2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

WELCOME TO

Day 3 | Thursday April 23

Fueling Space Dominance with Data & AI

event website

Cyber Readiness at the Speed of Space

Concurrent Activities

Cyber & AI Technologies Show and Tell

Location: Bldg 270, GCC 1
1000-1500, All Days

Experience the cutting edge of cyber security, AI, & IT through hands-on activities to touch, test, and explore the latest technologies. This interactive session offers a unique opportunity to engage with real world solutions to gain firsthand insight into the latest advancements in threat detection, defense mechanisms and IT capabilities.Be sure to visit the student interns presenting their SSC Cyber research and findings.

Vendor Exhibitors

Location: Bldg 270, Lobby & Courtyard
0900-1500, All Days

Visit 50 industry partner and Department of War (DoW) booths for information and partnership opportunities. Learn more about SSC mission areas, programs, and Deltas at the Space Force Front Door Booth!

The Blooming Space Van

Location: Outside of BX
1000-1400, All Days

We know conferences can sometimes be info-overload so don't burn out! Stop by the wellness van for a quick reset with breath work, tapping, aromatherapy, and other restorative experiences designed to help you recharge and refocus.

Lunch & Learn AI Workshop

Location: Bldg 270, Daedalian Room
1130-1230

Grab your lunch and head to the breakout room to connect with experts delivering our next-gen cutting-edge Generative AI tools. Deep dive into enterprise solutions through live demonstrations of key capabilities and get tailored answers to your specific use cases to determine which tools best support your mission needs.

1130-1150: Microsoft | 1150-1210: Edgerunner | 1210-1230: SpaceGPT & GenAI

2026 SSC CYBER EXPO PROGRAM ROADMAP

DAY 3- April 23

Fueling Space With Data & AI

Special Guest Speakers

Dr. Jose Angeles
Chief Data Officer
US SOUTHCOM

Ms. Alissa Knight
Founder & CEO, Chief AI Officer of Assail, Author, 6x Award Winning Film Producer

Event Website

Day 3: Fueling Space with Data & AI

Morning Schedule

- **0900 - 0905** Introductions
- **0905 - 0910** Welcome Remarks
  Mr. Bartley Stewart, SSC CDAO
- **0910 - 0935** Combatant Command Leadership Address
  Dr. Jose Angeles
- **0935 - 1005** Industry Keynote Address
  Ms. Alissa Knight
- **1005 - 1020** Break! Visit Exhibitors
- **1020 - 1100** Panel: DoW Data & AI leaders reveal mission-focused AI applications, strategies, programs, and partnerships
- **1100 - 1130** USSF AI Hub
- **1130 - 1230** Lunch & Learn AI Workshop
  Microsoft: 1130-1150
  Edgerunner: 1150-1210
  SpaceGPT & GenAI.Mil: 1210-1230

Special Guest Speaker

SSC.S6.CyberExpo@spaceforce.mil

Cyber Readiness at the Speed of Space

Detailed agenda available on website

Day 3: Fueling Space with Data & AI

Afternoon Schedule

- **1230 - 1300** Data as a Weapon System
- **1300 - 1400** Panel: Human-AI Teaming (HAT)
  - HAT Tools, Apps, & Processing Lab
  - Human-Machine Teaming Across DoW
  - Human Readiness Levels for Human-Machine Teaming
  - Measuring the Impact of AI via Joint Activity Testing
  - Real-Time Team Optimization
- **1400 - 1415** Break! Visit Exhibitors
- **1415 - 1545** AI Tools in Action: Day in the Life of a Guardian Powered by AI
- **1545** Closing Remarks & Complimentary Ice Cream

Enjoying the Expo?
Give us Feedback
Scan the QR Code

Questions? Contact us SSC.S6.CyberExpo@spaceforce.mil

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Welcome Remarks

Mr. Bartley Stewart

Space Systems Command, Chief Data & AI Officer

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Combatant Command Leadership Address

Dr. Jose O. K. Angeles
Chief Data Officer
United States Southern Command (USSOUTHCOM)

Cyber Readiness at the Speed of Space

United States Southern Command

Dr. Jose O. K. Angeles
Command Chief Data Officer

THE OVERALL CLASSIFICATION OF THIS BRIEF: UNCLASSIFIED

Distribution Statement A. Approved for public release: distribution is unlimited.

CAO: 20 Mar 26

U.S. Southern Command Headquarters

Gen Francis Donovan
Combatant Commander

SgtMaj Rafael Rodriguez
Senior Enlisted Leader

Lt Gen Evan Pettus
Deputy

AMB Stephanie Syptak-Ramnath
Foreign Policy Advisor

MG Javier Reina
Director for Mobilization and Reserve Affairs

MajGen Julie Nethercot
Chief of Staff

J1
Manpower and Personnel

J2
Intelligence

J3
Operations

J4
Logistics

J5
Strategy, Policy, & Plans

J6
Communications Systems

J7/9
Exercises & Coalition Affairs

J8
Resources and Analysis

J5 Deputy
United Kingdom

J5 Deputy
Brazil

J7/9 Deputy
Colombia

Partnership for the Americas!

Vision

U.S. Southern Command is a mission-ready and trusted partner that works collaboratively to ensure the Western Hemisphere is secure, free, and prosperous.

Mission

U.S. Southern Command deters aggression, defeats threats, rapidly responds to crises, and builds regional capacity, working with our allies, partner nations, and USG team members to enhance security and defend the U.S. homeland and our national interests.

CCDRs Priorities

- Reshape the U.S. Southern Command Headquarters for strategic operations at range, speed, and scale
- Impose total systemic friction on Drug Trafficking Organizations
- Develop and field modernized forces that leverage autonomous systems to increase lethality, domain awareness, and data sharing with allies and partners
- Deny adversary footholds and malign influence in the hemisphere

U.S. Southern Command Enterprise

U.S. Southern Command Headquarters

Doral, FL

- U.S. Air Forces Southern (AFSOUTH)
  Tucson, AZ
- U.S. Army South (ARSOUTH)
  San Antonio, TX
- U.S. Marine Corps Forces South (MARFORSOUTH)
  New Orleans, LA
- U.S. Naval Forces Southern Command (USNAVSO)
  Mayport, FL
- Special Operations Command South (SOCSOUTH)
  Homestead, FL
- U.S. Space Forces South (USSFSOUTH)
  Tucson, AZ
- Joint Interagency Task Force – South (JIATF-S)
  Key West, FL
- Joint Task Force Guantánamo (JTF-GTMO)
  Naval Base Guantanamo, Cuba
- Joint Task Force Bravo (JTF-Bravo)
  Soto Cano, Honduras
- Joint Task Force SOUTHERN GUARD (JTF-SG)
  Naval Base Guantanamo, Cuba

- U.S. Coast Guard Southeast District (Formerly District 7)
  Miami, FL
- U.S. Coast Guard Southwest District (Formerly District 11)
  Alameda, CA
- 22 U.S. Military Groups (MILGROUP)
  22 Senior Defense Officials
  Based in Embassies throughout the region

Partnership for the Americas!

Partnerships in Action

Military and DoW Organizations


Navy


Air Force


Army


Marine Corps


Space Force


Coast Guard


SOCOM


DIU


DTRA


National Guard

Allied and Partner Nation Liaison Officers


Argentina


Brazil


Canada


Chile


Colombia


Ecuador


France


Great Britain


Guatemala


Netherlands


Panama


Paraguay


Peru

Intelligence Community


DIA


NGA


CIA


NSA


NRO

Interagency Partners


Department of State


Department of Homeland Security


Federal Bureau of Investigation


Drug Enforcement Administration


Alcohol, Tobacco, Firearms, and Explosives


Department of Commerce


Department of Treasury


Department of State Diplomatic Security Service


DHS Immigration and Customs Enforcement


Department of Health and Human Services


U.S. Secret Service


Export-Import Bank of the U.S.


U.S. International Development and Finance Corporation


Inter-American Development Bank

Academic Institutions


William J. Perry Center


Inter-American Defense College


WHINSEC


Inter-American Air Forces Academy


NAVSCIATTS


Carnegie Mellon University


Florida International University


University of Miami


Arizona State University


Massachusetts Institute of Technology

Partnership for the Americas!

Challenges to US and Partner Nation Security

Data Analytics and Artificial Intelligence Adoption

- **Vision – Mature SOUTHCOM to a Data Driven Organization**
- **Mission**
  - **Increase Efficiency & Effectiveness across the Command**
  - **Reduce Risk to Mission & Risk to Force via Data Driven Leadership**
  - **Enable Joint Force /Global Integrated Operations**
- **Business Data Analytics – ADVANA (War Data Platform)**
- **Mission Data Analytics – Maven Smart System**
- **Agentic Workflow Solutions**
  - **GenAI or AskSage**
- **Remaining Challenges**
  - **Whole of Government Interoperability**
  - **Continuous Training of the Workforce at all Levels**

(U) Relevant, accurate, and timely data significantly enables decision advantage and reduces risk to mission and risk to force

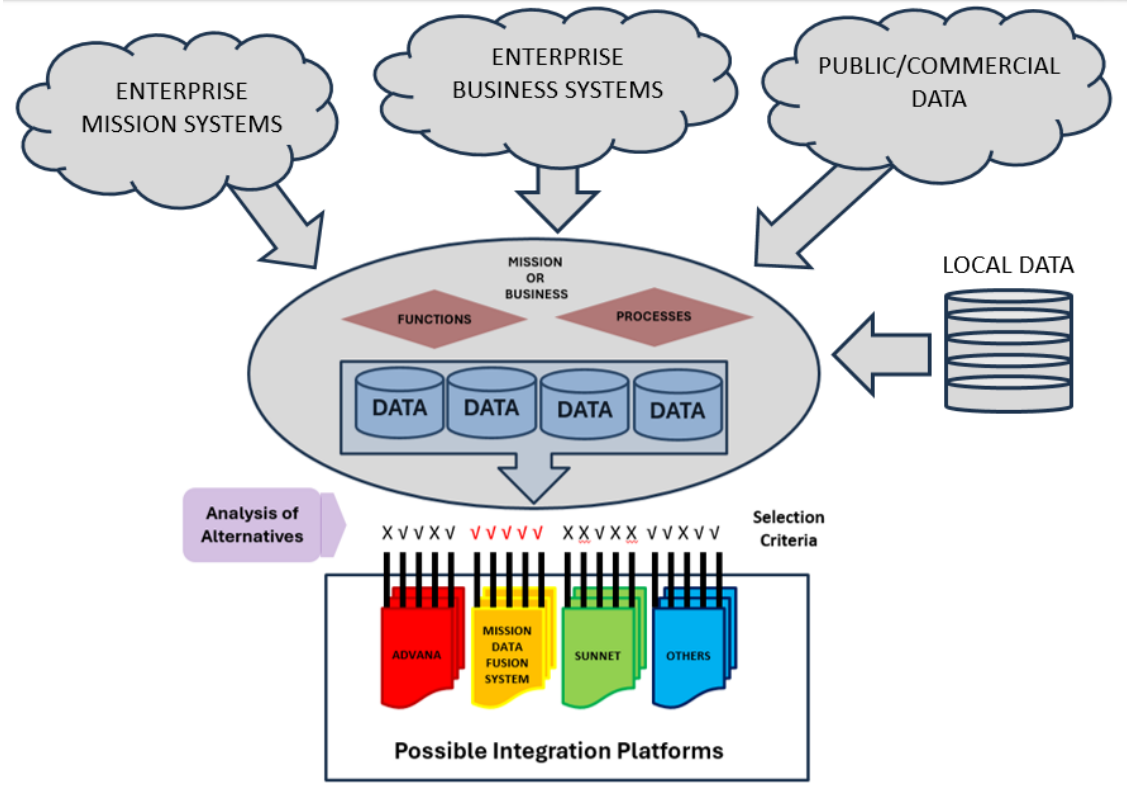
Data Analytics and Artificial Intelligence Adoption Process

- Address data visualization and analytics problems across business and mission activities through:

  - LOE 1 – Data Governance
  - LOE 2 - Data Assessment and Inventory, and Cataloging
  - LOE 3 – Data Stewardship and Quality
  - LOE 4 - Implementation of visualization, analytics, and AI solutions that address specific business and mission use-cases

Generalized Data Sources

Disparate Systems with Limited Visualization, Analytics and AI



Means for Data Visualization, Analytics and AI

Science and Technology

SOUTHCOM Science, Technology and Innovation conducts Joint and Combined experimentation and prototyping to discover innovative technical solutions to counter mutual threats and challenges, improve interoperability, and strengthen partnerships with our allies and partners.

SOUTHCOM – a "Hub of Innovation"

- Conduct multi-lateral Test and Evaluation (T&E) in a permissive, geographically relevant environment
- Train with US, NATO, & SOUTHCOM Partner Nations
- Increase interoperability, improve C2, data/comms and network security
- Enhanced Domain Awareness…for all SOUTHCOM Partner Nations

- **Respond Together**
  - Co-develop tech solutions with our trusted partners. Build defense industrial bases jointly
  - Combat influence of malign state actors
  - Improve Defense, Energy, & Environmental Security
  - Humanitarian Assistance and Disaster Relief

Science & Technology Priority Areas

- **Enhance Capabilities**
  - Long dwell ISR
  - Counter-UAS
  - Autonomy and Robotics
  - Advanced sensors
  - Contested Logistics
- **Secure Communications and Information Networks**
  - Cyber protected networks
  - AI/ML for improved data management, analytics, and dissemination
  - High speed communications and Future G
- **Joint and Combined Research, Development, Test, and Evaluation**
  - Collaboration in scientific and basic research
  - Co-development and cost sharing for cost-effective military capabilities
  - *Establishment of bilateral Research, Development, Testing and Evaluation (RDT&E) Agreements*
- **Increase operational capabilities and improve interoperability**
  - Expand Coalition Warfare Program (CWP) and Foreign Comparative Test (FCT) Program
  - *Expand OCONUS testing and evaluation in multi-lateral exercises with Partner Nations (PN)*

Exercises & Coalition Affairs – Opportunities for Evaluation

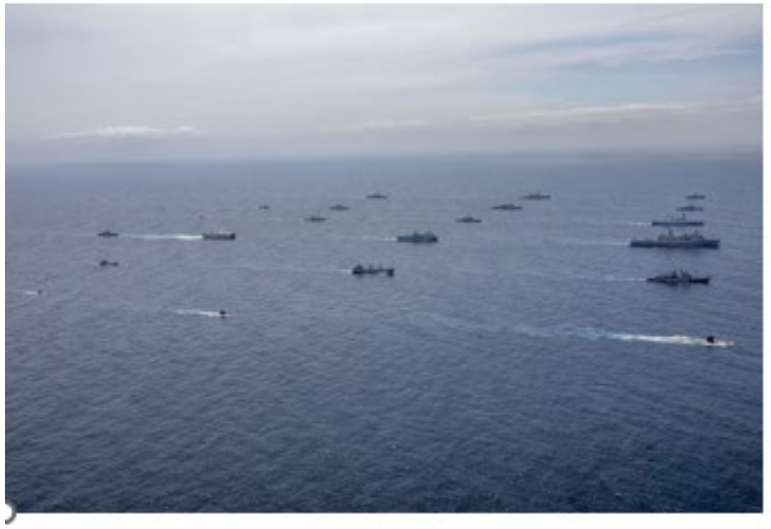
Joint Exercises Program (JEP) – Principal means for CCDR to train & ready forces; provides access, presence, and influence; lever to integrate allies/partners

- 8-9 exercises annually: 15,000 personnel / 35 countries
- Exercise Scenarios > Shared mutual interest
- Humanitarian Civic Assistance: Field Training Exercises
- Operational and Foreign Military Interaction (FMI). Joint Force WHEM
- Exercise Related Construction:

- PANAMAX (FY/26 PAN) – 2000 personnel / 20 countries
- SOUTHERN STAR (FY25/27 CHL) – 2000 personnel / 6 countries
- UNITAS (FY25 USA/26 PER) – 4300 personnel / 15 countries
- TRADEWINDS (FY25 TTO/FY26 ATG) – 1200 personnel / 24 countries
- CENTAM GUARDIAN (FY25 GTM/FY26 SLV/FY27 HON**) –** 1100 personnel / 6 countries
- FUSED RESPONSE (FY25 ARG/FY26 TBD) - 200 personnel / 2-3 countries
- FUERZAS COMANDO (FY25 SLV/ FY26 PRY/BLZ 27) – 500 personnel / 18 countries
- INTEGRATED ADVANCE (FY25 USA) – 1000 personnel / USSOUTHCOM
- RESOLUTE SENTINEL (FY26 BRA) – 1500 personnel / 10 countries

Humanitarian Assistance - To relieve or reduce endemic condition such as human suffering, disease, hunger, and adverse effects of UXO

- HAP is Military to Civilian program
- Four Sectors: Disaster Preparedness & Mitigation, Health, Education, Humanitarian Mine Action
- 5 Year HAP snapshot: 1,147 Projects
- Modular Field Hospitals: 72 /
- Rapid Modular Deployable Bridges: 2 countries
- Demining/Ordinance Disposal/Stockpile Management:



(U) USSOUTHCOM Exercises and Coalition Affairs Directorate leverages "Whole of Society" partnerships to deter aggression, rapidly respond to crisis, and build partner capacity through Humanitarian Assistance, Civil Affairs, Interagency Coordination, Individual Training & Readiness, and the Joint Exercise Program.

What is a Joint Integrated Space Team (JIST)?

- Mission:
  - JISTs *educate*, *integrate*, *advocate*, and *communicate* space issues within their respective host CCMD's staff to facilitate effective global (and regional) space operations

- CDR SPACECOM Intent:
  - *Seamlessly integrate* across the CCMD staff, allies, and mission partners at the strategic and operational levels
  - Support host CCMDs by *assisting* and *enabling* supported and supporting OAIs across competition and conflict

- Tasks:
  - Liaison between CDR USSPACECOM and CDR USSOUTHCOM
  - Support other host CCDR requirements as needed (*be* "*value added*")

- JIST SOUTH:
  - Director - Col John Kolb
  - Deputy Director - Mr. Paul F. Dudley,

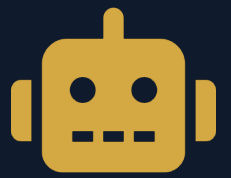
Overall Message

- Specific Data, Analytics, and AI transformation efforts must be tailored to the processes of a given organization

- Space Systems Command can test Minimum Viable Products in SOUTHCOMs permissive and geographically relevant environments

- Work via your Space Command/Space Force LNOs at SOUTHCOM and the J7/9 Science and Technology Team to evaluate/operational test new capabilities in either real world or exercise environments

Introduction of AI and Cyber in Technology Life Cycle Environments and Processes



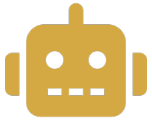
Perspectives for DoW Acquisition

Dr. Jose Angeles
USSOUTHCOM Chief Data Officer
USAF Acquisition Alumni

Objectives

Frame Complexity

Understand the complexity of a given technology environment across its full lifecycle
— from users to developers to sustainment teams.



Cyber & AI Impact

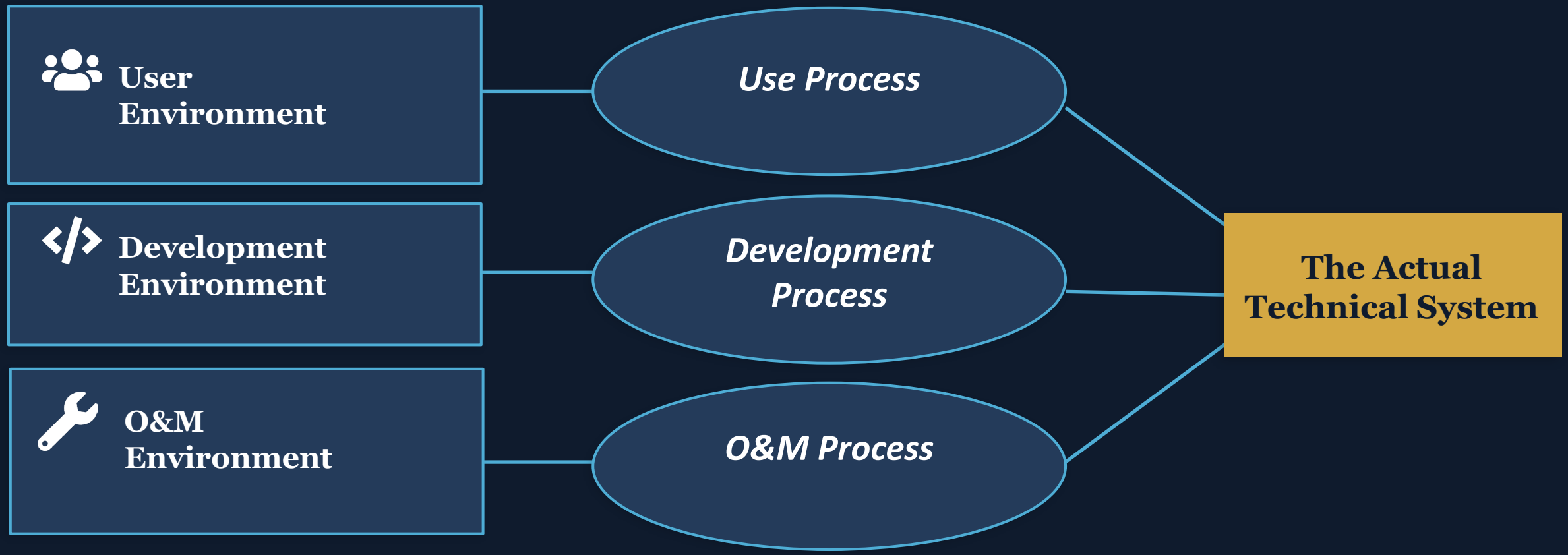
Introduce how cybersecurity requirements and AI capabilities have fundamentally changed each phase of a given technology’s environment.

AI Categories – Not All Inclusive

- Data Visualization / Data Analytics Tools
- Data Scraping and Classification Tools
- Named Entity Recognition Tools
- Object Detection Systems (Computer Vision) Tools
- Generative AI / Large Language Models
- Agentic AI Tools to Perform Tasks
- Speech Recognition and Text-to-Speech Tools
- Recommendation Systems
- AI-Powered Chatbots and Conversational AI Tools
- Sentiment Analysis Tools
- AI for Robotics
- AI for functions such as Cybersecurity, Finance, Health, Predictive Maintenance

A Life Cycle Model for Technical Systems

Ives et al. (1980) — Adapted for Modern Acquisition



Each environment and associated process has distinct cyber attack surfaces and AI integration opportunities

Ives B., Hamilton S., Davis, G. (1980); A Framework for Research in Computer-*Based Management* Information Systems; Management Science, Vol. 26, No. 9 (pp. 910-934)

Importance for DoW Acquisition

Growing Attack Surface

Every phase of delivery introduces cyber risk — from dev pipelines to fielded systems to sustainment networks.

AI Is a Force Multiplier

AI accelerates capability in every phase — but also introduces new vulnerabilities and dependency risks.

Shift-Left Imperative

Cyber and AI decisions made at requirements and design phases have cascading effects through the entire lifecycle.

Adversary Pacing Threat

Near-peer adversaries are integrating AI and exploiting cyber gaps faster than traditional acquisition timelines allow.

User Perspectives

Use Process

- Do users understand the system?
- Is it easy to use? Is it useful?
- Is use mandatory? Are users trained?
- What is the user operational experience base?

Is cyber protection part of the Use Process?

How are different types of AI part of the Use Process?

User Environment

- Is there training?
- Is there leadership support?
- Is it used by all or some of the organization?

Are cyber component explicitly explained?

Are AI components explicitly explained

Development Perspectives

Development Process

- Is there technology governance?
- Is there orderly progression from requirement to delivery (ITIL)?
- Do the tools exist (lab environment)?

