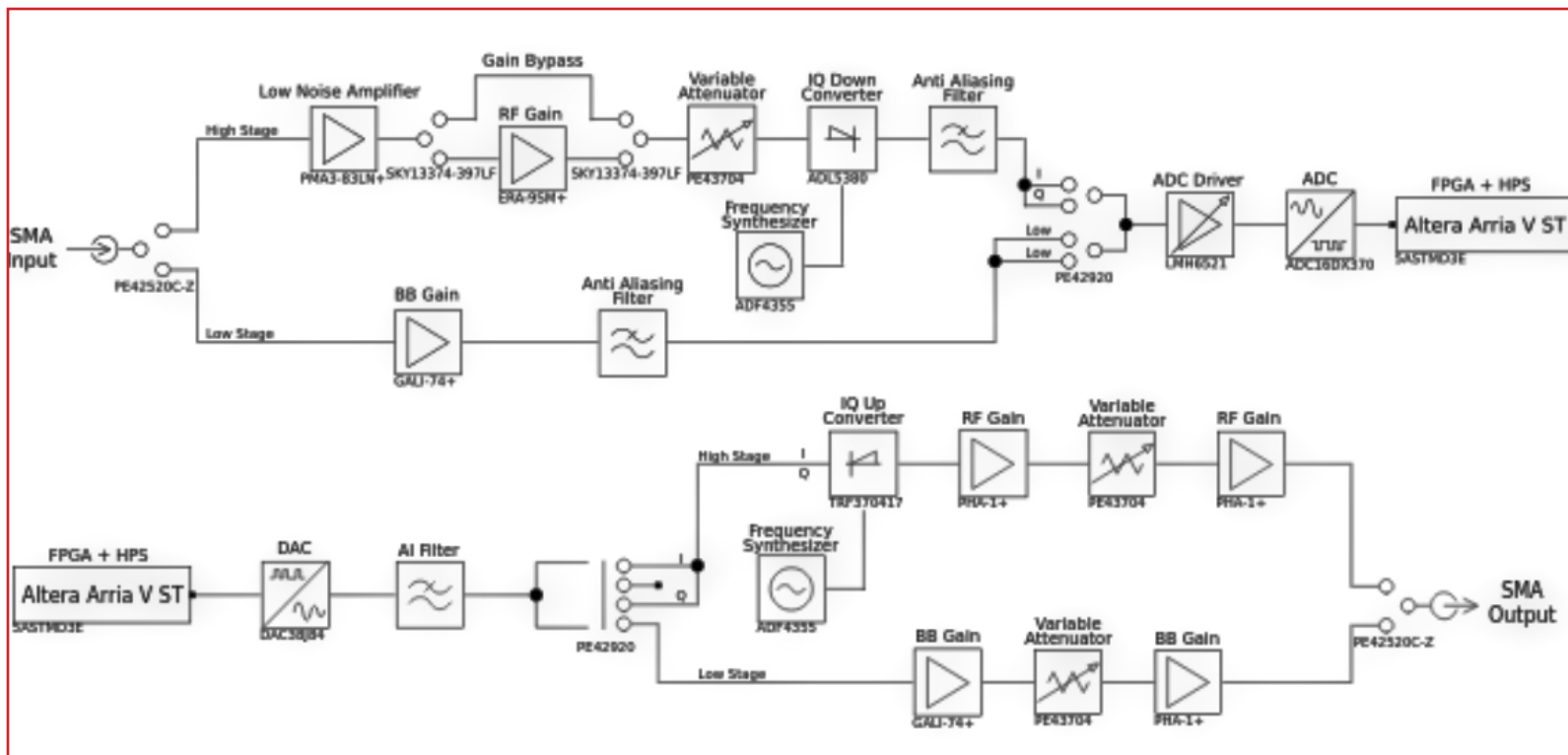


Figure 1: A high-level overview of Per Vices Rx (top) and Tx (bottom) boards is displayed.

This system provides information to the U.S. led **JSpOC (Joint Space Operation Center)**, which tracks space traffic and issues collision warning threats to global satellite operators. Based on these warnings, the satellite operators can move their spacecraft out of harm's way. An additional state-of-the-art systems that is currently being developed is Britain's **Deep-space Advanced Radar Capability (DARC)**, which will offer better accuracy, increased capacity and agile tracking.