Are cyber threats modeled and capabilities embedded from system inception?

Are AI capabilities embedded from inception? Are AI tools used to accelerate development?

Development Environment

- Are developers keeping up with technology trends?
- What are the developer skill sets?
- Can developers build systems that match requirements?
- Are there resources for the right tools?
- Does leadership understand the complexity?

Are cyber threats assessed during development?

Are AI tools used to speed up development, updates, and testing?

O&M Perspectives

O&M Process

- Are there standards/explicit expectations?
- Are appropriate resources (spares, tools, etc.) available?

Are cyber threats continuously addressed?

Is AI used to speed up/assist in operational availability?

O&M Environment

- Is the O&M organization the right size?
- Are they the right structure?
- Is there continuous training?
- What type(s) of OEM vendor support exists?

Are there means to assess cyber threats?

Are evolving AI tools introduced to enhance O&M?

Cyber Across the Technology Lifecycle

User

- Phishing & social engineering
- Credential management
- Insider threat
- Zero trust access

Development

- Supply chain attacks
- Code vulnerabilities
- CI/CD pipeline security
- Threat modeling

O&M

- Continuous monitoring
- Patch management
- Incident response
- Vendor risk management

KEY INSIGHT: Cyber must be resourced and planned across all three environments — not just the system itself

AI Across the Technology Lifecycle

User

- Intelligent decision support
- Natural language interfaces
- Automated workflows
- Trust calibration training

Development

- AI-assisted coding
- Automated testing
- Synthetic data generation
- MLOps infrastructure

O&M

- Predictive maintenance
- Anomaly detection
- Automated log analysis
- Intelligent help desk

KEY INSIGHT: AI integration requires data architecture and governance planned from Day 1 of acquisition

Key Takeaways

1. Technology Life Cycle Complexity is multi-dimensional — the Ives model helps us think about User, Development, and O&M environments as distinct but interconnected domains.

2. Cyber must be embedded from inception in every environment — not bolted on after system development. Resource it across the full lifecycle.

3. AI is both a capability and a tool — architect for AI integration in your system AND leverage AI to accelerate your development and sustainment processes.

4. Data is the foundation — without a deliberate data strategy from Day 1, neither effective cybersecurity analytics nor AI capabilities are achievable at scale.

2026 SSC CYBER EXPO

Industry Keynote Address

Ms. Alissa Knight

Click here for Presentation Slides

alissaknight.com

Founder, CEO, and Chief AI Officer of Assail, a venture-backed cybersecurity and artificial intelligence company building agentic AI systems for continuous exposure management of modern application stacks. With more than 26 years at the forefront of offensive security including U.S. intelligence cyber operations, she is globally recognized for uncovering systemic vulnerabilities in critical infrastructure and translating adversarial insight into defensible, scalable technology. She has advised the Pentagon and U.S. Marine Corps on API and application security and is the author of *Hacking Connected Cars* (Wiley). She's a 6x Telly award winner for television production and was successfully inducted into The Mob Museum where her hacking tools and laptop are permanently exhibited as part of the museum's global cybercrime collection.

2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

BREAK

VISIT EXHIBITORS!

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

PANEL

Data & AI Leadership

Moderator: Mr. Jorge Rativa, Lead Cyber Automation Engineer, SSC/S6

Panelists:

- **Mr. Michael Ficken**, Combat Forces Command Chief Digital AI Office (CDAO)
- **Mr. Bartley Stewart**, SSC CDAO
- **Dr. Jose Angeles**, U.S. SOUTHCOM CDO
- **Mr. Corey J Sinnott**, U.S. SPACECOM CDAO Senior Data Scientist
- **Col Robert Enrico**, Vice Chair of the SSC Data and AI Board

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

USSF AI Hub

Capt Drake Williams

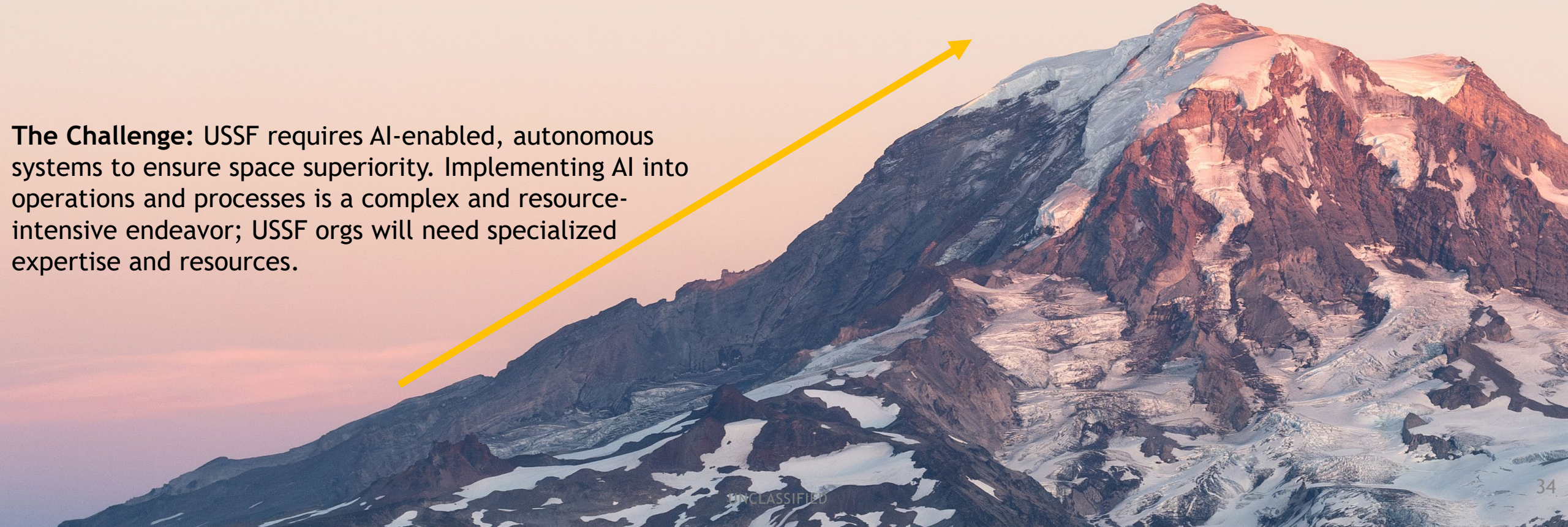
BMC3I, SYD 85, I3E Program Manager

Cyber Readiness at the Speed of Space

AI Hub Executive Summary

The Solution: Establish a centralized **USSF AI Hub** to drive AI/ML implementation service-wide. This will decrease the burden on mission owners, eliminate duplicate efforts, consolidate investment, and accelerate AI adoption across all USSF mission areas.

The Challenge: USSF requires AI-enabled, autonomous systems to ensure space superiority. Implementing AI into operations and processes is a complex and resource-intensive endeavor; USSF orgs will need specialized expertise and resources.



Strategic Context

Executive Order 14719, Jan 2025

"It is the policy of the United States to sustain and enhance America's global Artificial Intelligence (AI) dominance in order to promote human flourishing, economic competitiveness, and national security."

AI Strategy for Department of War, Jan 2026

"In the national security domain, AI-enabled warfare and AI-enabled capability development will re-define the character of military affairs over the next decade. This transformation is a race - fueled by the accelerating pace of commercial AI innovation coming out of America's private sector."

USSF Data & AI FY2025 Strategic Action Plan

"In this contested and congested domain, superiority will be defined by our ability to integrate with interagency, allies, and commercial partners to advance data capabilities, real-time analytics, and emerging AI technologies to outpace adversaries and maintain operational superiority."

Types of AI

Focus of USSF AI Hub

	Level 1 - Enterprise AI Foundational LLM Tools	Level 2 - Functional AI Grounded & Tailored LLM Tools	Level 3 – Mission-Specific AI Algorithmic Data Processing
Description	• Large Language Models (LLMs) & Agents • General-purpose tools for everyday office tasks • "Off-the-shelf" AI for broad productivity across the organization	• Grounded or Fine-Tuned LLMs & Agents • Customized and trained on specific, internal USSF data • Acts as an "expert" for specific teams, providing accurate and relevant answers.	• LLMs, Agents, Classical AI/ML, Multi-Modal • Specialized AI built for critical, core operational missions • Process vast amounts of mission-specific data • Automates complex decisions and predictions in real-time
Example Use Case	• Quickly summarize long reports, draft routine emails, or find information in technical documents.	• Contract drafting, proposal evaluation, interaction with intel data, ATO automation, cybersecurity monitoring, etc	• AI system that automatically analyzes satellite imagery to identify and track objects in space • AI system that predicts potential satellite malfunctions before they happen.

AI Hub will focus on USSF-specific requirements and align with DOW & DAF enterprise efforts

AI Hub Core Services

AI Personnel

Expertise - A dedicated team to assist mission owners and conduct outreach
Test & Evaluation, Cybersecurity - A repeatable AI validation framework
Partnerships - A central point for coordinating with FFRDCs, industry, and academia

AI Solutions

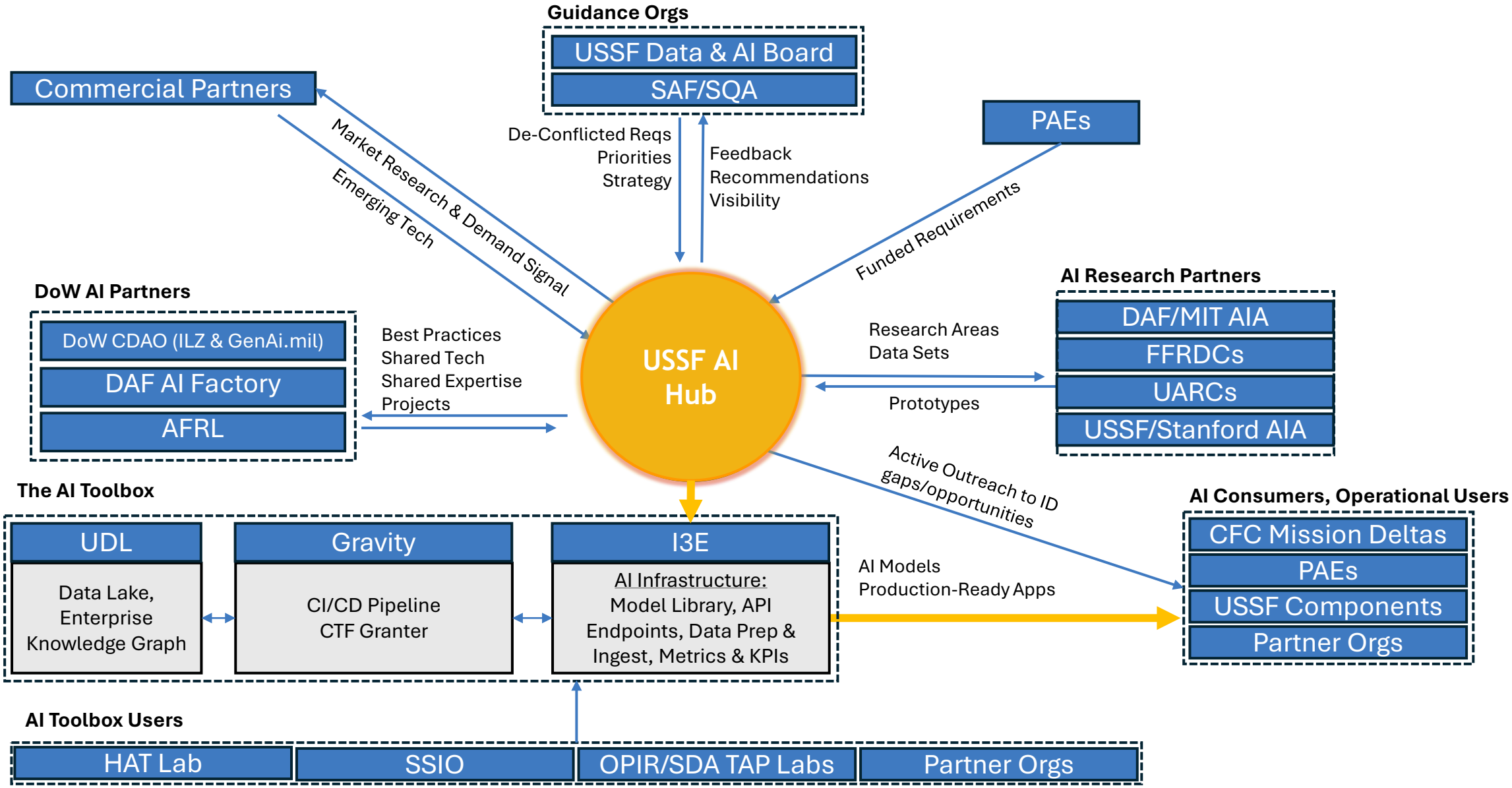
Hosted Capabilities – Production-level solutions and prototypes for mission owners

AI Platform

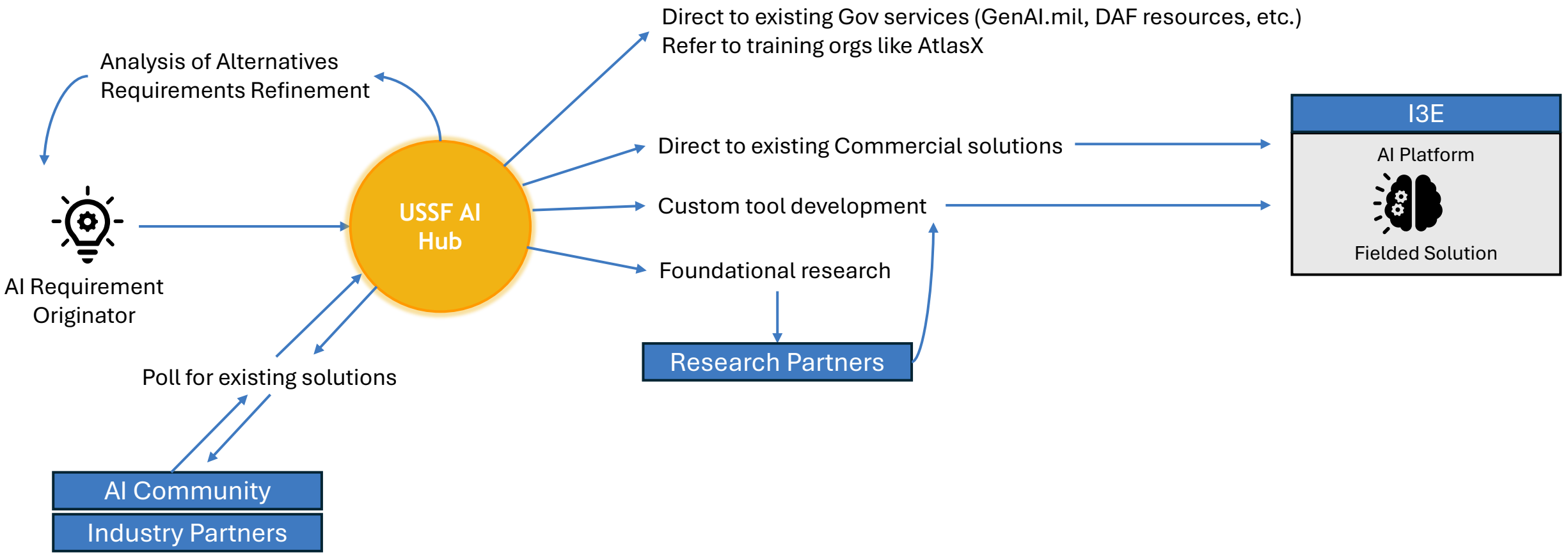
Rapid Onboarding - Accredited, production-level environments to field commercial AI tools
Development Infrastructure – USSF data connections, accredited models
Compute Power - Cloud-based or on-prem GPUs at all classification levels
Test & Evaluation, Cybersecurity Infrastructure – Accreditation pipeline, custom T&E benchmarks

AI HUB ENABLES RAPID, RESPONSIBLE FIELDING OF AI

AI Hub Relationship Map



AI Hub Process



- The goal is to direct requirement owners to existing resources and only undertake custom development when necessary
- This process helps requirement originators short-circuit the learning curve for AI, AI hosting, and AI accreditation

AI HUB PLATFORM
OBJECTIVE OV-1

I3E

Available Now | Available Fall 2026 | Future State

Data Sources & Connections
- Unified Data Library
- User Uploads
- meshONE-T
- Azure ExpressRoute

I3E Commercial	I3E Gov – IL5	I3E Secret – IL6	I3E TS/SCI	I3E SAP
AI Dev & Test ML DevOps Pipeline Pilots & Prototypes	AI Dev & Test ML DevOps Pipeline Pilots & Prototypes	AI Dev & Test ML DevOps Pipeline Pilots & Prototypes	AI Dev & Test ML DevOps Pipeline Pilots & Prototypes	AI Dev & Test ML DevOps Pipeline Pilots & Prototypes
AI Model Repository	Production AI Storefront Mature AI/ML Tools	Production AI Storefront Mature AI/ML Tools	Production AI Storefront Mature AI/ML Tools	Production AI Storefront Mature AI/ML Tools
Data Hub	AI Model Repository	AI Model Repository	AI Model Repository	AI Model Repository
	Data Hub	Data Hub	Data Hub	Data Hub
		Ops AI/ML Servers	Ops AI/ML Servers	Ops AI/ML Servers

CDS between I3E Commercial and I3E Gov – IL5

CDS between I3E Gov – IL5 and I3E Secret – IL6

CDS between I3E Secret – IL6 and I3E TS/SCI

CDS between I3E TS/SCI and I3E SAP

Internet, NIPR, SIPR, JWICS, other direct connections

Enterprise & Functional Users

STAR COMMAND

SPACE SYSTEMS COMMAND

- Acquirers
- Vendors & Commercial Partners
- Testers & Trainers
- TAP Labs
- DoD Partners

Operational Users

USSF COMBAT FORCES COMMAND

UNITED STATES SPACE COMMAND

- C2 Systems
- MW/MT Systems
- SDA Systems
- PNT Systems
- COCOMs

I3E-Fielded AI/ML Algorithms

AI Hub Recent Use Cases

CFC Epic Fury Support

CFC CDAO needs to analyze commercial SDA data to:

- Analyze pattern of life
- Detect jamming
- Detect sat movements

CFC does not have access to a compute environment.

AI Hub is providing access to I3E Commercial with pre-existing connections to UDL.

Contract Warrant Prep

SSC/PK needs an AI application to prepare COs for their warrant boards more efficiently.

SSC/PK lacks AI expertise, access to a production environment, and a contracting pathway.

AI Hub assisted SSC/PK with an informal AoA and will provide a contracting pathway, accreditation, and ensure enterprise alignment.

Acq Candidate Eval

SAF/SQD needs an automated mechanism to assess officer records. A Guardian self-coded a grounded LLM application.

The self-coded application needs to be accredited for PII and hosted at IL5.

AI Hub is helping accredit and field this application to I3E IL5.

On-Prem Experimentation

SSC/S6 needs on-prem NVIDIA DGX Sparx platforms to conduct cutting-edge experiments.

S6 lacks contracting pathways and funding for dedicated AI compute resources.

AI Hub is funding and acquiring 10 GPUs to enable rapid, low-overhead prototyping for eventual fielding into I3E.

Thank You!

For more information, please contact:

Capt Drake Williams
AI Hub & I3E Program Manager
drake.williams.3@spaceforce.mil

Camilla Wu
AI Hub & I3E Deputy PM
camilla.wu@spaceforce.mil

Lt Devrin Chullandana
AI Hub Deputy Program Manager
devrin.chullandana.1@spaceforce.mil

Luke Shellhorn
I3E Architect
shellhorn_luke@bah.com

Michael Moniger
I3E Technical Lead
moniger_michael@bah.com

Thursday, April 23rd
Dining Options

BX Restaurants
Tenkatori
Gusto's
Coffee & Bakery

Food Trucks
Chicken King
Ice cream (Dip Deez)

South Bay Bar & Grill
$15 Buffet Special
Fried or baked fish
2 sides & Hush Puppies
Side Salad & Drink

CHICKEN KING

DIP DEEZ Paletas

SOUTH BAY BAR & GRILL

LUNCH & LEARN AI WORKSHOP
Daedalian Room

Sessions:

Microsoft	1130-1150
edgerunner AI	1150-1210
GENAI.MIL & SpaceGPT	1210-1230

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Global Mission Data Dominance (BNN)
Treating Data as a Weapon System

Lt Col Devon Messecar
BMC3I, SSC SYD 85

Cyber Readiness at the Speed of Space

Process vs Product Innovation

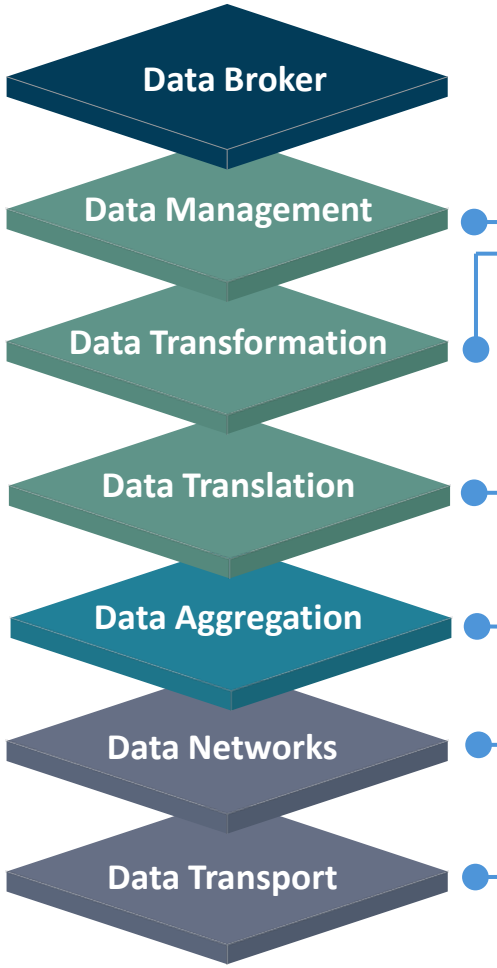
The hub and spoke model allowed American Airlines to compete with other airlines such as Pan Am, by offering a more efficient and connected travel experience.

Three Objectives	Three Parts of the Architecture
Connect the systems	Provide Enterprise Networking and Data Transport Services
Federate the data	Enable Data Access and Discoverability Services
Enable use of the data	Generate Multi-Cloud and Data Access for AI Development Services

GMDD Federated Stack

GMDD provides the data foundation enabling the Space Force and Joint Force to access, integrate, and share mission-relevant data at speed. It addresses long-standing data stovepipes to improve decision quality, collaboration, and operational effectiveness across domains.

GMDD Federated Stack



DATA FEDERATION

Integrated, Immersive, Intelligent Environment (I3E): Evolving into AI Hub: Migrate GenAI efforts into a consolidated, sustainable, enduring model focused on mission-specific AI development, lowering barrier to entry across the service.

Integrated Operations Networking (ION): Collection of projects to rapidly integrate existing capabilities into the data and networking architectures, therefore accelerating closure of the space warfighting kill chain.

Unified Data Library (UDL)/Allied Exchange Environment (AxE): Cloud-based, multi-classification data backbone providing federated access and distribution of space mission data across the Joint Force and Intelligence Community to meet space warfighting needs.

DATA NETWORK AND TRANSPORT

Red LAN: 24/7 custom ingest, processing, correlation, translation, filtering, and dissemination system that delivers space observations at a tactically relevant speed across classification domains.

Satellite Communication Upgrade (SCU): Connects SDA sensors to MDA networks through systematic upgrading of sensor interfaces to expose data and enable machine to machine (M2M) tasking.

Space Domain Awareness Network (SDAnet): Manages edge translation services and distributes space object location data and sensor taskings, enabling orchestration of a global network of SDA sensors.

meshONE-Terrestial (m1T): m1T is the global, resilient data transport provider for USSF missions and a key component of the DAF Battle Network black core, enabled by a networked mesh of nodes.

Connect the Systems: Data Networks & Transport Services

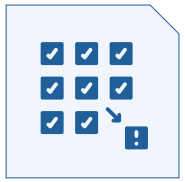
Objective

Transform the Space Force's data transport infrastructure from isolated point-to-point connections into a meshed ecosystem

Problem Set

The Space Force's ability to make rapid, data-driven decisions is limited by the absence of an integrated data-centric ecosystem

Disconnected systems



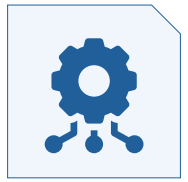
Stove-piped solutions

No Performance Monitoring

Solution

Establish a resilient, multi-classification enterprise-centric network architecture to accelerate connectivity between weapon systems for dynamic tasking and information distribution

Mesh Network



Mission Integration

Enterprise Services

Enterprise Network & Data Transport Architecture

SENSE

COLLECT & INGEST DATA FROM MULTI-SOURCES

Space-Based & Other Mission Sources

Authoritative mission data at the source

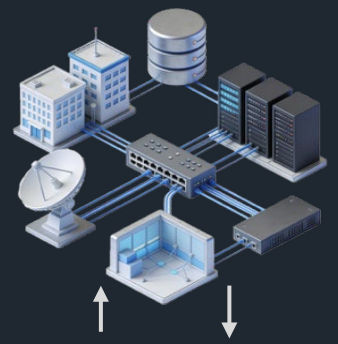
Transport

RAPID AND CONTINUOUS CONNECTIVITY

Networks

Cross Domain Services | Classified Core Networking | Enterprise Core Services

Edge Translation & Transport | Encryption Services | Data Transport Broker



Federated, governed data delivery

Data Access

Data Access, across the ecosystem: C2, Cloud, and Edge/Remote

DATA FEDERATION
Access and Availability

MAKE SENSE + ACT

DATA ENABLES DECISION RESPONSE

Operational Decision Makers

Speed
Near Real-Time Access

Trust
Governed & Traceable Data

Control
Data Ownership Preserved

Federate the Data: Data Access & Discoverability Services

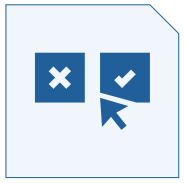
Objective

Transform the Space Force's data infrastructure from isolated, duplicative, and monolithic systems into a unified, distributed ecosystem

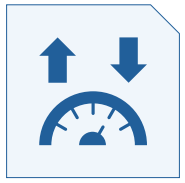
Problem Set

The Space Force's ability to make rapid, data-driven decisions is limited by the absence of an integrated data-centric ecosystem

Disconnected systems



Inconsistent access controls



Latency across networks

Solution

Federate data access, not duplicative long-term storage – data stays in place, but is discoverable and usable across domains

Federated Access

Policy-as-Code

Query Data at the Source

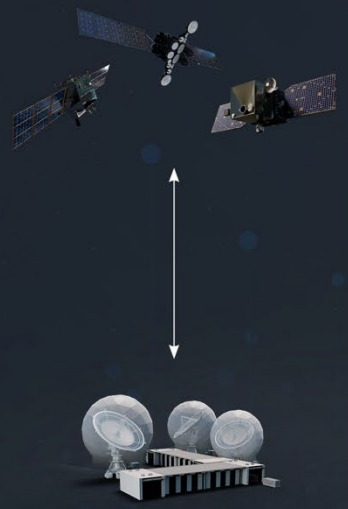
Federated Data-to-Decision Architecture

SENSE

COLLECT & INGEST DATA FROM MULTI-SOURCES

Space-Based & Other Mission Sources

Authoritative mission data at the source



DATA FEDERATION

MAKING DATA DISCOVERABLE, ACCESSIBLE, USABLE, AND INTEROPERABLE

Where Data Dominance Occurs

Knowledge Graph
AI Librarian
Orchestration

Secure Data Transport

Transports data across domains and ensures secure and reliable movement of data

Query to data — not bulk transfer

- Data Broker
- Data Management
- Data Transformation
- Data Translation
- Data Aggregation
- Data Transport
- Data Networks

Secure Data Transport

Transports data across domains and ensures secure and reliable movement of data

Federated, governed data delivery

* Data Transport operates continuously across the architecture, enabling secure, governed movement of data from source to decision

MAKE SENSE + ACT

DATA ENABLES DECISION RESPONSE

Operational Decision Makers

ASSESS

RAPID AND CONTINUOUS ASSESSMENT

Speed — Near Real-Time Access

Trust — Governed & Traceable Data

Control — Data Ownership Preserved

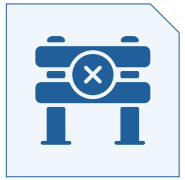
Enable Use of the Data: AI Development Services

Objective

USSF requires AI-enabled, autonomous systems to ensure space superiority. Implementing AI into operations and processes is a complex and resource-intensive endeavor; USSF orgs will need specialized expertise and resources

Problem Set

In FY26, USSF is investing in 25 programs with "AI" in their J-Books. The status quo means that each program will start from scratch on market research, cloud hosting, cyber security, and AI tooling before getting AI solutions into development and into operations



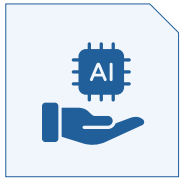
High Barrier to Entry

Inconsistent Tooling

Rework across Enterprise

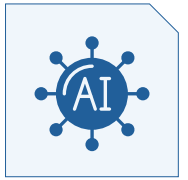
Solution

Establish a centralized USSF AI Hub to drive AI/ML implementation service-wide. This will decrease the burden on mission owners, eliminate duplicate efforts, consolidate investment, and accelerate AI adoption across all USSF mission areas



Shared AI Infrastructure

Vetted AI Tools



Reusable AI Services

AI-Enabling Infrastructure

AI Personnel

Expertise:
- A dedicated team to assist mission owners
- Ops and PAE outreach team identifies and fills gaps with AI operational units

Test & Evaluation, Cybersecurity: A repeatable framework for validating AI models, enduring relationship with SCA team builds shared understanding of AI

Partnerships: A central point for coordinating with FFRDCs, industry, and academia

AI Software

AI Solutions: AI Hub lowers the barrier to entry for mission owners to test and field solutions

AI Platform

Compute Power: Cloud-based GPUs at all classification levels

Test & Evaluation, Cybersecurity Infrastructure:
- Accreditation pipeline ensures policy compliance and security
- Test and Evaluation tools and benchmark datasets ensure effectiveness

Rapid Onboarding Infrastructure:
- Central library of approved and accredited AI models for “off-the-shelf” use
- Pre-existing data connections to USSF data sources
- Accessible API endpoints for AI models
- Data ingestion, preparation, and labeling pipeline

AI hub reduces barrier to entry for AI development, enabling rapid, responsible deployment of AI capabilities

How can we innovate our process around data?

Our processes must be data-centric, warfighter-focused and treat data as a weapon system!

Data as the Weapon System:

- **Mission and Security Operations Centers –** Tools for monitoring the performance, security, and trends of the data networking and transport solutions

- **Data Factory –** Focusing on how data is prepared, federated, and used in AI to reduce barriers to entry and enable rapid delivery of capabilities by abstracting away core/repeatable services across a large customer base

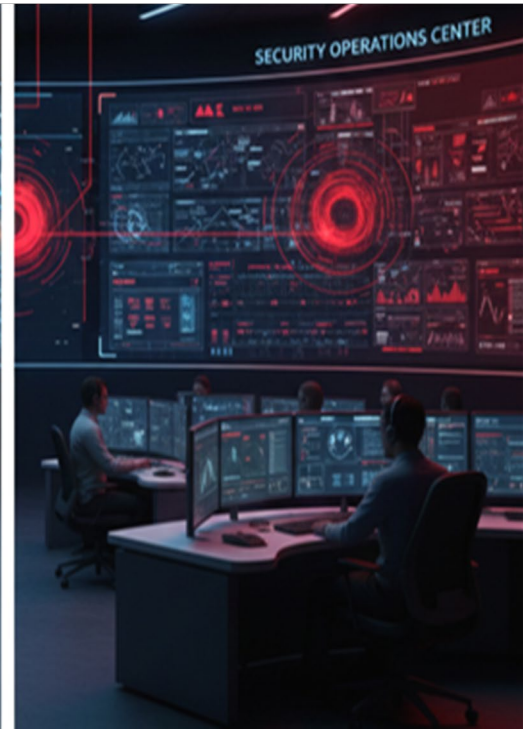
Operationalizing Data as a Weapon System

Maintaining the health of weapon systems and
Ensuring Mission Accomplishment

Mission Assurance [NOC | SOC]

- **Quality of Service Metrics:**
  - Performance Monitoring
  - Bandwidth
  - Latency
  - Data Loss/Data Quality
  - Audits (maintenance trends)

- **Protecting and Defending:**
  - Predictive Analytics
  - Maintenance Trends
  - Intelligence Indicators
  - Cyber Security



Operationalizing Data as a Weapon System

- **Data Factory: One service, many consumers**

- **Data-Centric Services:**
  - Data transport, encryption, translation, federation, processing, storage, quality, help desk, performance monitoring, etc.

- **Customer-centric Services:**
  - Emphasizing teams for on-boarding data from new and heritage sensors, generating APIs, tracking accesses, implementing policy-as-code, tagging data, validating metadata requirements, building schemas, verifying customer needs for volume and veracity.

Questions?

2026 SSC CYBER EXPO

PANEL | Human-AI Teaming

Moderator: **Dr. Cindy Dominguez**, MITRE

Panelists:

- **Human AI Teaming Tools, Applications, and Processing Lab (SSCs HAT LAB)**: Mr. Bart Stewart, Space Systems Command CDAO
- **Human-Machine Teaming Across the Department of War**: Dr. Glenn J. Lematta, MITRE
- **Human Readiness Levels for Human-Machine Teaming**: Dr. Judi E. See, Sandia National Labs
- **Measuring the Impact of AI: Joint Activity Testing**: Dr. Taylor B. Murphy
- **Integrating BCIs into AI Systems for Real-Time Team Optimization**: Dr. Richard E. Niemeyer, USAFA

2026 SSC CYBER EXPO

Human AI Teaming Tools, Applications, and Processing Lab (SSCs HAT Lab)

Mr. Bartley Stewart

SSC Chief Data & AI Officer

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Human-Machine Teaming Across the Department of War

Dr. Glenn J. Lematta

MITRE

Agenda

- **Definition and overview of Human-Machine Teaming**
- **HMT Across the DoW**
  - Multi-Domain Command and Control
  - Ground-Based Electro-Optical Deep Space Surveillance (GEODSS) Telescope
  - Test Resource Management Center (TRMC) HMT Assessment Guide

What is Human-Machine Teaming?

Adaptive, bi-directional team interaction among humans and machines that augments human capabilities for improved mission outcomes

- Improve joint human-machine performance
- In real mission contexts
- Using evidence-based methods

Why is Human-Machine Teaming Critical?

It's about the operational context…

Stay aware and aligned in mission transitions: decisions, exchanges in control, shifts to contingencies, special cases, and emergencies.

Support distributed operations: mission-critical events and states need to be propagated to the right stakeholders at the right time.

Manage cognitive demands: technologies intended to simplify workloads introduce new cognitive demands like understanding, predicting, and directing system behavior.

Maintain security, lethality, and efficiency over time: systems and missions evolve, changing how Guardians must operate for mission success.

Teaming enables adaptation to threats, complexity, and surprises inherent in real missions

Human-Machine Teaming Across the DoW

Joint All-Domain Command and Control

Ground-Based Electro-Optical Deep Space Surveillance Telescope

Test Resource Management Center HMT Assessment Guide

Joint All-Domain Command and Control

Support distributed operations: What are the essential design elements and capabilities underlying a common picture for JADC2 situational awareness?

User Engagements

Interviews and discussions with over 50 Subject Matter Experts to elicit COP HMT needs

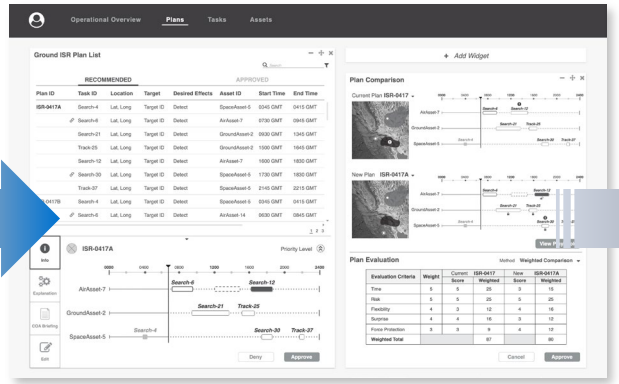
Translation to Design

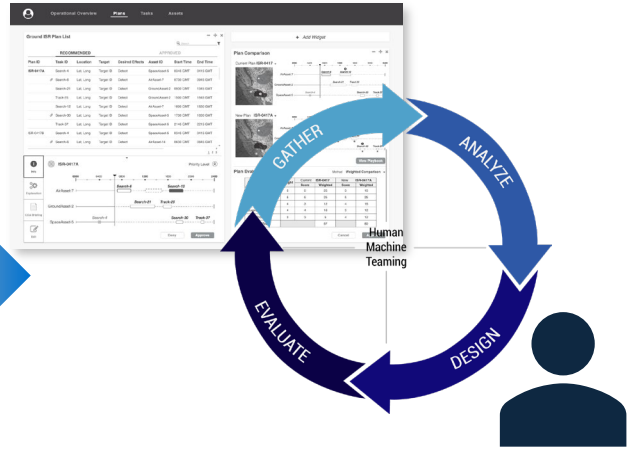
Translate needs into lightweight mock-up designs

User Feedback

Seek out feedback from users on design and its ability to meet their needs

Cross domain x Cross function





GEODSS: Vision for Human-Machine Teaming

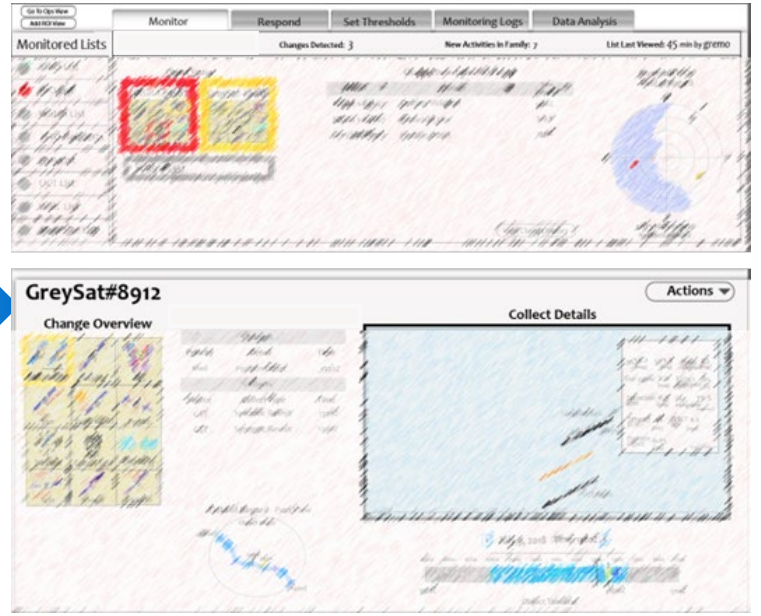
Stay aware and aligned in mission transitions: develop GEODSS capabilities to enable better operator cognizance and flexibility

Manage cognitive demands: Help operators offload routine and mundane tasks

HMT Design Themes

Design Content			Design Process
Transparency	**Augmenting Cognition**	**Coordination**	**Design Specifics**
Observability Transparency into what an automation partner is doing relative to task progress	***Directing Attention*** Orient attention to critical problem features and cues	***Directability*** Humans can direct and redirect an automation partner's resources, activities, and priorities	***Information Presentation*** Format information to support understandability & simplicity
Predictability Future intentions and activities are observable & understandable	***Exploring the Solution Space*** Leverage multiple views, knowledge, and solutions to jointly understand the solution space	***Calibrated Trust*** Understand when and how much to trust automation partner	***Design Process*** Guidance on the systems engineering processes for HMT
	Adaptability Recognize and adapt fluidly to unexpected situations	***Common Ground*** Pertinent beliefs, assumptions, intentions are shared	

Sample Tactical Monitoring Display for Satellites

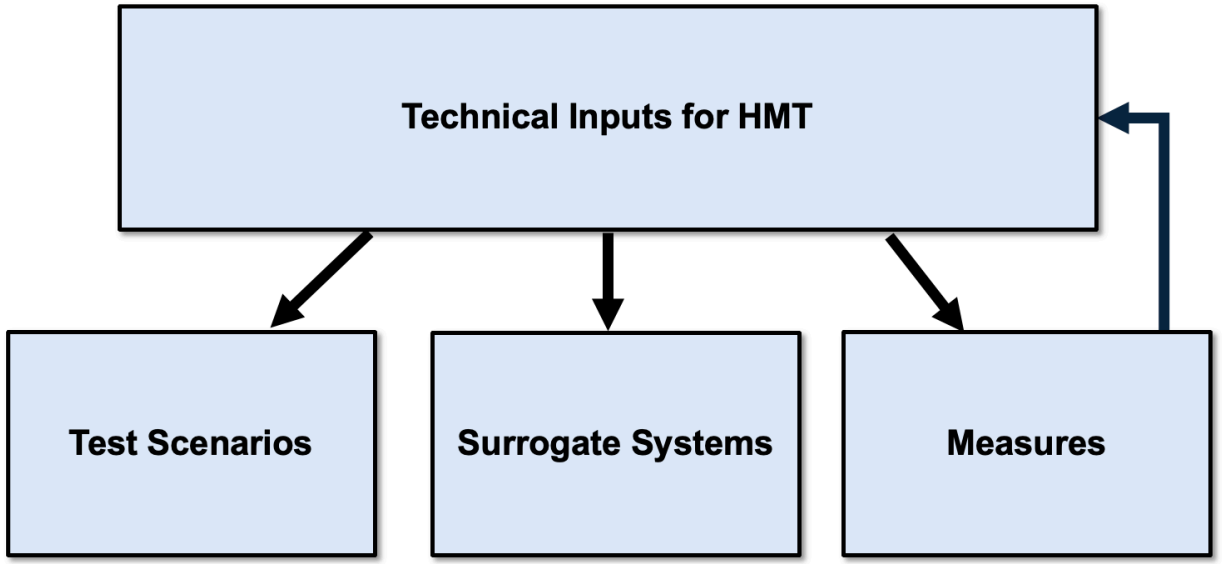


Test Resource Management Center HMT Assessment Guide

To provide consistent and evidence-based information about how to assess human-machine teaming in a "101-style" guide tailored to DoW use cases

- Integrate HMT assessment into acquisition strategy
- Discover, prioritize, and assure HMT performance requirements
- Test with scientific rigor across levels of system maturity

Test design elements for HMT assessment



For HMT Assessment Guide (Distro A) access, contact glematta@mitre.org

Conclusion

- Human-machine teaming is an established discipline in the DoW
- However, HMT needs to be thoughtfully integrated into programs: it's cheaper and faster to start early.
- The S6 Human-AI Teaming Lab can leverage scientific principles and techniques of HMT to improve SSC governance and support Guardians' missions

2026 SSC CYBER EXPO

Human Readiness Levels for Human-Machine Teaming

Is the machine ready for human use?

Dr. Judi E. See

Sandia National Labs

Sandia National Laboratories

National Nuclear Security Administration

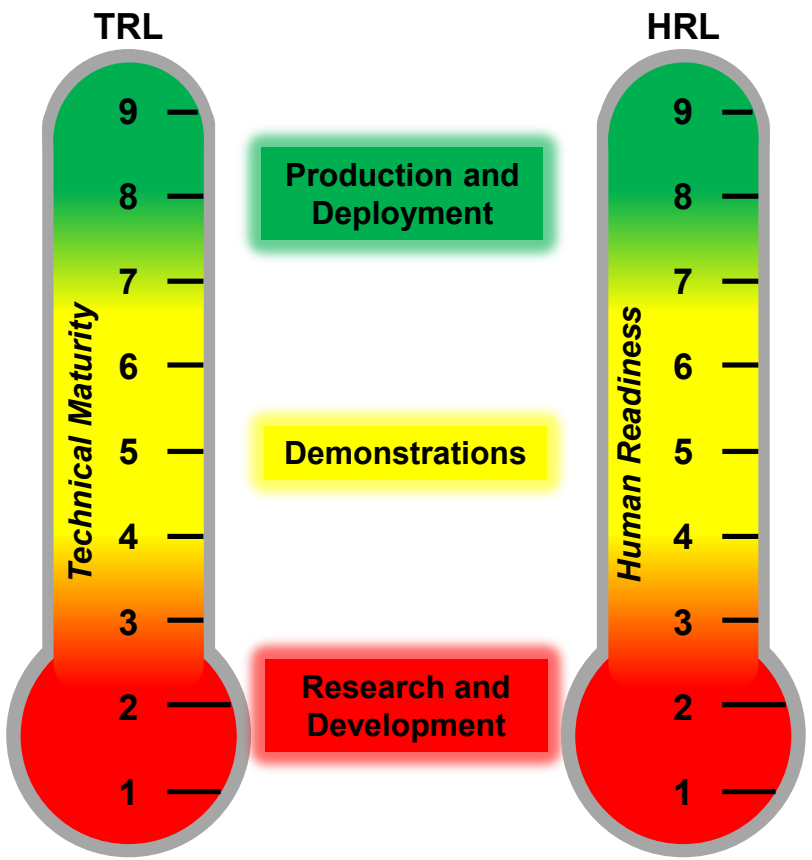
U.S. DEPARTMENT OF ENERGY

Cyber Readiness at the Speed of Space

Agenda

- What are HRLs?
- How were HRLs developed?
- What is ANSI/HFES 400?
- Why are HRLs significant?
- How do HRLs apply to SSC?
- What's next for HRLs?

What are HRLs?



- Evaluate, track, and communicate readiness for human use
- Complement and supplement TRLs
- Mitigate human issues early in lifecycle

Provide Assurance That:	
TRL Scale	Technology will function as intended
HRL Scale	Humans are able to use technology as intended

HRL scale provides a single number to communicate readiness for human use

How were HRLs developed?

Tier 1 standards are essential for DOD systems effectiveness, safety, and interoperability

What is ANSI/HFES 400?

Human readiness is readiness of technology for use by intended human users in specified intended operational environment

- **Defines nine HRL levels and provides guidance for their application**
- **Supports multiple iterative evaluations of human readiness**

Evaluation Activity	HRL Level
Usage scenarios	HRL 3 - 9
Human performance metrics	
Human-machine allocations	
Human factors engineering	
Safety and occupational health	
Manpower, personnel, training	
Environment	
Other relevant HSI domains	
Maintenance and sustainment	
Strategies for human use	
Conformance to guidelines and principles	HRL 4 - 9
User procedures and other manuals	
Issue tracking system	HRL 6 - 9

HSI = Human Systems Integration

Why are HRLs significant?