Researchers from the **University of Arizona** have proposed an **SDIF (Space Domain Information Fusion)** model that defines six levels (ranging from 0 to 5) of an SDA system. In level 0, the raw data enters the system and is then stored in level 1. The data in the form of beliefs and knowledge is subjected to strict scrutiny in level 2 of the model. In level 3, users provide their questions and decision-making criteria. For instance, for one user, an object that is 1 km away from a space asset might be threatening, whereas another user may be comfortable with a space object that is 100 meters away from the space asset. Decisions based on the criteria defined in level 3 are made in level 4. Any result from level 4 that needs further information is passed to level 5, where sensors and information sources are instructed to collect new information. (See *Figure 2 on the following page.*)

CAPABILITIES OF MODERN SSA/SDA

Modern SSA/SDA equips satellite operators with all essential information that can almost guarantee a successful and safe operation in space. Modern SSA/SDA determines the orbit of another satellite or debris in the space as well as any change in the orbital trajectory of the satellite's propulsion/thruster. They also detect RF interference by offering real-time monitoring and detection of EMI, in addition to providing geolocation and mitigation strategies.

Today, SSA/SDA plays a fundamental role in satellite surveillance in space. These systems track the long-term performance of the satellite and provide access to its vulnerabilities. They also offer bandwidth services that include monitoring the efficiency of transponders, determine effectiveness, and assess anomalies in L-/S-/C-/X-/Ku-bands often used for satellite uplinking/downlinking.

NASA uses a tactical tool known as **CARA (Conjunction Assessment Risk Analysis)** to prevent collisions in space. CARA refers to the process of analyzing conjunction events to identify the associated threat to the asset. The main goal of CARA is to safeguard the orbital environment from the collision between NASA non-human space flight missions and other tracked and classified objects in orbit. The tactical tool analyzes the conjunction event to assess any related threat to the satellite.

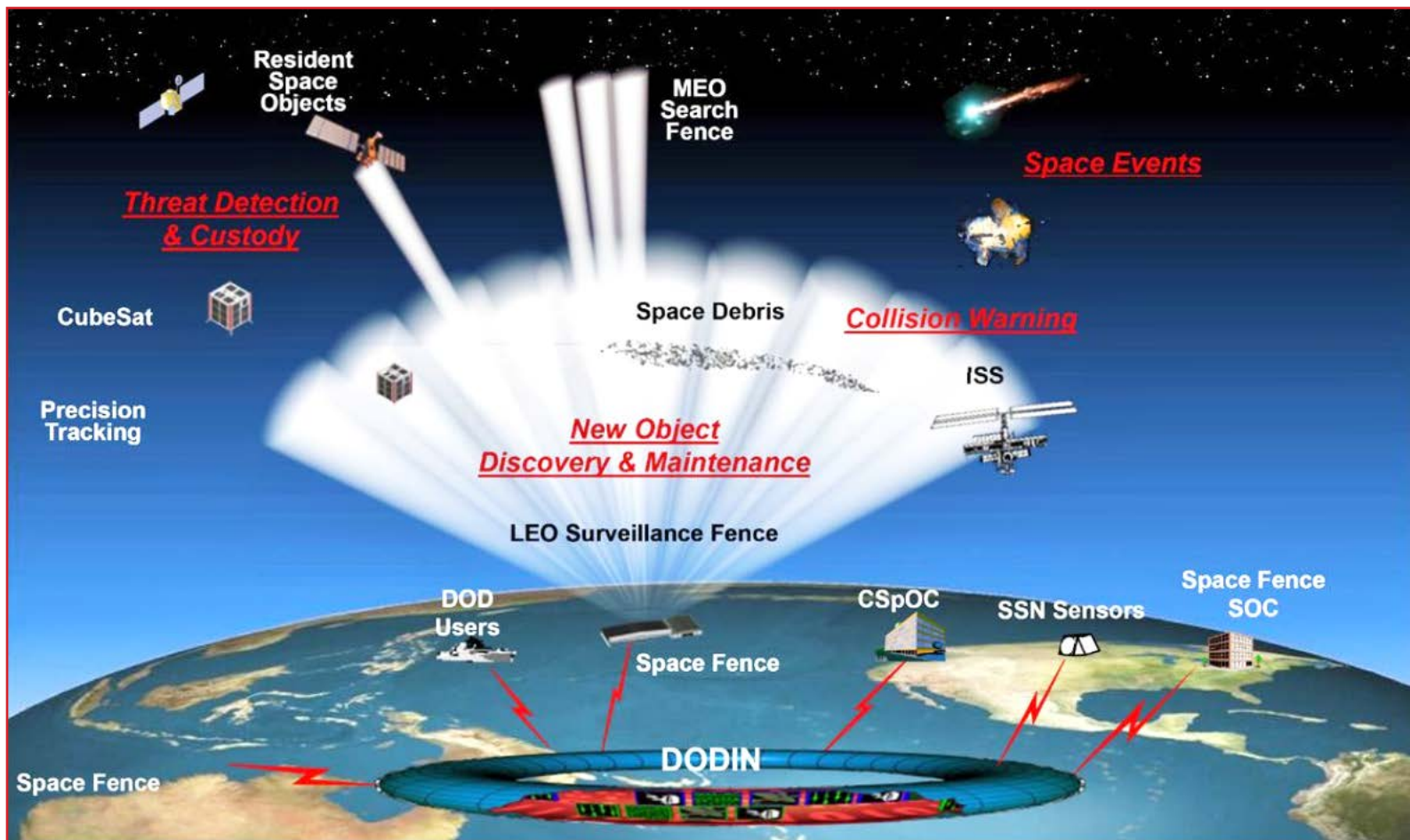
As an example, CARA helps to avoid incidents with a collision on launch assessment (**COLA**), essentially screening a powered flight trajectory against a catalog of pre-launch missions. This assessment system has the objective of establishing launch times/windows which are not forecasted to result in a close approach during flight.