- **HRLs measure human-machine integration**
- **Neglecting HRLs increases risk of degraded system performance**

General James N. Mattis (Ret.), 19 Jan 2018

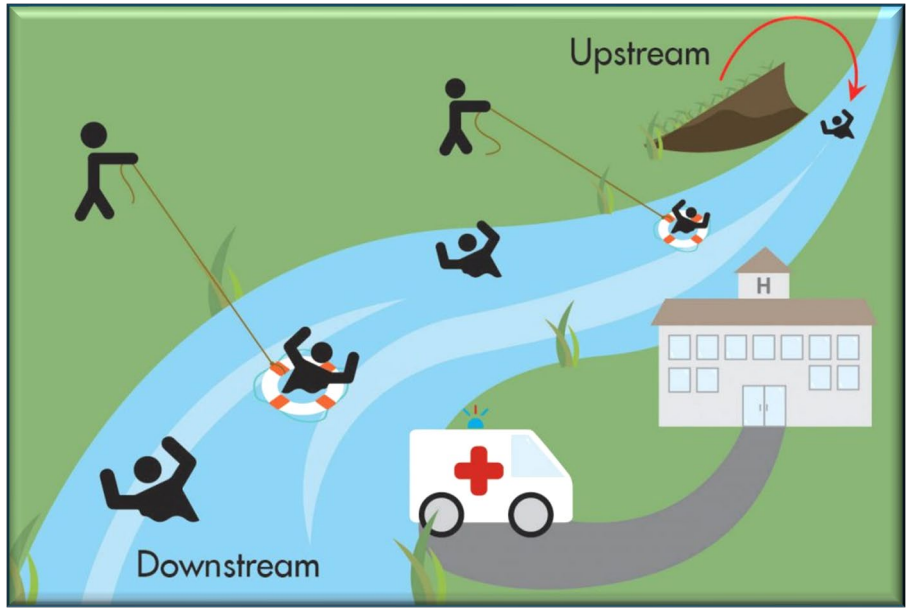
"Success does not go to the country that develops a new technology first, but rather, to the one that better integrates and more swiftly adapts its way of fighting."

Both technical maturity *and* human readiness are necessary to produce systems that are **useful**, **usable**, and actually **used**.

How do HRLs apply to SSC?

Decision support may be negatively impacted if low HRL tools arrive at HAT Lab

- **Effectiveness of AI for decision support hinges on human usability**
- **HRLs need to be evaluated upstream before arriving at HAT Lab for evaluation**



Incorporating users during ML learning and training enhances trust

Using HRL language to communicate with tool vendors will enhance speed and efficiency

What's next for HRLs?

- **Currently undergoing required five-year revision**
  - Writing targeted revisions to maintain currency
  - Incorporating specific guidance for AI
- **Revised standard redesignated ANSI/HFES 400-2026 upon approval**

"The future is not just something we predict; it's something we create."
Charlie Brown, SSC/S6 Deputy Director

Thank You!

For more information, please contact:

Judi E. See, PhD
Sandia National Laboratories
Systems Analyst
jesee@sandia.gov

Questions?

2026 SSC CYBER EXPO

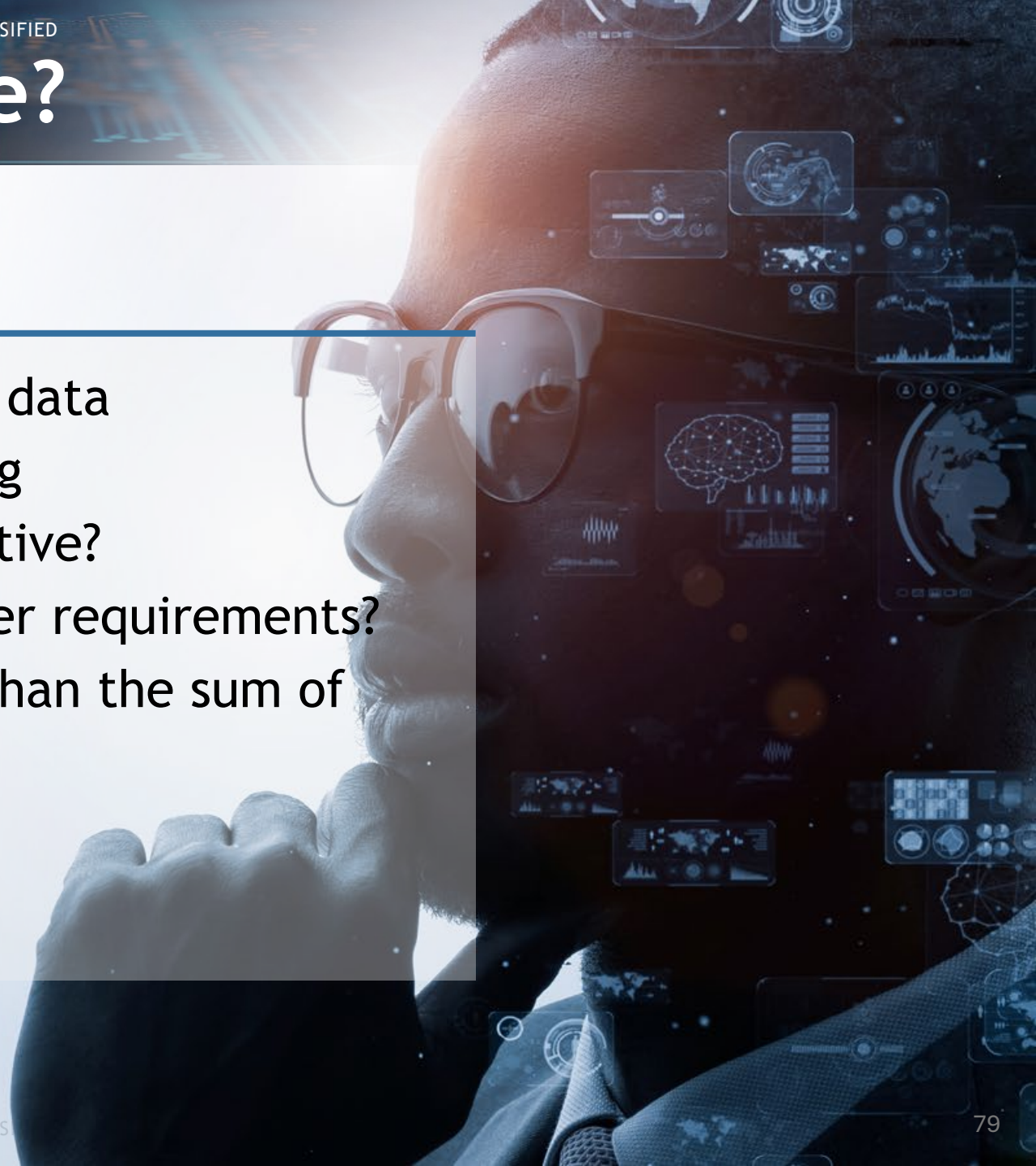
Measuring the Impact of AI: Joint Activity Testing

Dr. Taylor B. Murphy

National Geospatial Intelligence Agency (NGA)

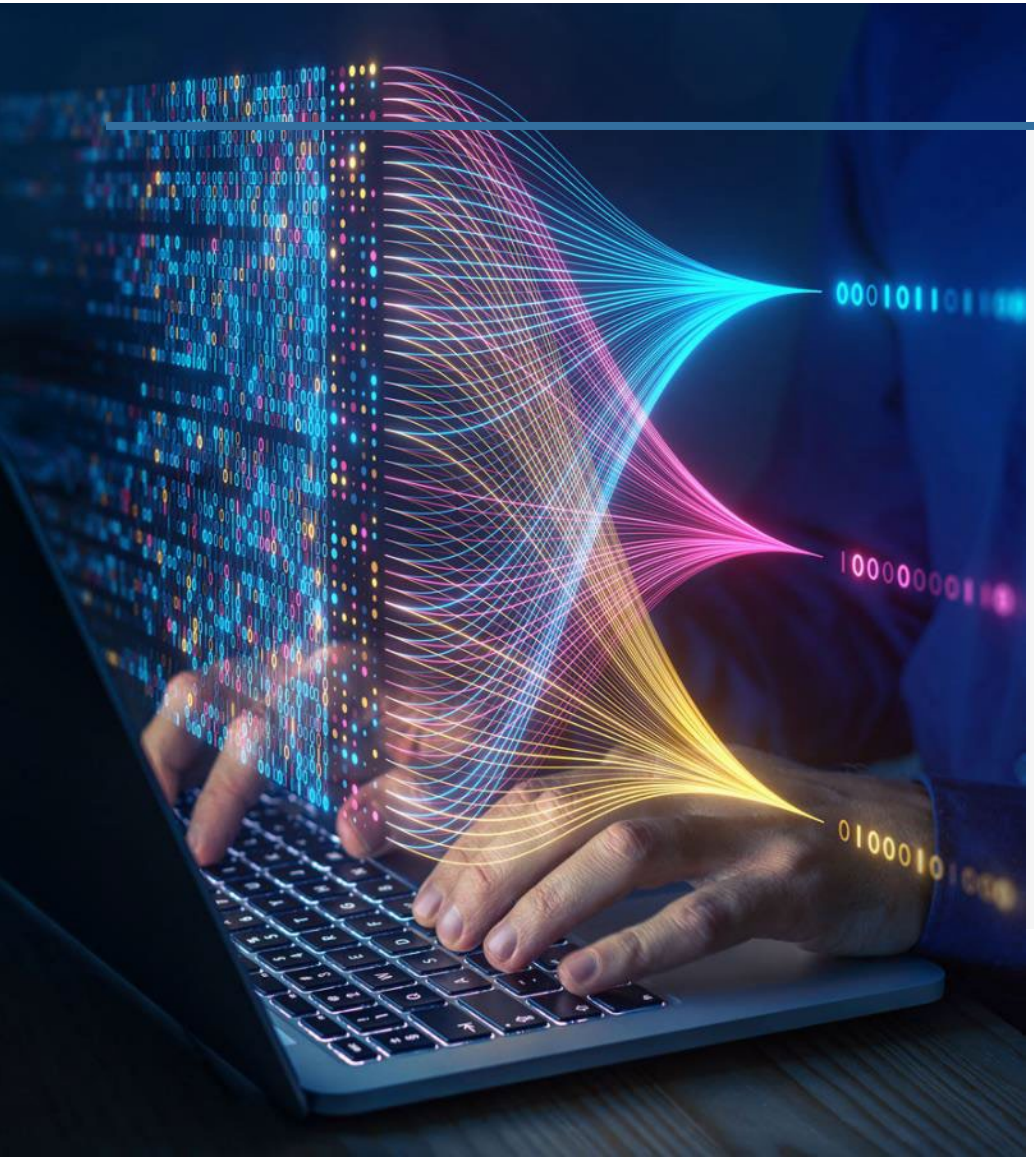
Cyber Readiness at the Speed of Space

Why Should We Care?



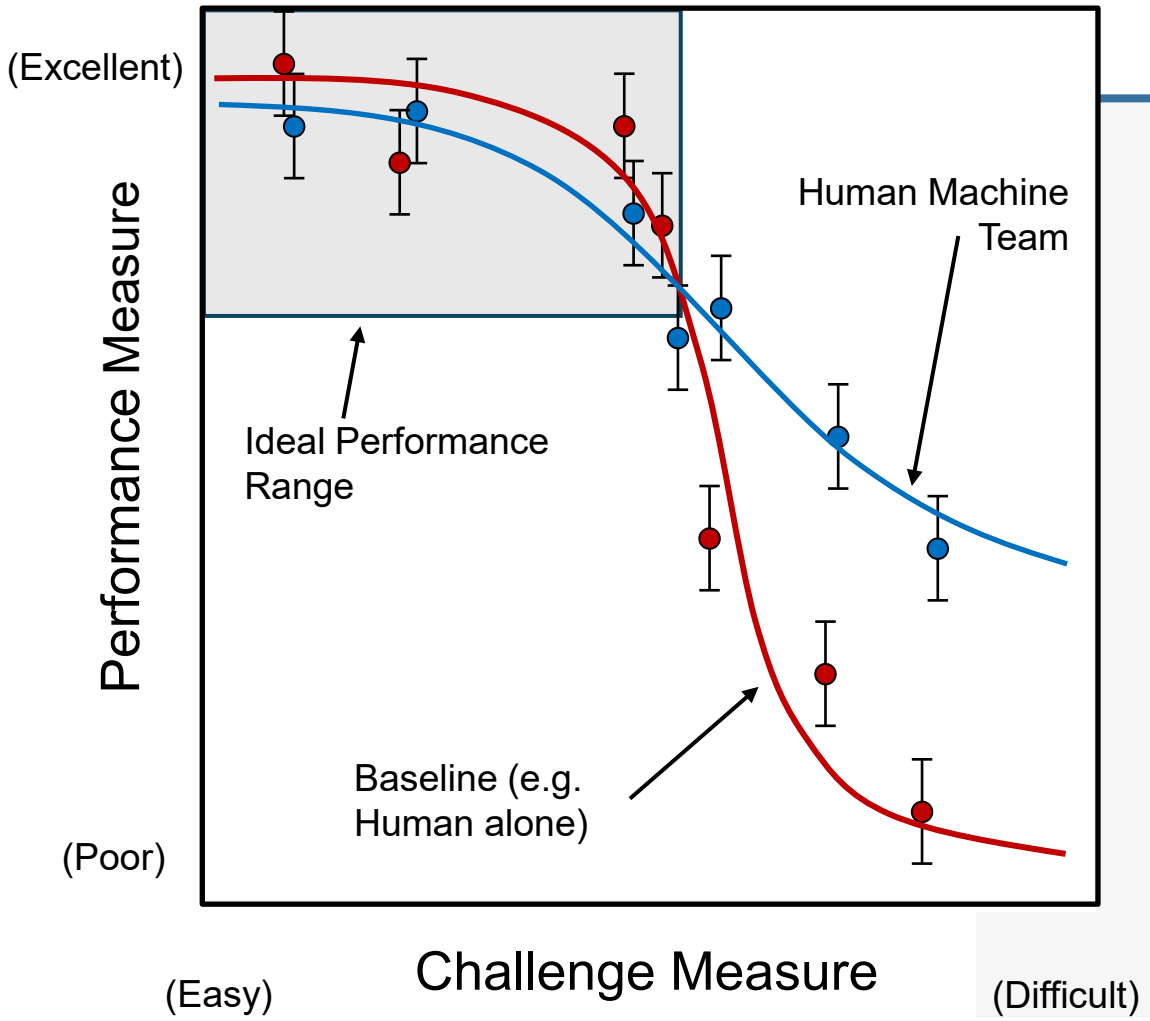
- We need AI—exponentially more data
- AI tools augment decision making
- How do we know tools are effective?
- How can government write better requirements?
- Real world performance—more than the sum of parts

Measuring Real-World Performance?



- Frame performance as result of a team:
  - Back end (algorithms)
  - Front end (data visualization)
  - Human warfighter
- Change a component, change performance
- Measure performance against baseline. Is team resilient?

What Is Joint Activity Testing (JAT)?



- **Challenge Measures**: What makes work difficult?
  - Time pressure, data overload, data ambiguity, unknown signatures, etc.
- **Performance Measures**: What do you need the team to do?
  - Number of relevant things found, time per product, etc.
- Performance = Area under curve
- Resilience = Slope

What Are Our Takeaways?

- We need AI
- AI needs to work for real people
- Don’t just measure algorithm performance
- MEASURE TEAM PERFORMANCE!

Questions?

2026 SSC CYBER EXPO

Integrating BCIs into AI Systems for Real-Time Team Optimization

Dr. Richard E. Niemeyer
USAFA

Cyber Readiness at the Speed of Space

DISCLAIMER

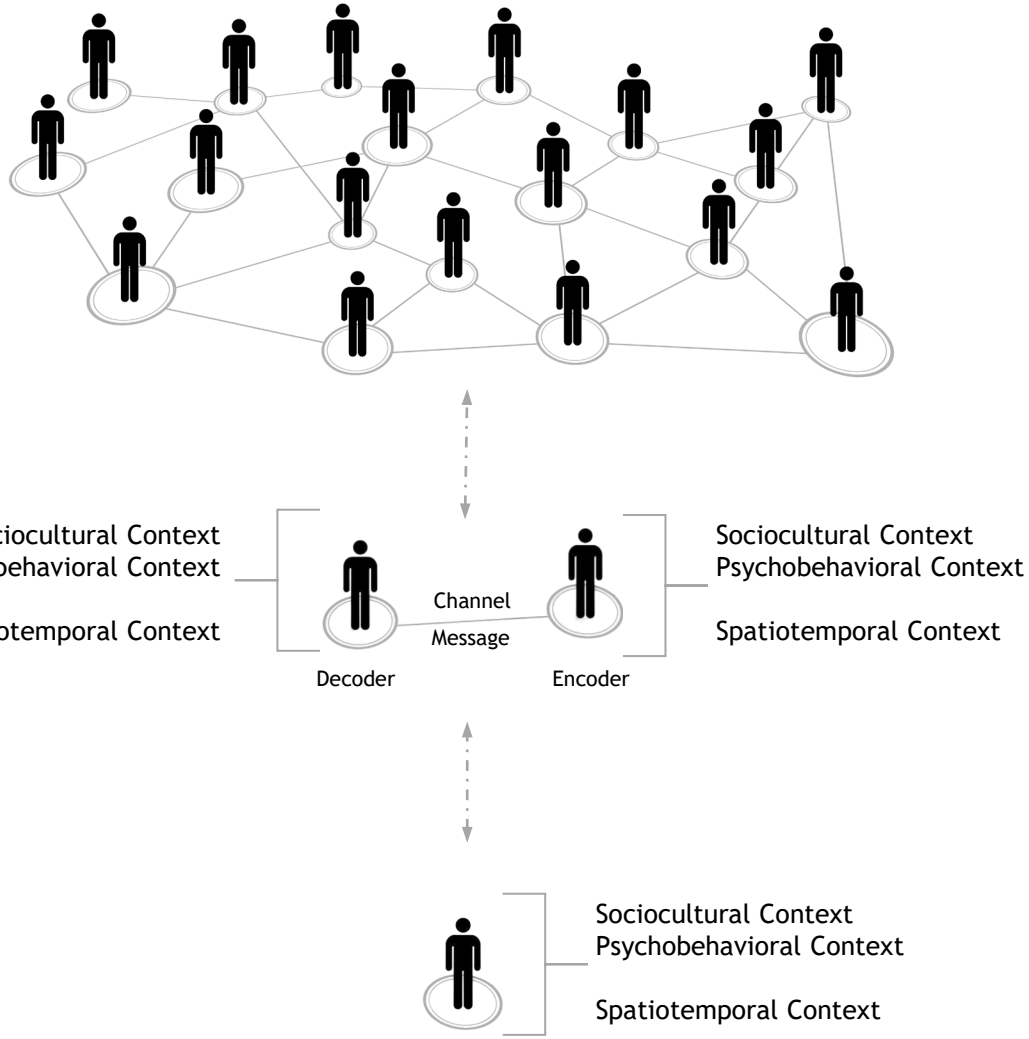
Opinions expressed in this talk are those of the speaker and do not necessarily reflect those of the US Air Force Academy, the US Air Force, the US Department of War, or the US Government.

BLUF

- Functionality of LLMs is advancing rapidly, but critical problems remain.
- The “wickedest” problems emerge during HMT/HAT/HRT.
- Solving these problems requires novel frameworks and methodologies that integrate *The Sciences*®
- USAFA DFBL WERC is working towards this solution.

WHAT DO WE MEAN WHEN WE CALL FOR NOVEL FRAMEWORKS?

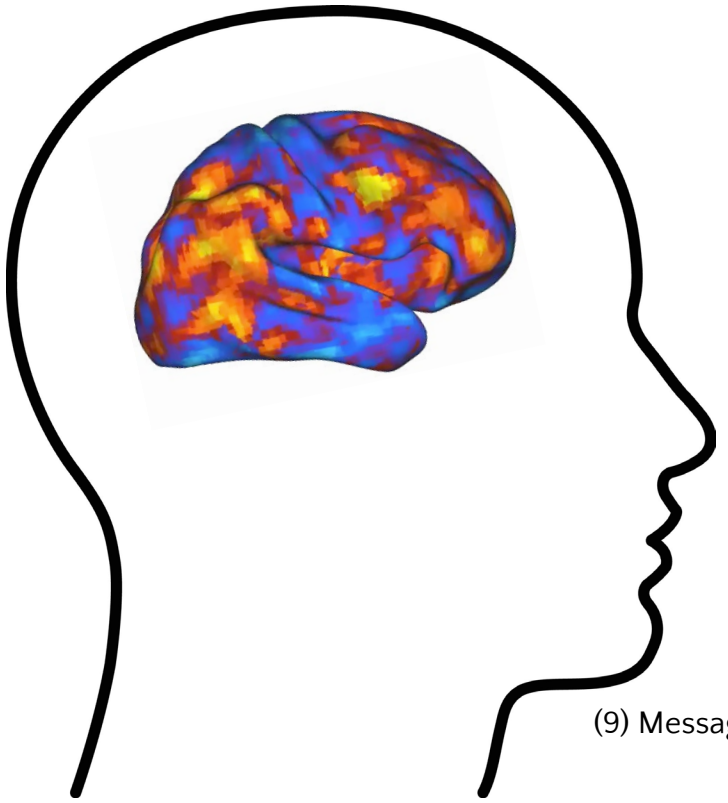
NOVEL FRAMEWORKS



NOVEL FRAMEWORKS

(10) Sociocultural Context of Message Receiver,
(11) Psycho-behavioral Context of Message Receiver,
(12) Neurocognitive Context of Message Receiver, and
(13) Eco-temporal Context of Message Receiver

(1) Sociocultural Context of Message Provider,
(2) Psycho-behavioral Context of Message Provider,
(3) Neurocognitive Context of Message Provider, and
(4) Eco-temporal Context of Message Provider



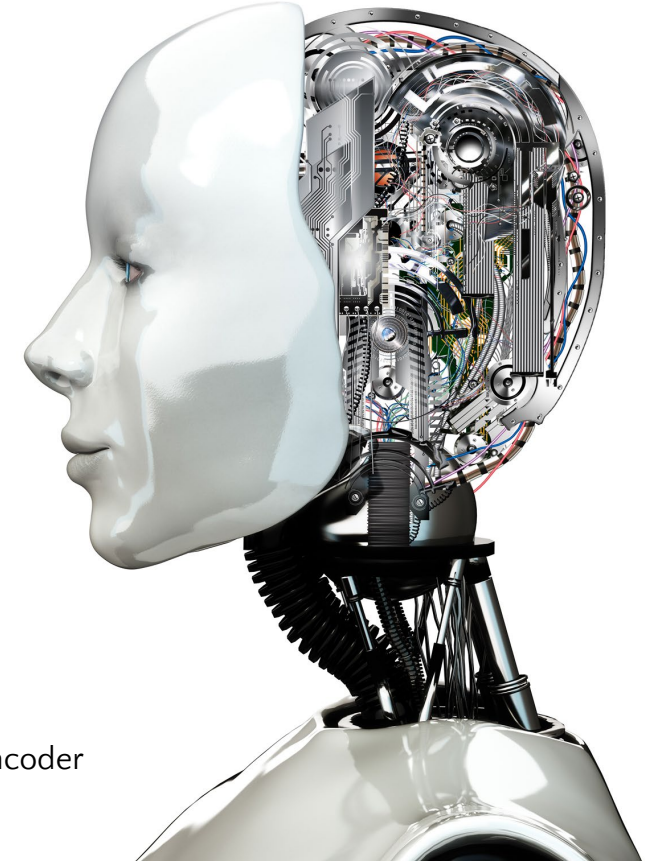
(8) Noise

(7) Message

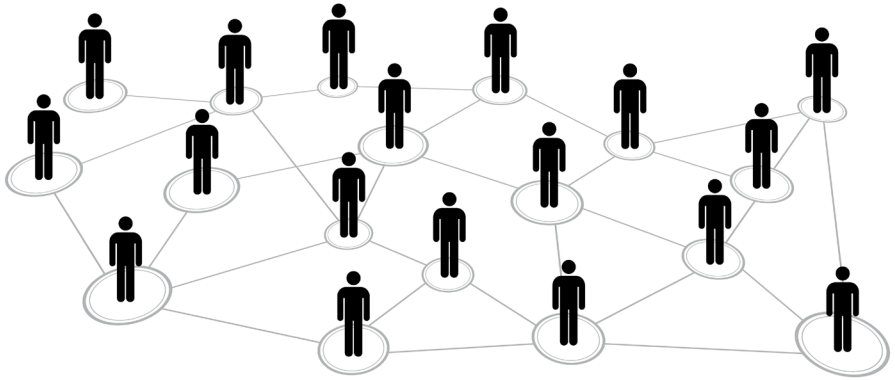
(9) Message Decoder

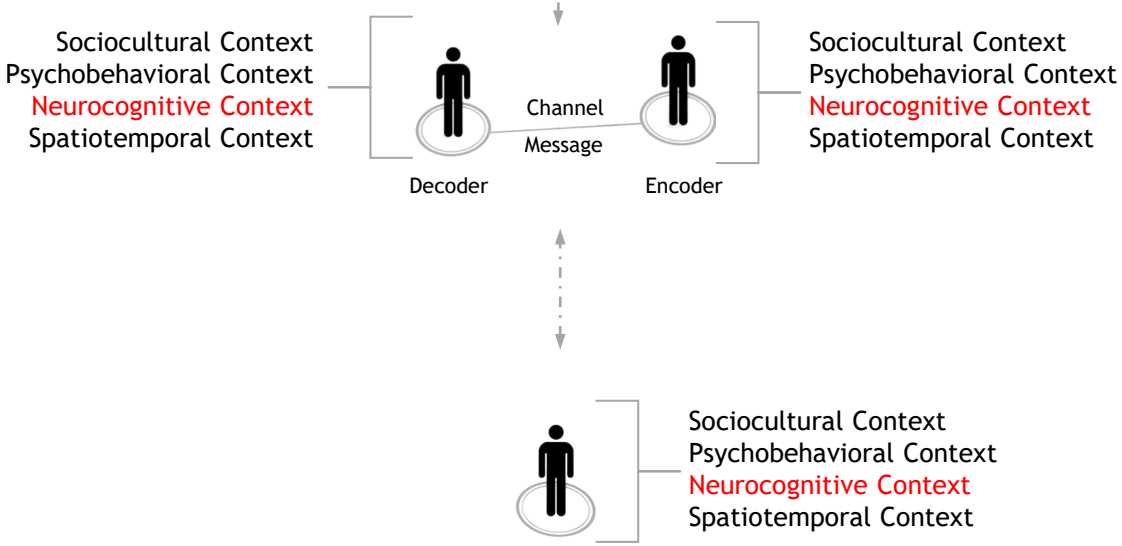
(6) Channel

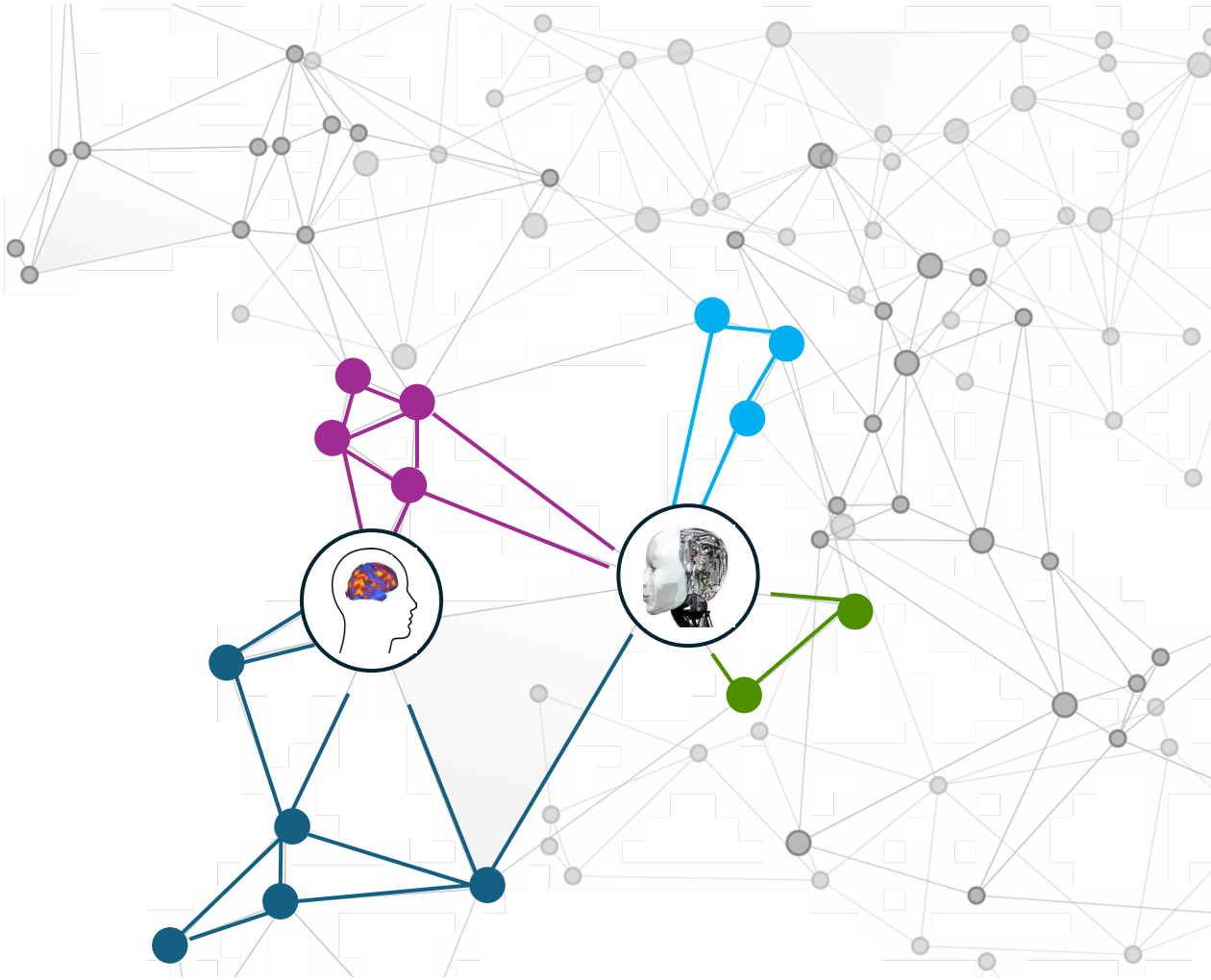
(5) Message Encoder



NOVEL FRAMEWORKS







WHAT DO WE MEAN WHEN WE CALL FOR NOVEL METHODOLOGIES?

NOVEL METHODOLOGIES

NOVEL METHODOLOGIES

Thank You!

For more information, please contact:

Richard E. Niemeyer, PhD
Associate Professor
United States Air Force Academy
Richard.Niemeyer@afacademy.af.edu

Cassie Eng, PhD
Assistant Professor
United States Air Force Academy

Sarah Bostrom, PhD
Research Scientist
United States Air Force Academy

Daniel Holman, PhD
Research Scientist
United States Air Force Academy

2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

BREAK

VISIT EXHIBITORS!

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

AI Tools in Action | *Day in the Life of a Guardian Powered By AI*

L1 - Enterprise Generative AI Tools Overview: Ms. Rachel Souder-Arguedas, SSC AtlasX

- Azure OpenAI
- **USSF AI Assistant**

L2 - Functional AI Tools

- **Edgerunner**
- **CyberSAGE & Streamlining the ATO Process**
- **Digital Guardian**
- **Space Force AI Accelerators**
  - **MIT Accelerator**
  - **Stanford Accelerator**

2026 SSC CYBER EXPO

AI Tools in Action

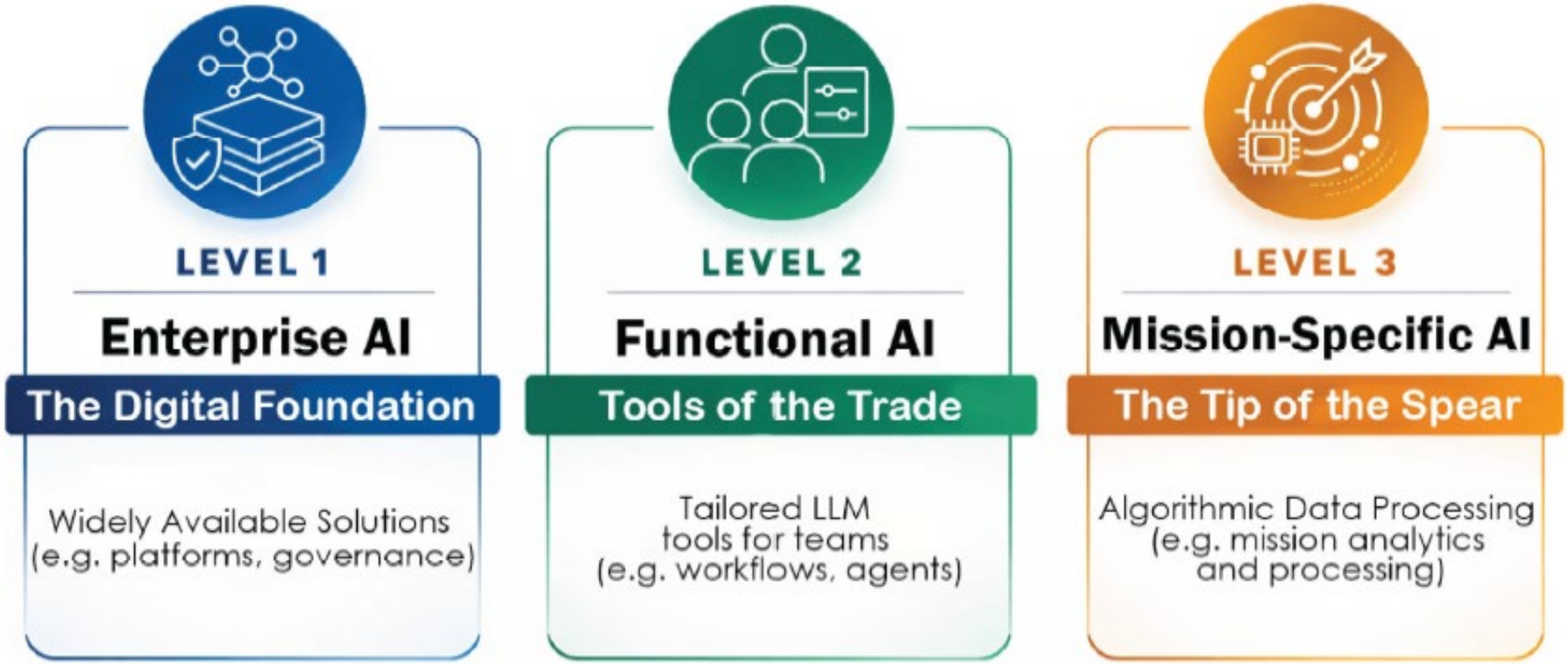
Ms. Rachel Souder-Arguedas

Director, SSC Business Innovation Office (AtlasX)

Cyber Readiness at the Speed of Space

SSC AI Action Plan Focus Areas

SSC AI Vision: Igniting space superiority through trusted AI & unified insight empowering our Guardians to outpace any threat and win



SSC AI Unity of Effort

SSC S6
Levels 1, 2, & 3

- SF/S6 and SSC Level Governance (DAB)
- Establish vision and reference architecture
- Use case oversight
- Piloting enterprise AI tools

AtlasX
Levels 1 & 2

- Deliver recurring training
- Tailor tools for business MVPs
- Promote available business resources
- Facilitate competitions and best practice events

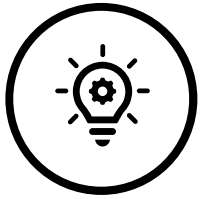
AI Hub
Levels 1 & 3

- Create and accredit a hosted scalable test and training environment
- Support infrastructure, integration, and enablement of mission/business solutions
- Facilitate mission-focused hackathon

SSIO (SQA)
Levels 1 & 3

- Chair Requirements & Resource Allocation working groups
- Digital Engineering Ecosystem (DEE/DECO)
- Operations-centric MVPs

AtlasX Intent: AI Upskilling



Awareness

- Discover how AI is transforming business and driving innovation
- Understand the benefits of using AI for greater efficiency

Adoption

- Gain a practical understanding of AI and core capabilities
- Apply core AI frameworks to enhance your workflow

Ability

- Champion a culture by applying best practices for AI implementation
- Develop the strategic thinking to apply AI to mission-critical challenges

Authorized SSC GenAI Offerings

GENAI.MIL

SPACEGPT

Copilot

AcqBot

USSF AI ASSISTANT

ENVISION Powered by WARP CORE

edgerunner AI

2026 SSC CYBER EXPO

Azure OpenAI

Ryan Zoeller, Microsoft

Microsoft's AI advantage

Comprehensive AI platform

Developer Tools	Copilot Studio	Visual Studio	GitHub Copilot		
AI Services	Azure AI Foundry	Azure OpenAI Service	Model as a Service (MaaS)	Azure AI Services	Azure Machine Learning
App Services	Azure Kubernetes Service	Azure Container Apps	Azure App Service	Azure API Management	Azure Functions
Data Services	Microsoft Fabric	Azure SQL Database	Azure Cosmos DB	Azure Database for PostgreSQL	
Privacy, safety and security	Azure AI Content Safety	Microsoft Purview	Microsoft Defender		
AI Infrastructure	GPU-, CPU-powered compute	InfiniBand Networking	Azure storage	Management services	

Agenda

- **Azure OpenAI Service**
- **Model Catalog**
- **Custom Use Cases**
  - Agents
  - SimpleChat (RAG Solution Accelerator)
  - Content Extraction and Indexing

Azure OpenAI Service

Enterprise AI at all classification levels

Azure OpenAI Service

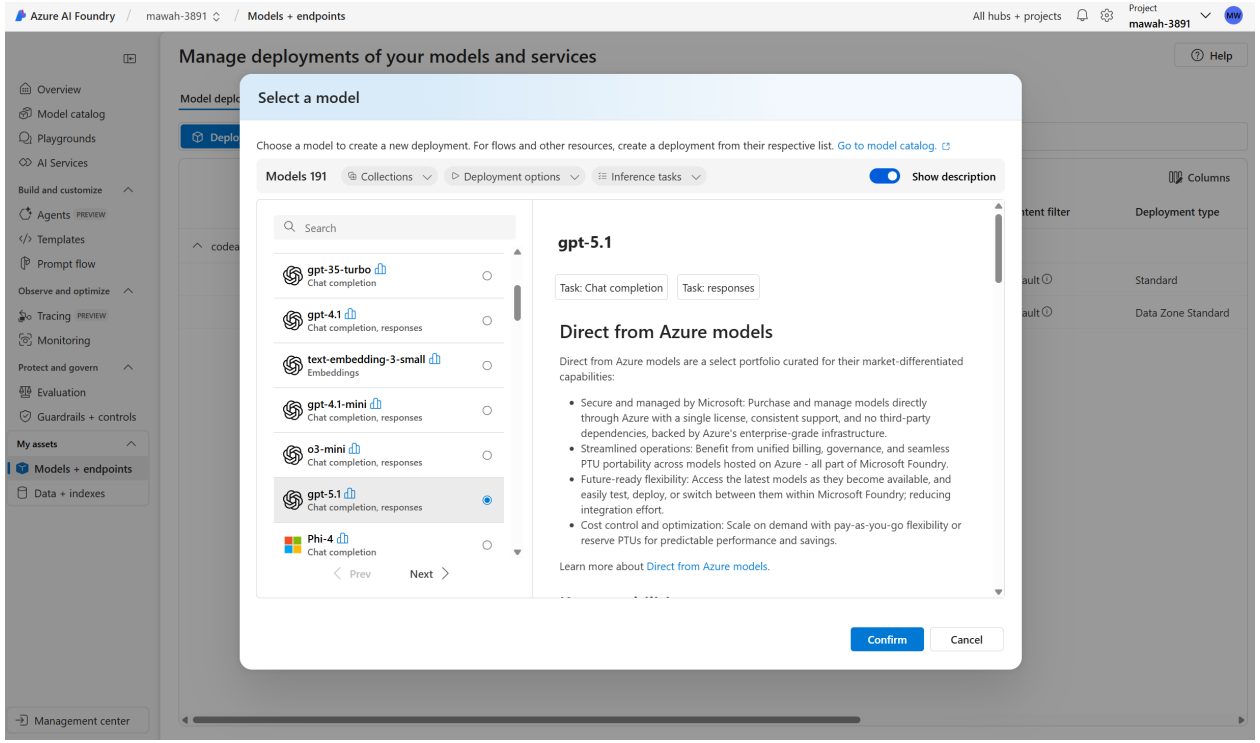
- Azure OpenAI in your subscription, with your data protected by your security
- Leverage modern OpenAI GenAI models in secure environments
  - Available today: GPT 5.1 in IL4/5, GPT 5.4 in IL6, GPT 5.2 in TS
    - New models/approved are added as approved
  - Features such as multimodal inputs and structured outputs are supported
- Pay-as-you-go and provisioned throughput options available
- Combine with Azure API Management to implement custom policies for quota management, spillover between endpoints, and error handling
- Share your insights with workspace & grant access via RBAC & ACL

Model Catalog

Your model, your data, your security

Model Catalog

- Your model, your data, your security controls
- Deploy AI models from a wide range of providers, including OpenAI, Llama, Mistral (over 190+ models in Government)
  - Serverless and self-hosted options
- Develop agents with tools for information retrieval, memory, and external actions
- Include guardrails to ensure secure and appropriate function
- Observe and evaluate agent conversations
- Bring your own Model

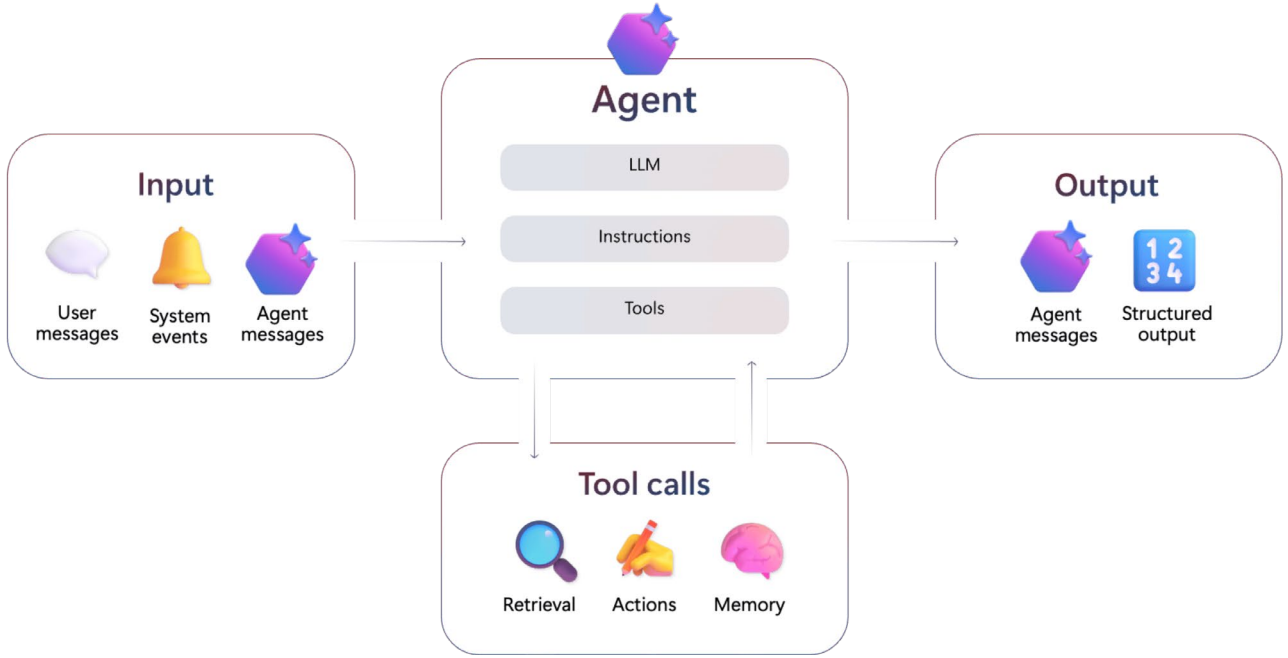


Custom Use Cases

Secure Mission-ready AI tools

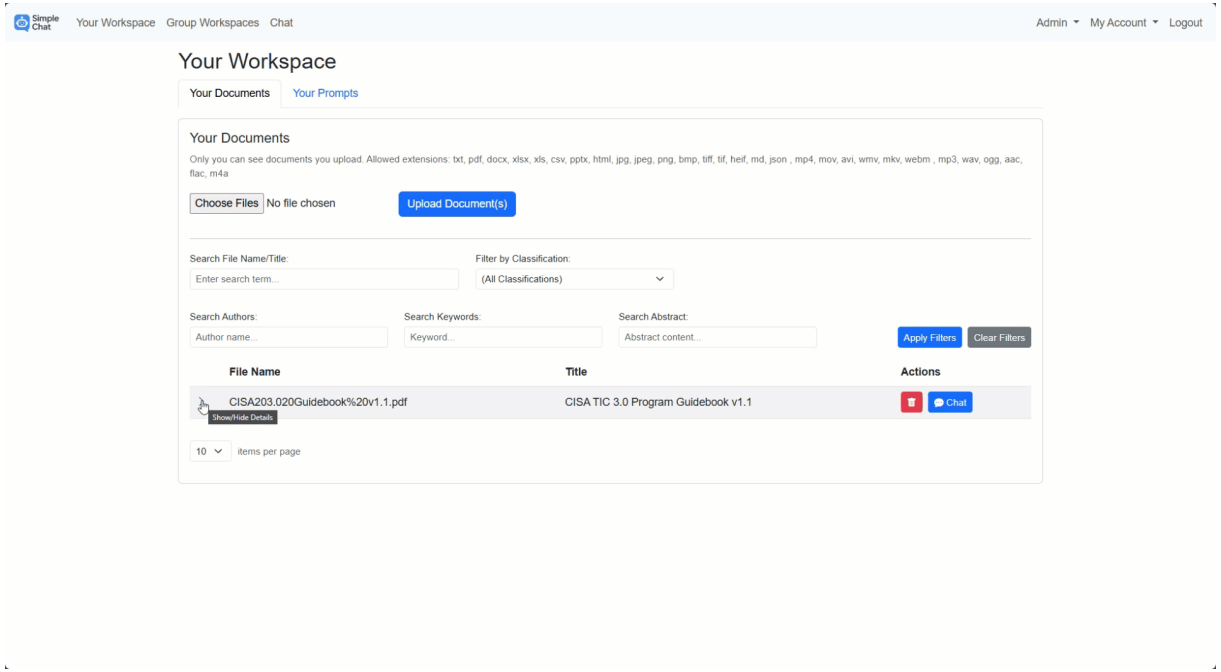
Agents

- Develop custom agents with Microsoft Agent Framework, Semantic Kernel, and other OS SDKs
- Supports community-standard MCP and A2A frameworks
- Inspect every model call, tool invocation, and decision with agent tracing
- Convert existing REST APIs into MCP tools with Azure API Management



SimpleChat

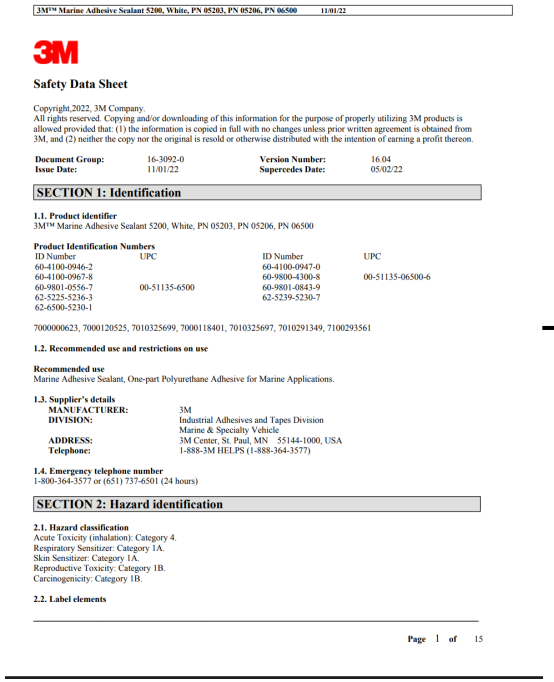
- Solution Accelerator (open source project with IaC) for chat-over-data
- Individual and group workspaces/data stores
- Automatically process data from complex file types
- Separate roles for administrators, users, and feedback evaluators
- Choose between JIT source upload and persistent document sets



See github.com/microsoft/simplechat

Content Extraction and Indexing

- Foundry Tools (Document Intelligence, Content Understanding) and GenAI models pull content from a wide range of file types
- Automatically leverage OpenAI models for vectorization on ingest/search with Azure AI Search or PostgreSQL databases
- Structured Outputs ensures valid responses in your custom formatting



3M™ Marine Adhesive Sealant 5200, White, PN 05203, PN 05206, PN 06500 11/01/22

3M

Safety Data Sheet

Document Group: 16-3092-0 **Version Number:** 16.04
Issue Date: 11/01/22 **Supercedes Date:** 05/02/22

SECTION 1: Identification

1.1. Product identifier
3M™ Marine Adhesive Sealant 5200, White, PN 05203, PN 05206, PN 06500

Product Identification Numbers

ID Number	UPC	ID Number	UPC
60-4100-0946-2		60-4100-0947-0	
60-4100-0967-8		60-9800-4300-8	00-51135-06500-6
60-9801-0556-7	00-51135-6500	60-9801-0843-9	
62-5225-5236-3		62-5239-5230-7	
62-6500-5230-1			

7000000623, 7000120525, 7010325699, 7000118401, 7010325697, 7010291349, 7100293561

1.2. Recommended use and restrictions on use

Recommended use
Marine Adhesive Sealant, One-part Polyurethane Adhesive for Marine Applications.