THE SDRS ROLE IN SSA/SDA SYSTEMS

SSA/SDA systems can benefit from SDRs as they help to test and simulate uplink/downlink modulation or demodulation schemes employed in satellite positioning or ranging communications. They also help in inter-satellite tracking. FPGAs can execute DSP for different calculations in inter-satellite communication such as **received signal strength (RSSI)** and two-way ranges and Doppler shifts. These calculations help to estimate relative ranges between satellites in space.

Modern FPGA systems enable real-time adaptive beamforming for phased array radar used in such SSA/SDA systems. SDRs are characterized by their low noise floor and high SFDR for identifying weak signals in RSSI-based tracking systems. SDRs offer low latency and high throughput wireless links, vital for a timely delivery of SSA/SDA data to satellite operators.

Companies, such as Per Vices, are offering the lowest latency SDRs, which are capable of meeting or exceeding customer needs for low latency requirements. Phased array radars employed in satellite tracking ground stations require **MIMO (Multiple Input Multiple Output)** capabilities. Per Vices also offers **MIMO SDR** which employs MIMO technologies. MIMO SDRs by Per Vices, like that pictured in Figure 3, possess as many as 16 RF channels for MIMO operations and dynamic configurations.



Legend

CSpOC - Combined Space Operations Center
DOD - Department of Defense
DODIN - Department of Defense Information Network
ISS - International Space Station

LEO - Low Earth Orbit
MEO - Medium Earth Orbit
SOC - Space Fence Operation Center
SSN - Space Surveillance Network

Tens of thousands of objects are present orbiting around the Earth. SDA/SSA helps to develop and maintain comprehensive data of the location and nature of the objects present and plays an active role in identifying orbital debris to reduce the risk of collision in space with satellites and/or space shuttles.

SDRs are playing a significant role in this field, due to the high performance capabilities in both the radio front end and the digital backend featuring an FPGA for advanced DSP.

www.pervices.com/

A highly responsive and accurate SDA/SSA system is often driven by advanced algorithms and a diverse global network of radar systems and telescopes is used to supports the decision-making process of satellite operators. Timely decisions based on reliable information provided by SSA/SDA system culminate in the success of satellite missions in space.



Figure 3: Per Vices' Cyan is an SDR that allows MIMO.

Author *Brandon McHugh* is a Field Application Engineer and Technical Writer at Per Vices. He possesses a degree in theoretical and mathematical physics from the University of Toronto.

Author *Rafia Shabbir* is a top rated technical writer and educational content developer who is passionate about writing on software, tech and educational topics.



Brandon McHugh