1.3. Supplier's details
MANUFACTURER: 3M
DIVISION: Industrial Adhesives and Tapes Division
Marine & Specialty Vehicle
ADDRESS: 3M Center, St. Paul, MN 55144-1000, USA
Telephone: 1-888-3M HELPS (1-888-364-3577)

1.4. Emergency telephone number
1-800-364-3577 or (651) 737-6501 (24 hours)

SECTION 2: Hazard identification

2.1. Hazard classification
Acute Toxicity (inhalation): Category 4.
Respiratory Sensitizer: Category 1A.
Skin Sensitizer: Category 1A.
Reproductive Toxicity: Category 1B.
Carcinogenicity: Category 1B.

2.2. Label elements


```
...
"uses_advised_against": [],
  "supplier_details": {
    "mfr_cage": null,
    "company_nm": "3M",
    "contact_addr_info": {
        "addr_ln_1": "3M Center",
        "addr_ln_2": null,
        "po_box": null,
        "city": "St. Paul",
        "state_province": "MN",
        "postal_code": "55144-1000",
        "country": "USA",
        "phone": "1-888-3M HELPS (1-888-364-3577)",
        "er_phone": "1-800-364-3577 or (651) 737-6501
(24 hours)",
        "fax": null,
        "website": null,
        "email": null
    }
  }
},
"hazard_identification": {
  "class_sub_mix": [
    {
      "haz_code": "H332",
      "haz_stmt": "Harmful if inhaled",
      "haz_class": "Acute Toxicity",
      "class_cat": "Category 4",
      "route_exposure": "inhalation",
      "spec_effects": "Harmful if inhaled",
      "route_entry": "Inhalation",
      "organs_affected": "Respiratory Tract"
    },
  ...
```

Microsoft Azure is the complete cloud for AI

Thank You!

For more information, please contact:

Michelle Harper
Strategic Account Director
micharper@microsoft.com

Ryan Zoeller
Dir. Strategic Acct. Tech. Spec.
ryanzoe@microsoft.com

Zach Yearsley
Dir. Specialist, Cloud & AI
zyearsley@microsoft.com

Mary Wahl
Prin. AI Solution Engineer
mawah@microsoft.com

Questions?

2026 SSC CYBER EXPO

USSF I3E AI Assistant

Michael Starr
Principal Architect
Microsoft

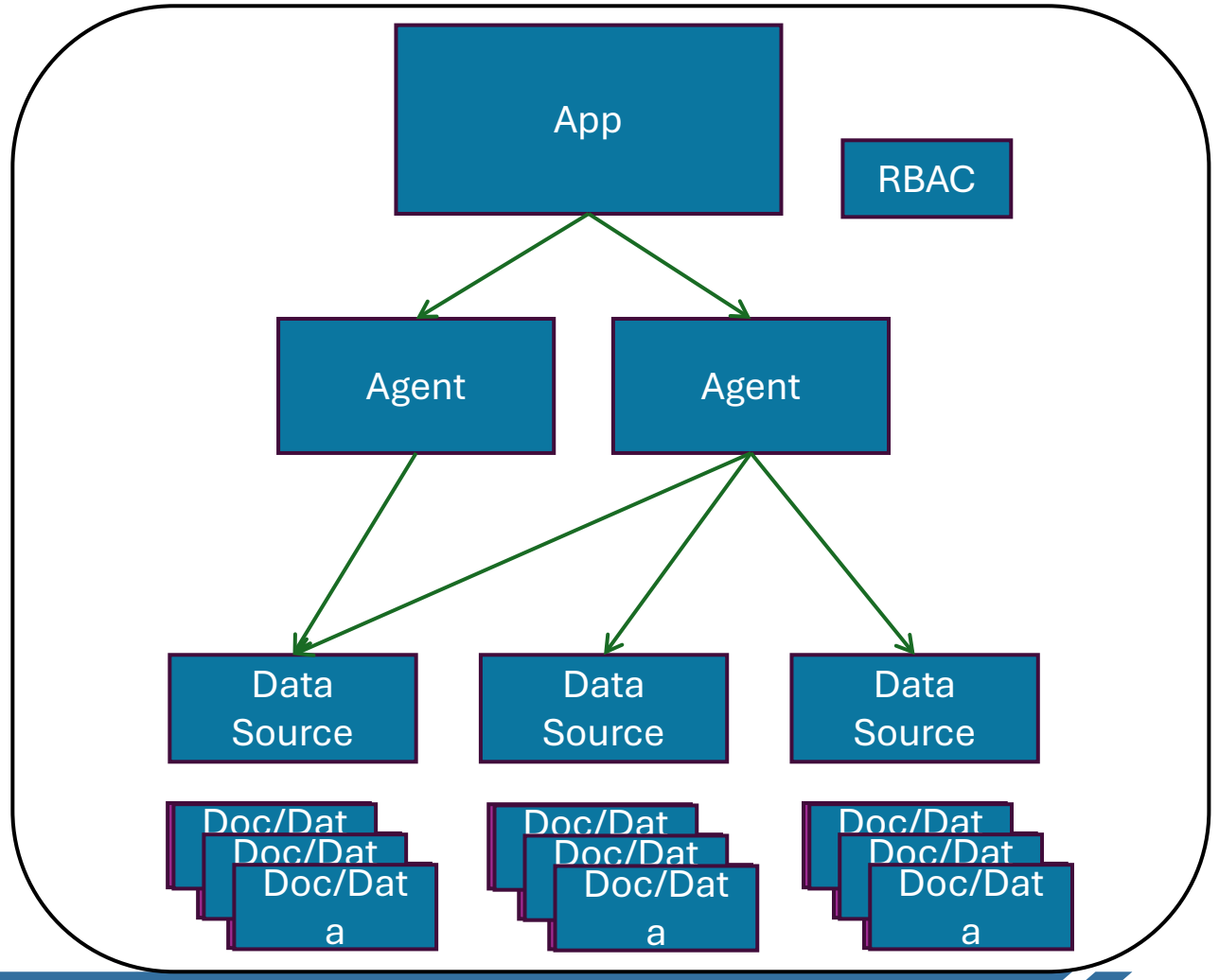
Cyber Readiness at the Speed of Space

USSF AI Assistant Overview

- USSF Owned and Operated made for Guardians as part of I3E.
- Operational ATO at Impact Level 5
- Adaptable via Workspaces, AI Assistant Apps, Agents Generation
- Retrieval Augmented Generation (RAG) makes it an expert in YOUR content.

USSF AI Assistant Features

Personal Workspaces	• Shareable
AI Assistant App model	• Security Boundary
Agent – Virtual SME	• Agent Prompts • Set Data Source(s)
RBAC	• Apps • Data Sources
Automated Data Ingestion	• Unstructured data • Structured data sources



USSF AI Assistant Use Cases

USE CASE	DESCRIPTION
General Officer Speech Writer	Assists in drafting speeches for general officers based on comms style, preferences, and topic.
Pilot Training Scheduler	Coordinates and schedules pilot training sessions given parameters on scheduling best practices
RFI/RFP/Contract Writer and Evaluation	Generates, reviews, evaluates RFIs, RFPs, vendor submissions, and contracts.
Regulations, Publications, Specialist	Provide guidance and information from comprehensive list of USSF/USAF publications, and regulations.
RMF Agent	Supports Risk Management Framework activities as a SME and assisting in evaluations

USSF AI Assistant is available for use in I3E through 2026
As GenAI.mil's offerings improve, USSF AI Hub encourages users to migrate to the enteprise solution

Thank You!

For more information, please contact:

Michael Starr
Principal Architect
micstarr@microsoft.com

Questions?

2026 SSC CYBER EXPO

Edgerunner

Mr. Colton Malkerson
Edgerunner

Cyber Readiness at the Speed of Space

edgerunner AI

Domain-specific AI on-device for the Warfighter

SSC Cyber Expo - April 23, 2026
Space Systems Command
Los Angeles Air Force Base

EdgeRunner AI introductions

Colton Malkerson

Co-Founder & COO

Company highlights

Name:	EdgeRunner AI, Inc.
Founded:	February 2024
Stage:	Series A (completed May 2025)
Investors:	Madrona Ventures, HP Tech Ventures, Four Rivers Ventures, and Alumni Ventures
Total Funding:	$17.5M
Employees:	22 full-time
CEO:	Tyler Saltsman (Co-Founder & CEO) and Colton Malkerson (Co-Founder & COO)
Headquarters:	Bellevue, WA
CAGE Code:	9Z176
UEI:	SLZTJUA8DBD3

Our goal is to become the standard for **military-specific AI on-device**

Defending western principles and protecting democracies.

Equipping the warfighter with domain-specific
AI agents and LLMs that run everywhere without internet.

EdgeRunner will increase our chance of winning the fight by arming the warfighter with domain-specific AI agents

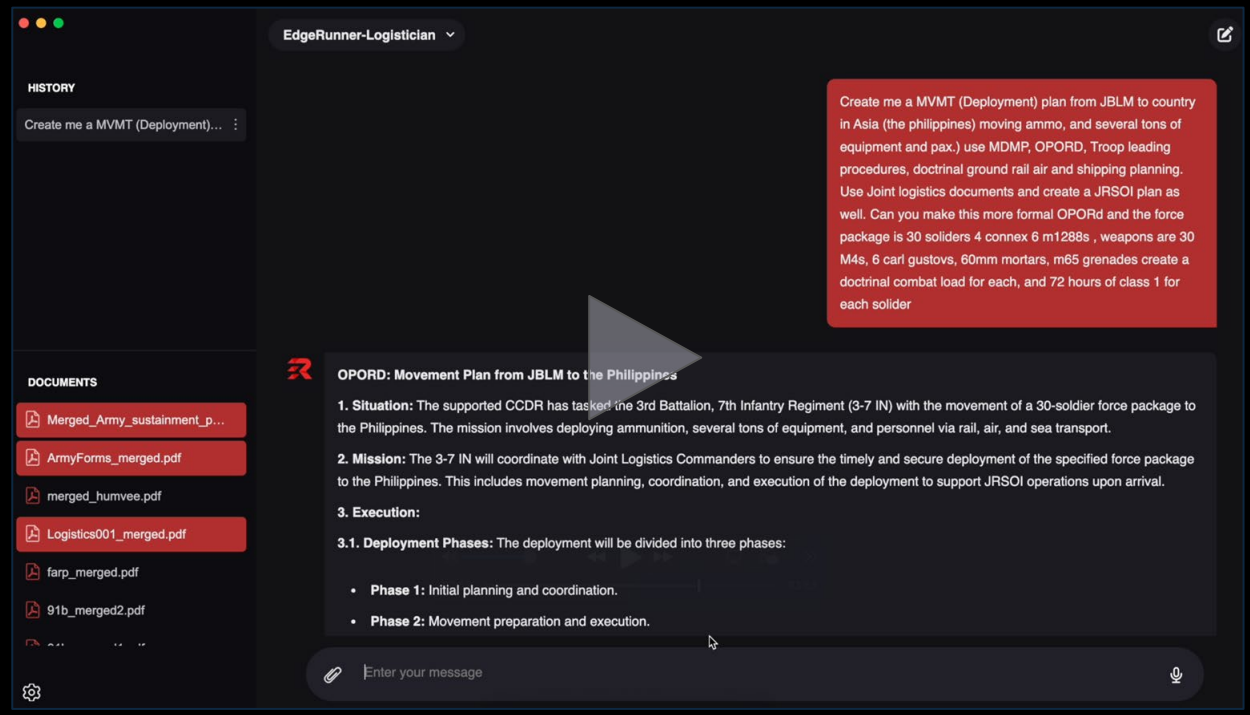
- Enable disconnected AI-powered operations
- Dramatically reduce specialized training requirements
- Accelerate decision making and command and control
- Bridge the gap between human and machine

Applied AI has the potential to transform warfighting, but AI at the edge is limited by several factors

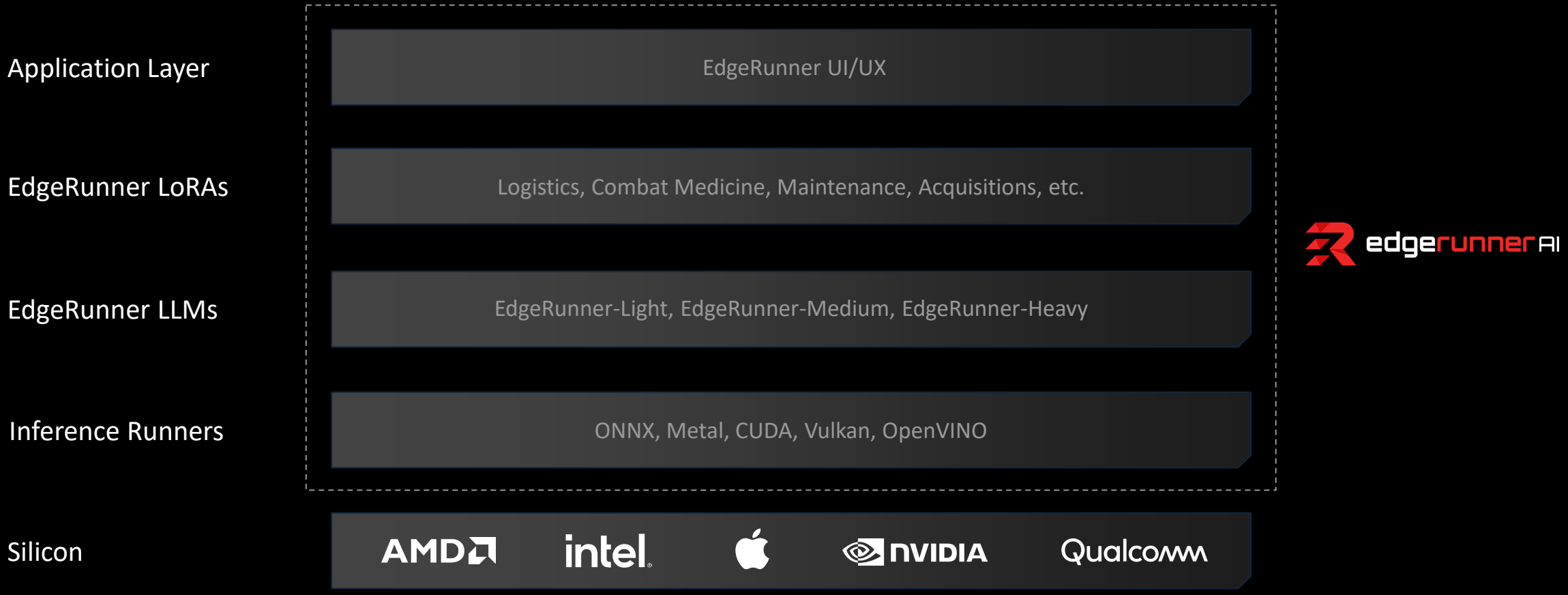
- Commercial LLMs lack domain-specific military knowledge
- Cloud hosting costs are unpredictable and expensive
- Commercial LLMs have restrictive guardrails and Terms of Service
- Sending data to the cloud risks data privacy and operational security
- Performance is unreliable in DDIL or contested environments
- Most solutions and partners can’t support sensitive use cases

The product: hardware agnostic platform bringing military-specific AI everywhere, even without the network or cloud

- **MOS-Specific**
  Trained on military data and doctrine
- **Rapid Deployment**
  Deploy in minutes
- **DDIL-Ready**
  Runs on-device without the internet
- **Hardware Agnostic**
  Runs on any mission system
- **Full Control**
  User owns the data and models



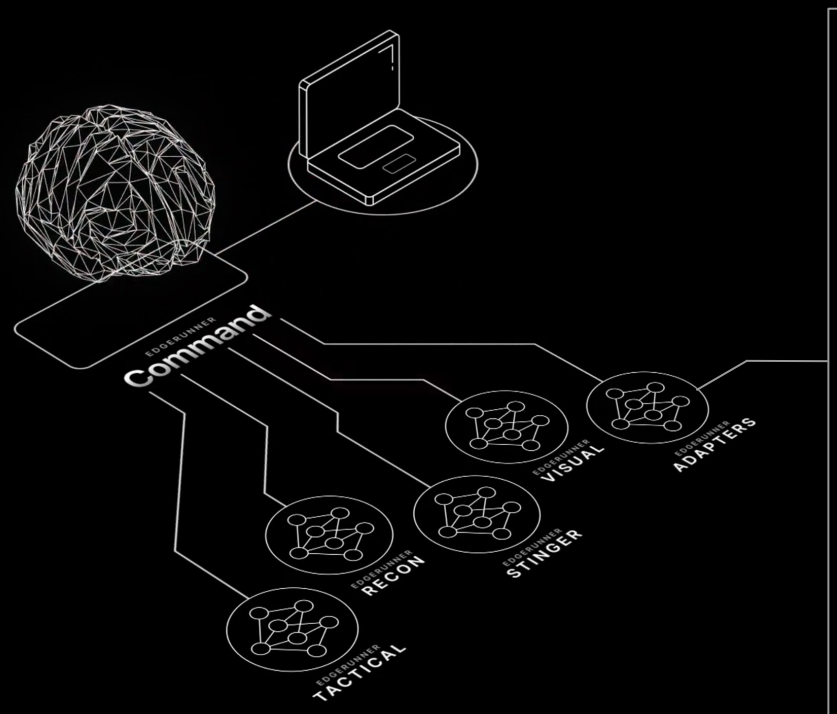
We capture value by building the full stack from inference runners to application layer

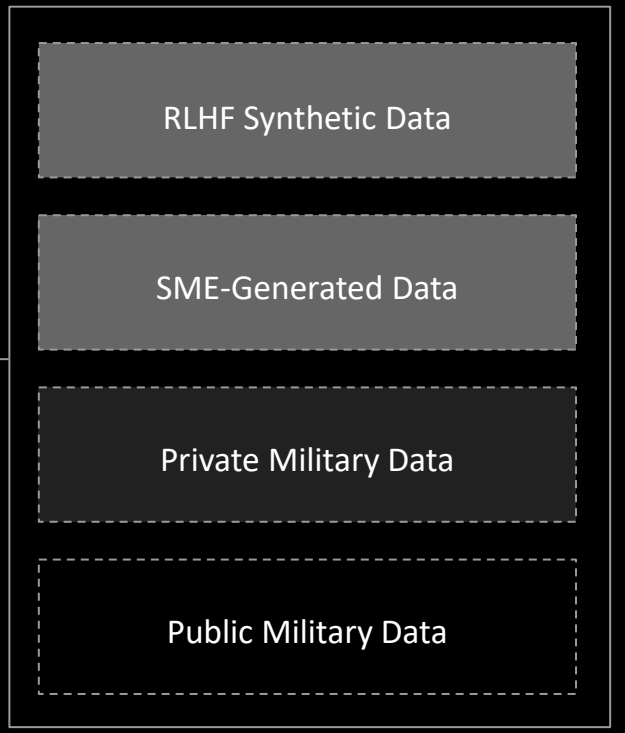


Military-specific LLMs with LoRA adapters provide more accurate and relevant responses

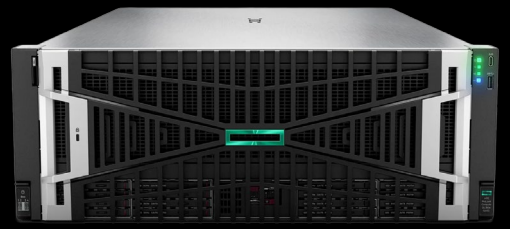
LoRA-based adaptation enables fast, low-cost tuning of AI models using real operational data and SME input

- Full Retraining Not Required
- Orders of Magnitude Cheaper
- Easily Deployable Updates
- MOS-Specific





Deploy across multiple platform types

ATAK/Smartphone	Laptop/Tablet	On-Prem/VPC
		
4GB+ VRAM Required	8GB+ VRAM Required	40GB+ VRAM Required
~0.5B+ Parameter LLM	~4B+ Parameter LLM	~24B+ Parameter LLM

EdgeRunner WarClaw: Autonomous digital operations at the front lines

A hardened agentic orchestration layer inspired by the popular OpenClaw agent framework, purpose-built for the U.S. military

- Agentic Autonomous Execution
- Runs Locally On-Device
- Integrates Into Common DoW Systems
- Reduces Cognitive Load

Defense One

SCIENCE & TECH

Startup debuts agentic AI assistant for war

As the Pentagon eyes agentic AI, a veteran-founded company introduces a tool that puts the military first.

BY PATRICK TUCKER

The Pentagon is eager to incorporate AI "agents"—software that can autonomously execute complex tasks like customer service, scheduling, or code writing—into more of what soldiers and defense civilians do. But a growing body of research shows that agents built from well-known large language models exhibit unpredictable and dangerous behaviors even in benign settings.

Article link

Modulate Open System Approach (MOSA)

- Hybrid Deployment / Cloud Agnostic > Operate on any cloud (e.g. AWS, Azure, GCP), on-prem (i.e. self-hosted server), or edge device (e.g. Intel, AMD, NVIDIA, Qualcomm, Apple).
- Edge Capability > Operate at the edge on ruggedized or low power devices. 16GB+ VRAM recommended as minimum compute today; smaller devices (e.g. ATAK) on roadmap for fall 2025.
- Multi-Vendor / Bring Your Own Model > Built with a modular architecture that supports flexible integration and deployment across DoD environments and various devices. The backend exposes a standard OpenAI-compatible API, enabling interoperability with other tools and systems. EdgeRunner provides our own domain-specific custom LLMs, but off the shelf open-source LLMs can be easily swapped in.
- Containerization / Open Source > Platform can be containerized, supporting VMs as needed. ODIn application is proprietary, but leverages open source LLMs and can be deployed on-device (vs. cloud hosted), reducing inference costs and increasing flexibility.
- Sustainment / Life Cycle / Improvement > Platform continually updated on a monthly or quarterly basis with newer LLMs and performance improvements. Updates occur remotely.

EdgeRunner & U.S. Space Force

USSF Guardian Role Specific Personas

- *AI Agents capable of running in the cloud or offline on device aligned to a given SFSC*

Acquisitions Support for SAF/SQ

- *EdgeRunner has built an Acquisitions specialist trained on the FAR and DFARS deployed in Azure ILZ. This agent is designed to help Guardians in Acquisitions roles shorten acquisition timelines with expert guidance*

ACES Integration

- *EdgeRunner has integrated with the Acquisition and Contracting Enterprise System (ACES) providing the backend AI support for acquisitions workflows*

ACQUISITION Reform Simulator

- *WarClaw - locally hosted multi agent configuration for Acquisition COA development*

Demo

2026 SSC CYBER EXPO

Cyber Security AI Guidance Enginer (CyberSAGE)

Think RMF/ATO

Ms. Penny McKenzie, PNNL Sr. Cyber Security Engineer

Cyber Readiness at the Speed of Space

Agenda

- **CyberSAGE Overview**
  - Design
  - User Interface
  - Authority to Operate (ATO) Assistant (Astraeus)
  - Q&A

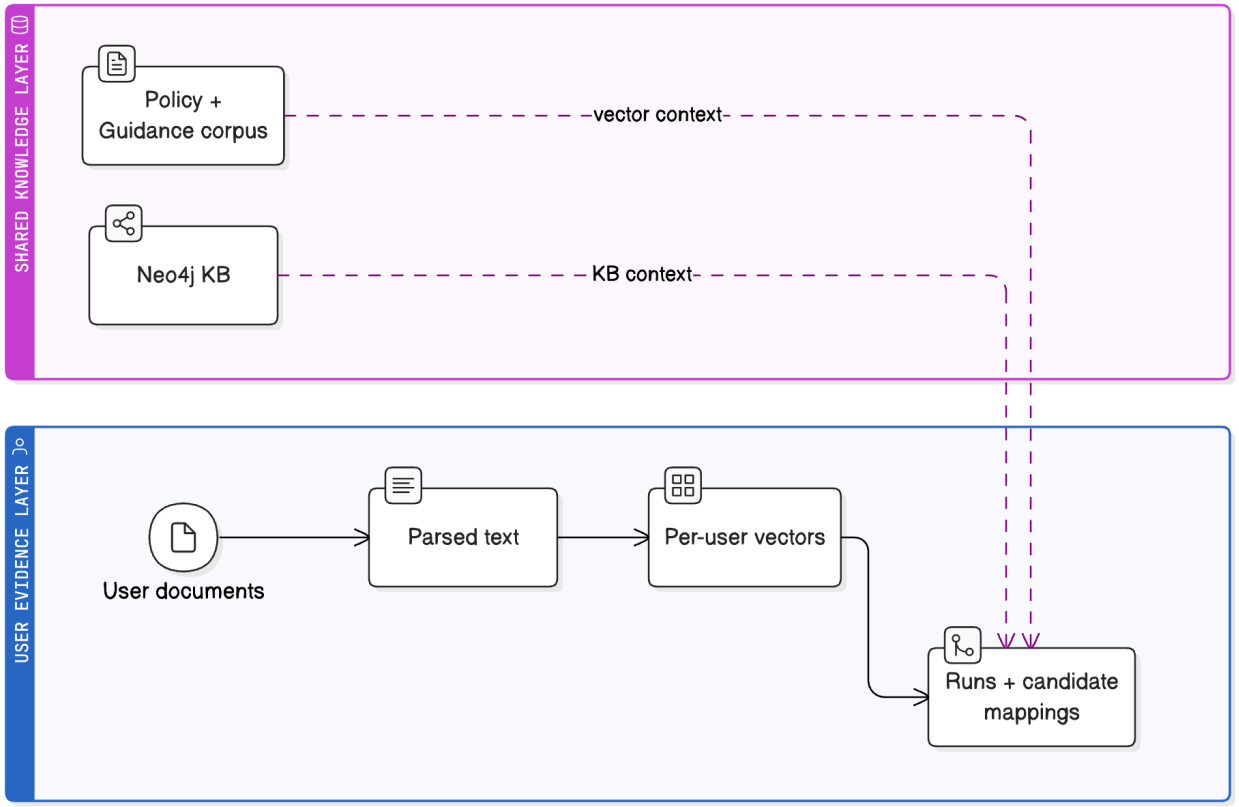
CyberSAGE Design

- Acceleration of Risk Management Framework (RMF) and ATO Delivery
  - Reduce manual efforts across:
    - Control selection
    - Implementation
    - Assessment
    - Authorization activities
  - Baseline security controls, implementation statements, test procedures
    - System maps RMF control requirements
    - Produces and maintains evidence for RMF artifacts
      - Control implementation narratives
      - Test results
      - Assessor ready documentation and reporting

CyberSAGE Platform

Two Knowledge Layers

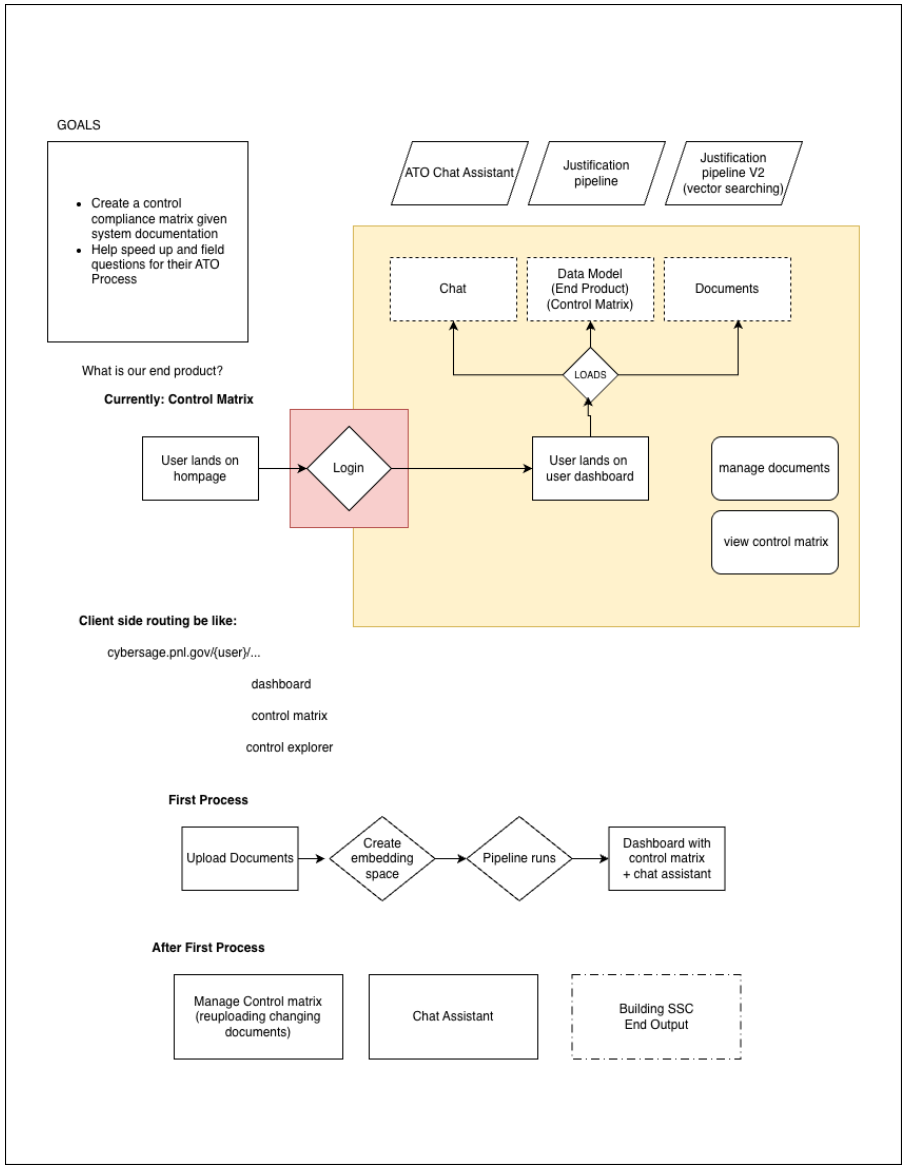
- Shared Knowledge Layer
  - Control, Policy, and Guidance Corpus
- Evidence Layer
  - User documentation
- Intentional Separation



CyberSAGE Platform

User Workflow

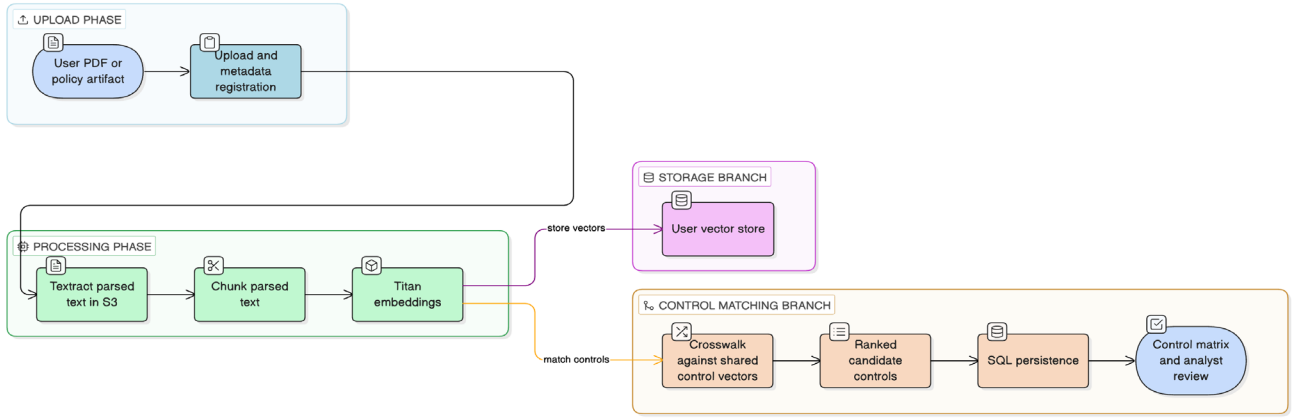
- User Interaction
- Generation of Information
- Process Flow
- Output

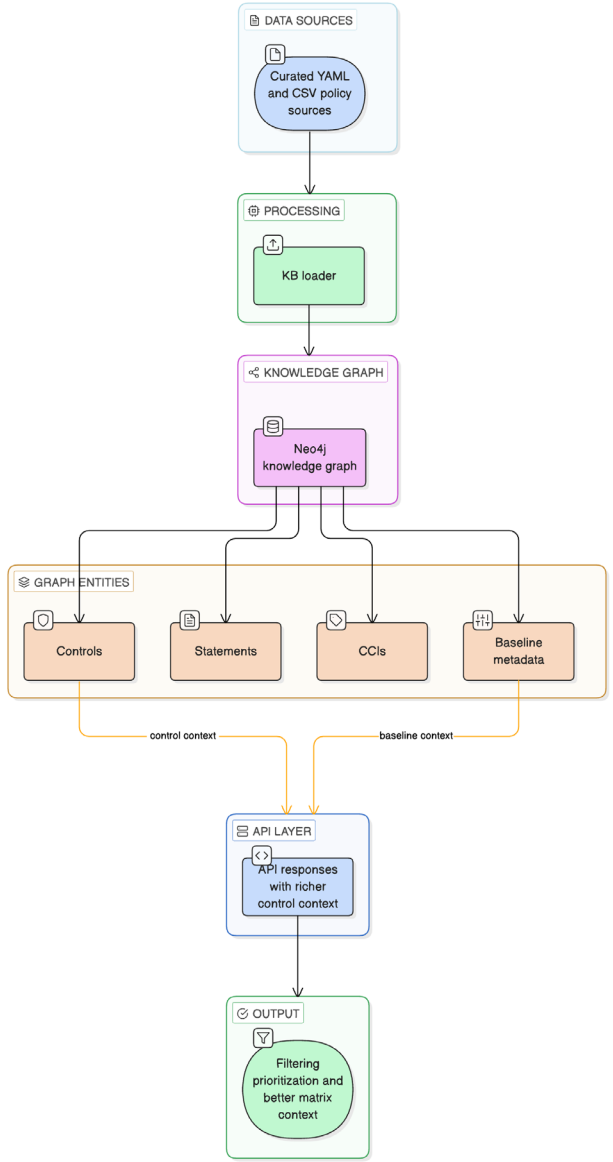


CyberSAGE Evidence & Priority

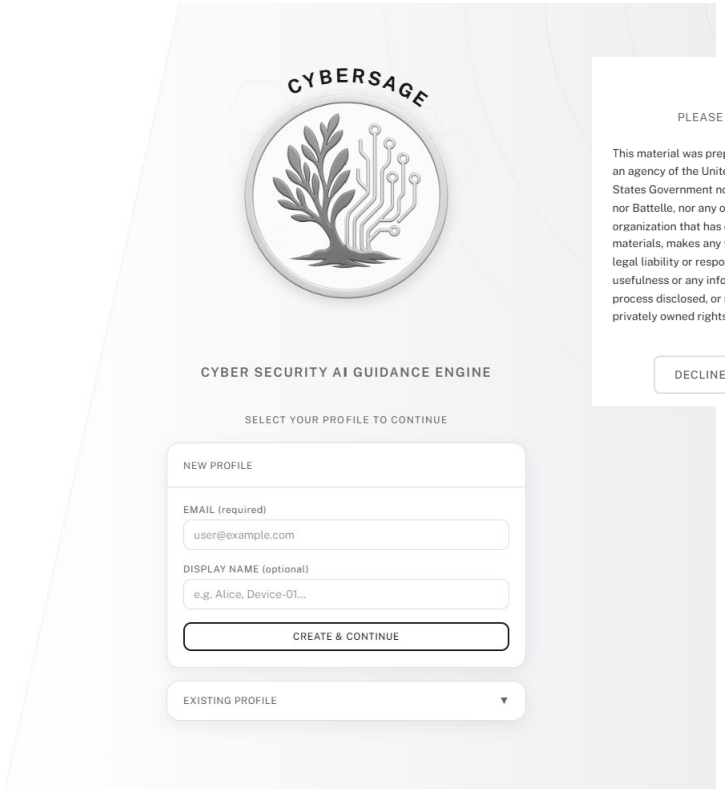
Enrichment + Prioritization

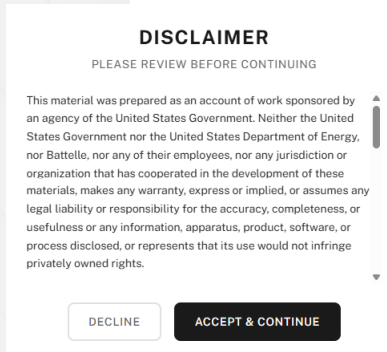
- **Hybrid Approach**
  - **Graph database with a defined topology**
  - **Vector store of policies**
- **Prioritizing baselines, filter by relevant scope, generate a better context aware control matrix**

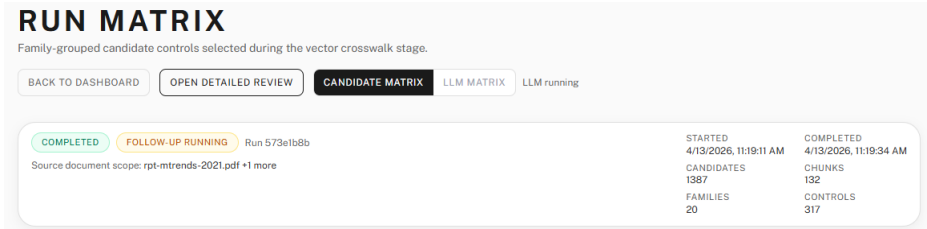


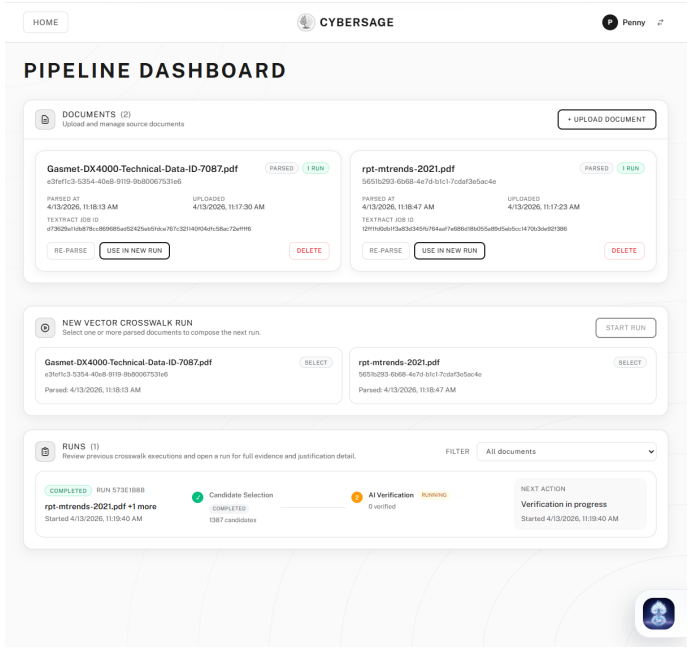


CyberSAGE User Interface





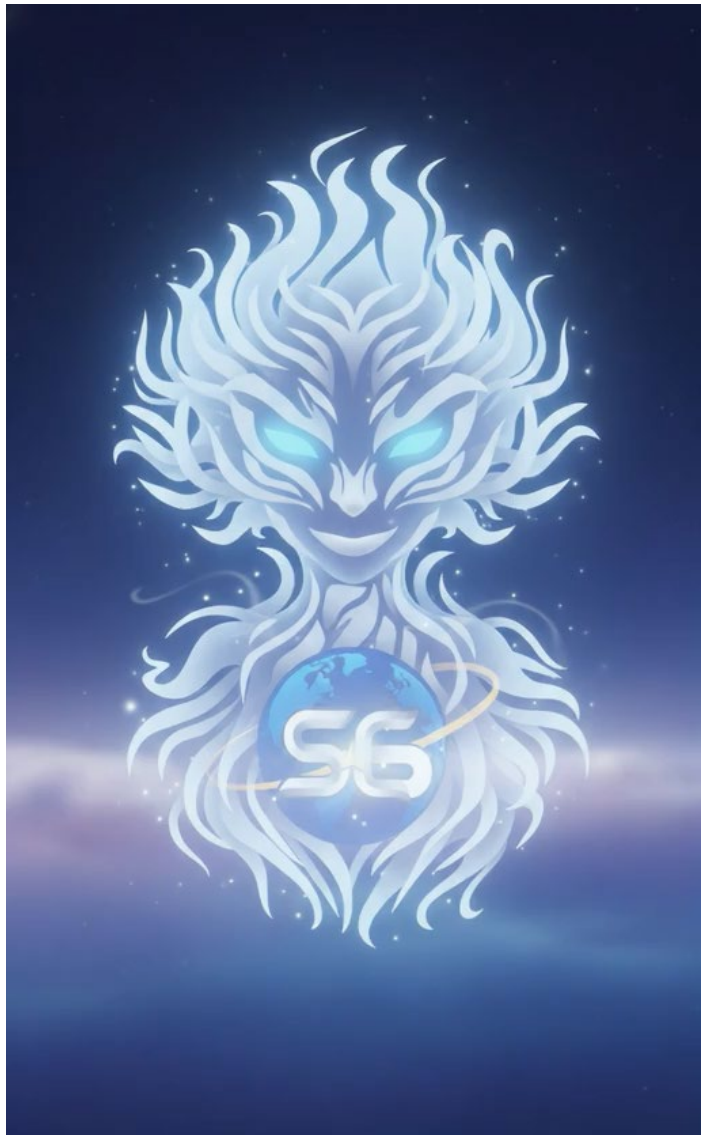




CyberSAGE Assistant

Astraeus

- Interactive assistant designed to support users throughout the ATO process
- Utilizes system, network, and policy documentation
- Provides immediate feedback
- Designed for scalability and extension



Questions?

2026 SSC CYBER EXPO

Digital Guardian

Strategic Framework for Resilient and Mission-Focused AI

Mr. Stew Sutton
SSC/S6

Cyber Readiness at the Speed of Space

Agenda

- BLUF & Executive Summary
- Technical Philosophy: SLM + LLM Hybrid
- Relationship & Depth Components
- Ops Focus: Acquisition Advisor & Issue Stacking
- The AI Agentic Harness
- Technical Roadmap & Maturation Strategy

BLUF & Executive Summary

- Digital Guardian transforms the Space Force into a hybrid human-AI force that out-paces adversary decision cycles
- Delivers three core value propositions:
  1. De-Risking AI Adoption
  2. Technical Superiority via the “Harness”
  3. Weaponizing the Human-AI Partnership

USSF must transition beyond legacy software to become a “ready, digital force”

Technical Philosophy

The SLM + LLM Hybrid Solution

SLM

Fine-Tuned SLMs

- Precision & Security
- Domain-specific, government-approved data only
- Integrated with Knowledge Graphs
- Secure by Design – IL5+ GovCloud or edge (DGX Spark Phone / Station)

+

LLM

Commercial LLMs

- Context & Analysis
- Breadth and creative synthesis
- Secure back-end environments
- Handles complex analysis across untraceable datasets

Structural Relationship and Depth

Total Workflow Harmony

RELATIONSHIP

Personalized to the Guardian

- Roles-based — adapts to Guardian specialty and operational tempo

Syncs cadence and rhythm of work

DEPTH

Ever Expanding Expertise

- Expert in USSF doctrine, DAU standards, and FAR
- Delivers rationalized, actionable advice

Doctrinally sound & factually accurate

AI Persona (Colonel Forge's) Produced COA

Issue Stacking - DoDI 5000.20, Paragraph 5

Technical/Engineering (Sparky)

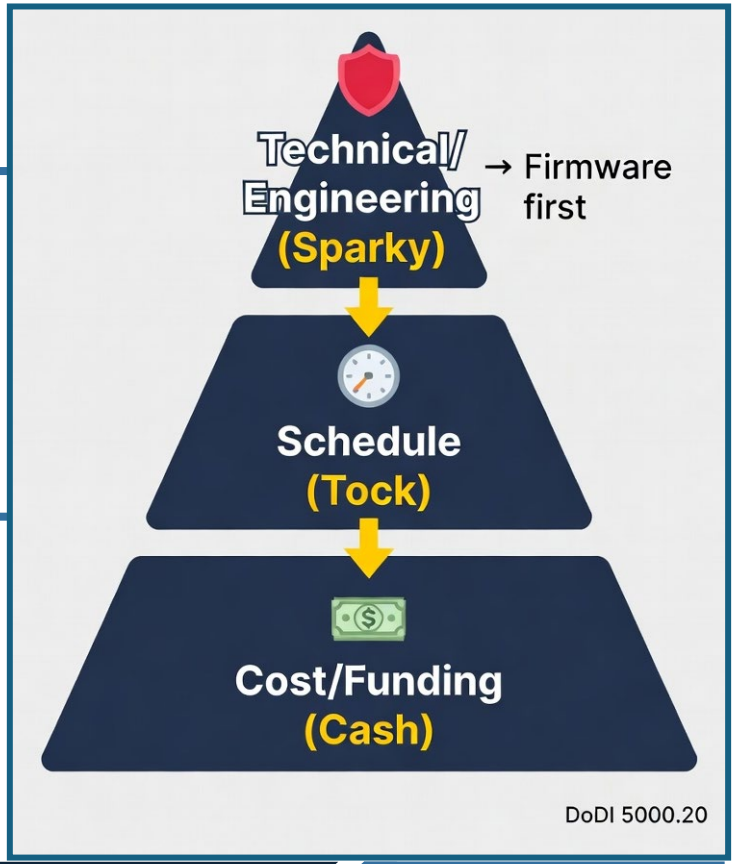
- Patch firmware vulnerability immediately
- (Primary mission protector)

Schedule (Tock)

- Accelerate radiation-hardened enclosure delivery or find substitutes

Cost/Funding (Cash)

- Address stop-work order and funding last

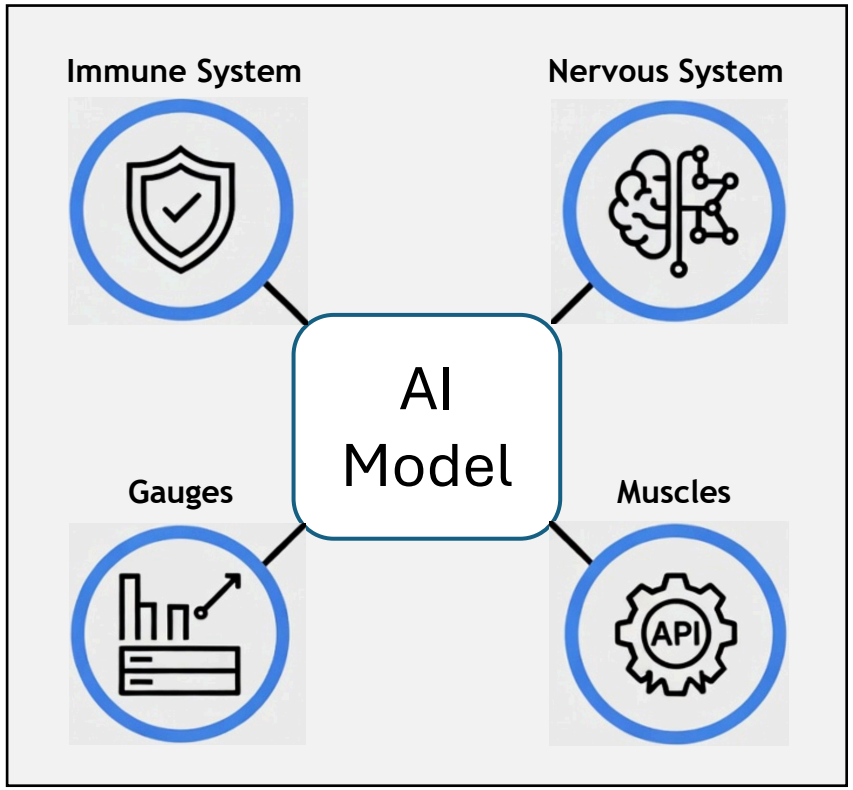


Next Tech Integration: The AI Agentic Harness

Models → Work Engines (10-20% AI Model / 80-90% Harness)

Four Functional Subsystems:

- **Immune System** – Security layer; blocks malicious inputs, filters PII, kills hallucinations
- **Nervous System** – Context & memory management; prevents "context rot"
- **Gauges** – Operational visibility (health, resources, latency)
- **Muscles** – Execution layer; connects to external APIs and databases



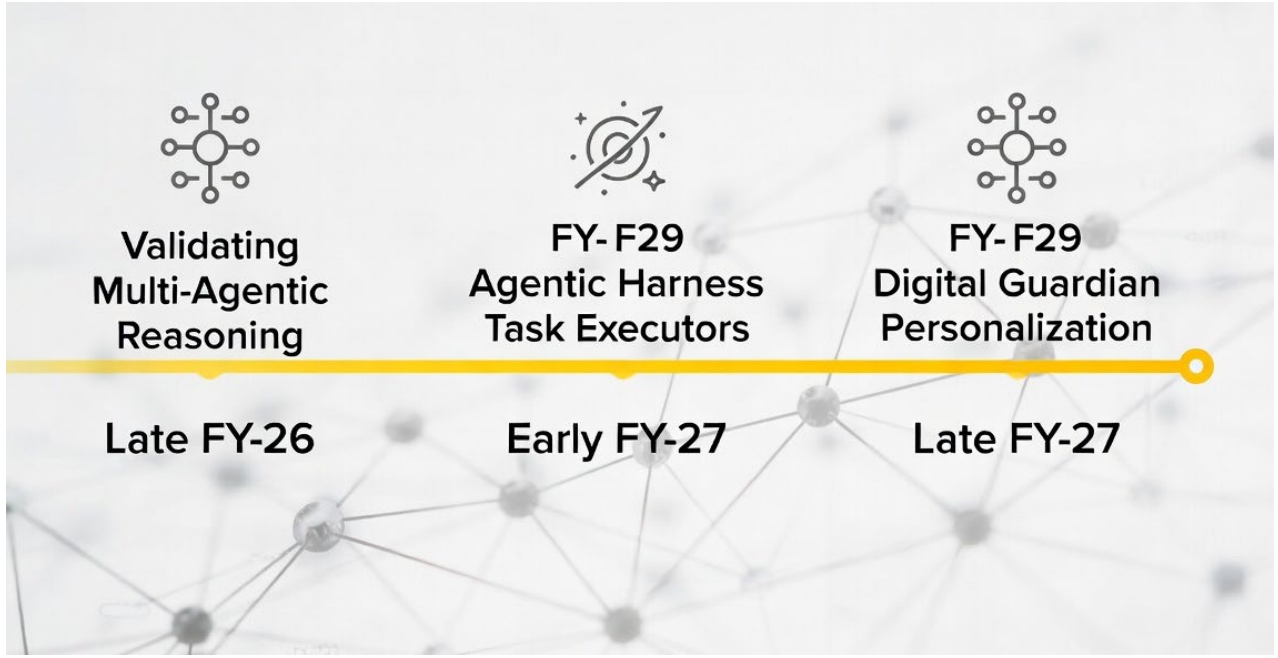
The Harness turns a stateless model into a robust, factually accurate work engine.

Technical Roadmap & Maturation Strategy

Buying down tech risk via rapid commercial-first integration & retaining full control of the technical baseline

Milestones:

- **Late FY-26:** Validating Multi-Agentic Reasoning (Collaborative AI Personas)
- **Early FY-27:** Agentic Harness Task Executors (HITL mixed with HOTL)
- **Late FY-27:** Digital Guardian Personalization via AI Agentic Harness

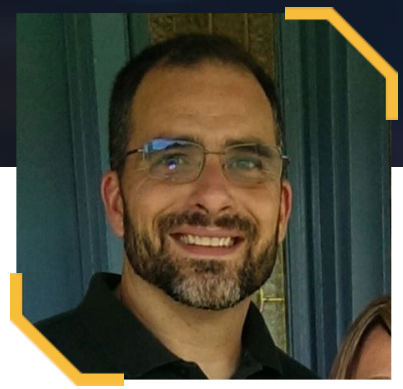


The Harness turns a stateless model into a robust, factually accurate work engine.

Questions?

Thank You!

For more information, please contact:



Bart Stewart
USSF SSC CDAO &
Information Dominance
Div Chief

Jhorda Funes
Director
The Aerospace Corporation

Stew Sutton
Sr. Data Scientist
The Aerospace Corporation

2026 SSC CYBER EXPO

MIT Accelerator - Acquisition Workspace

Maj Alejandro Maldonado
GenAI Branch Chief, SAF/SQ
Marine Corps Officer

Cyber Readiness at the Speed of Space

Agenda

- **MIT Phantom Fellowship Overview**
  - AI Agent Platform Research
- **ACES: Acquisition Contracting Enterprise System**
  - Agentic acquisition and Automation Pipeline
- **Key Results and Path Forward**
  - Questions

MIT Phantom Fellowship

Program Overview

- **Focus Area: AI/ML research and solution sets**
  - Acquisitions Contracting Enterprise System(ACES)

  An agentic platform for program managers and Contracting officers
- **Participant: Maj Alejandro Maldonado, USSF (SAF/SQ)**
  - Generative AI Branch Chief

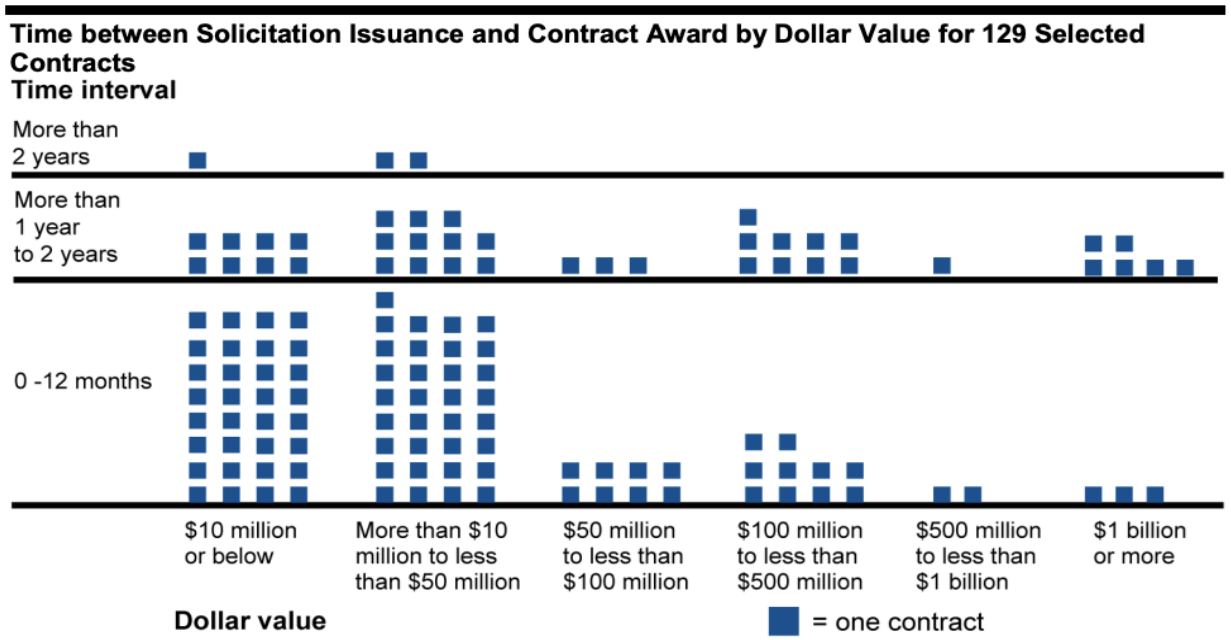
MIT Phantom research focuses on AI/ML topics

Key Project

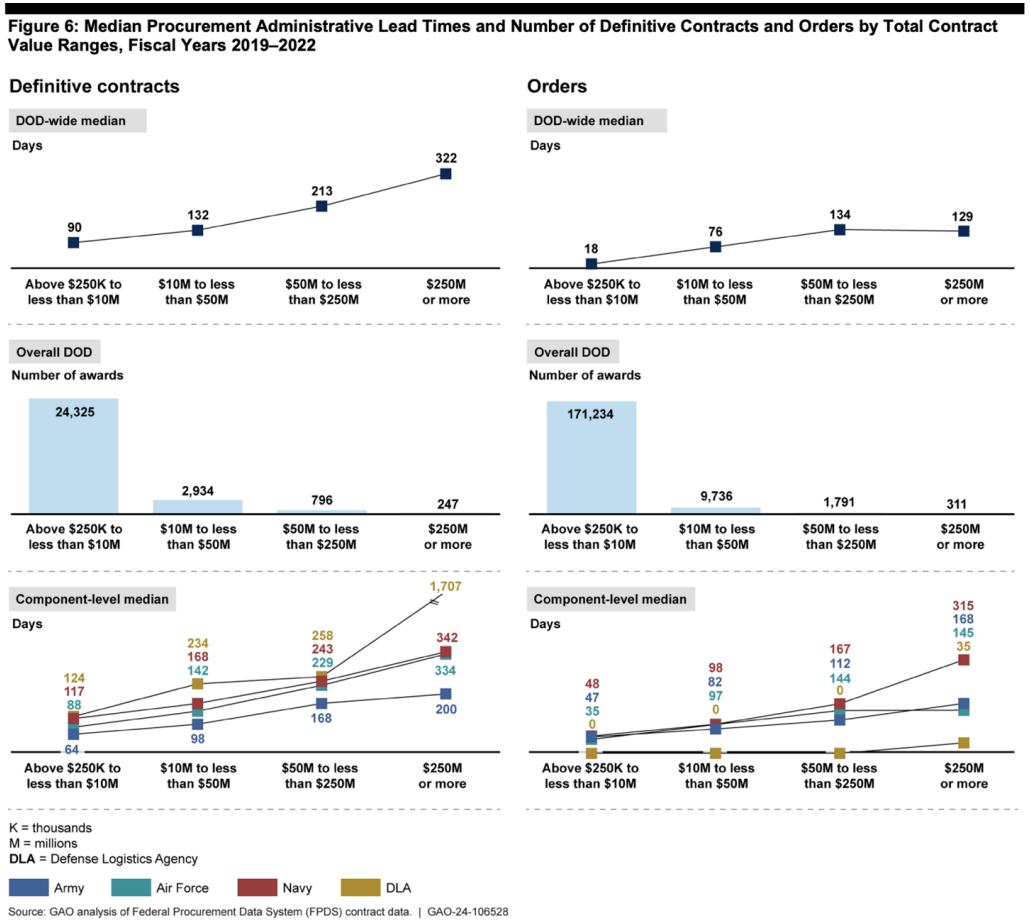
ACES System

- 38-agents integrated into an acquisition automation pipeline
  - Generates program acquisition documents for program managers and contracting officers
  - time savings vs. manual process
- Project workflow
- Smart Live editor with persistence and AI integrations
- Commit History tracking
- Approval workflow
- Compliance reports
- Drag and drop any document in live editor
- export feature

The Problem



Source: GAO analysis of Federal Procurement Data System-Next Generation and Department of Defense contract data. | GAO-18-467



Note We excluded contracts from our analysis that were valued at or below $250,000, generally the simplified acquisition threshold. A solicitation date—used to measure procurement administrative lead time—is not required to be reported into FPDS for awards at or below this threshold. According to DLA officials, the large median procurement administrative lead time we calculated for DLA definitive contracts with total contract values of $250 million or more is likely due to its use of what officials referred to as administrative contracts or orders, issued under existing long-term base contracts.

[1] https://www.nationalww2museum.org
[2] https://www.gao.gov/products/gao-25-108528
[3] https://www.gao.gov/assets/gao-24-106528.pdf

Agentic platform: Agent and Automation Pipeline

Architecture and Tech Stack

The Problem

Multiple documents and hundreds of pages per major acquisition package

- Weeks of manual effort each cycle
- Improve communication through approval workflows

Agentic Solution

- **Claude SDK and API with RAG (FAISS)**

Tech Stack

- **Python, Docling,all-MiniLM-L6-v2,FAISS,Tavily API,JSON,**
  - FAR/DFARS/NMCARS/AFFARS compliant

Three-Phase Pipeline

Pre-Solicitation

- Market Research, IGCE, SOW/SOO
  - Automated requirements analysis

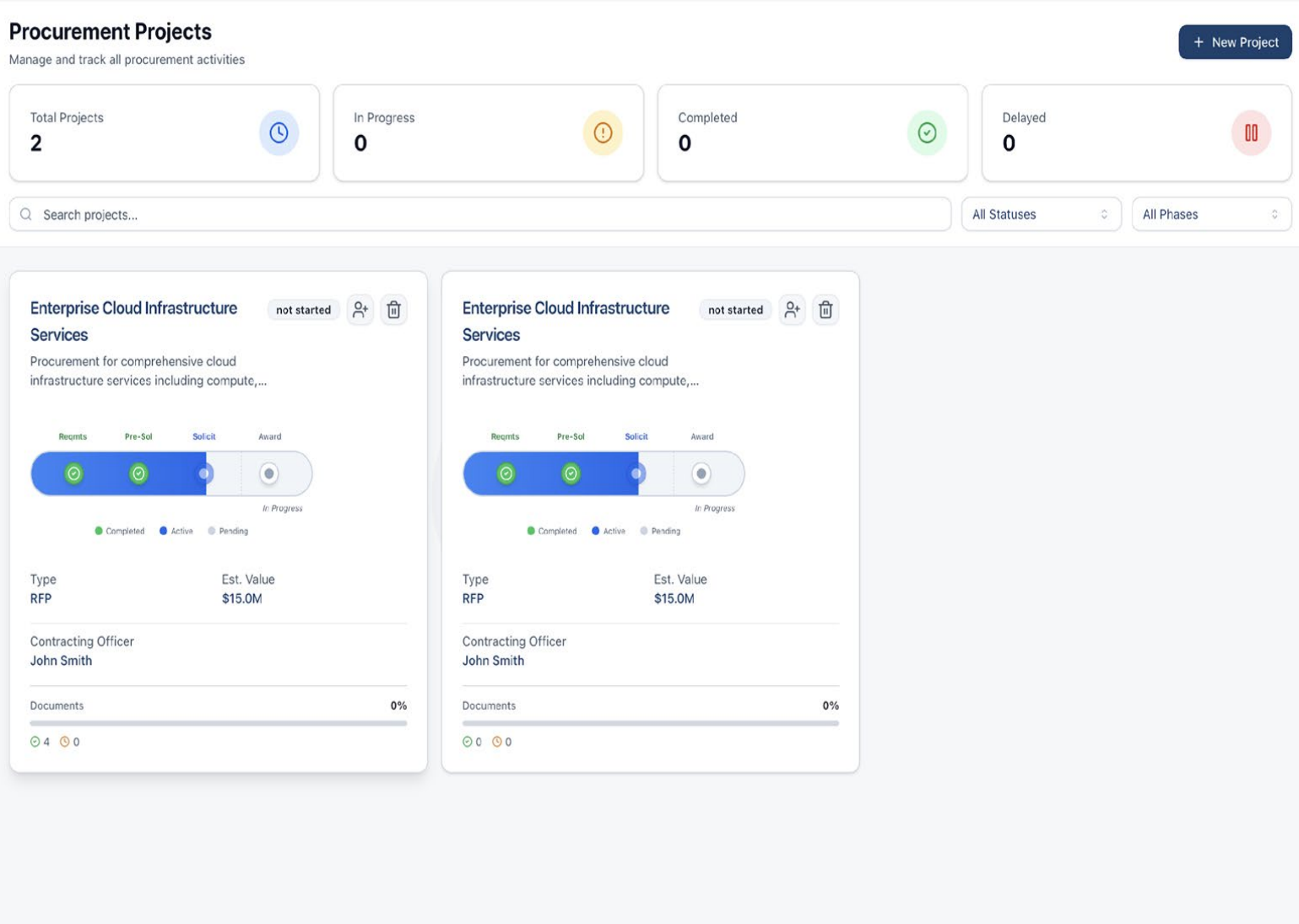
Solicitation

- RFP, Eval Criteria, Source Selection
  - AI-generated evaluation frameworks

Post-Award

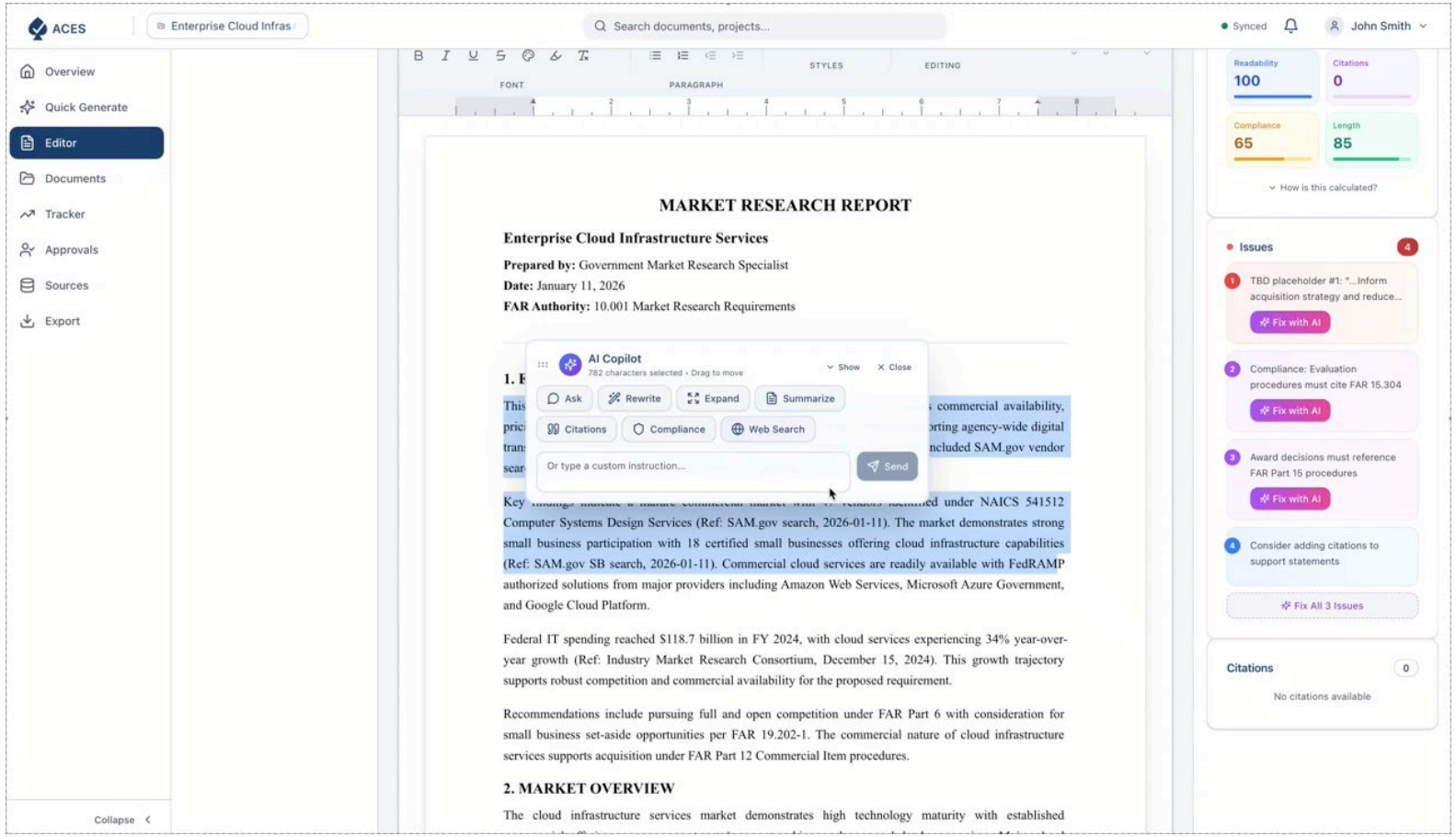
- Award Docs, Notifications, QAE Plans
  - Post-award compliance automation

Features



- RBAC profiles
- Project workflow
- Documentation generation
- Smart Live editor with persistence and AI integrations
- Commit History tracking
- approval workflow
- Compliance reports
- Drag and drop any document in live editor
- export feature

Features



- RBAC profiles
- Project workflow
- Documentation generation
- Smart Live editor with persistence and AI integrations
- Commit History tracking
- approval workflow
- Compliance reports
- Drag and drop any document in live editor
- export feature

ACES: Compressing DoW Acquisition from **Months to Minutes**

AI-orchestrated acquisition documentation with measurable speed and cost impact.

METHODOLOGY

Manual Baseline Costs:

- Estimated 400–800 hours per acquisition package
- Manual document preparation costs **$40,000~$96,000** per acquisition
- Using the OPM GS-13 Step 5 locality-adjusted rate for Washington-Baltimore at **400–800** hours
  $56.32/hour base
  $100–$120/hour fully loaded

$750 per acquisition

How Is the $750 Per Acquisition Cost Calculated?

- LLM API usage: $15–$25
- Human review time: 4–8 hours: **$400–$960**
- Infrastructure (prorated): $50–$100
- **Total Cost Per Acquisition: $750**

PROJECTED SAVINGS

Mid-range estimates ($66,000 manual cost, $750 ACES cost per acquisition)

Acq./Year	Manual Cost	ACES Cost
5	$330,000	**$3,750**
10	$660,000	**$7,500**
20	$1,320,000	**$15,000**
50	$3,300,000	**$37,500**

DoW-SCALE IMPACT

Adopting ACES at minimal level

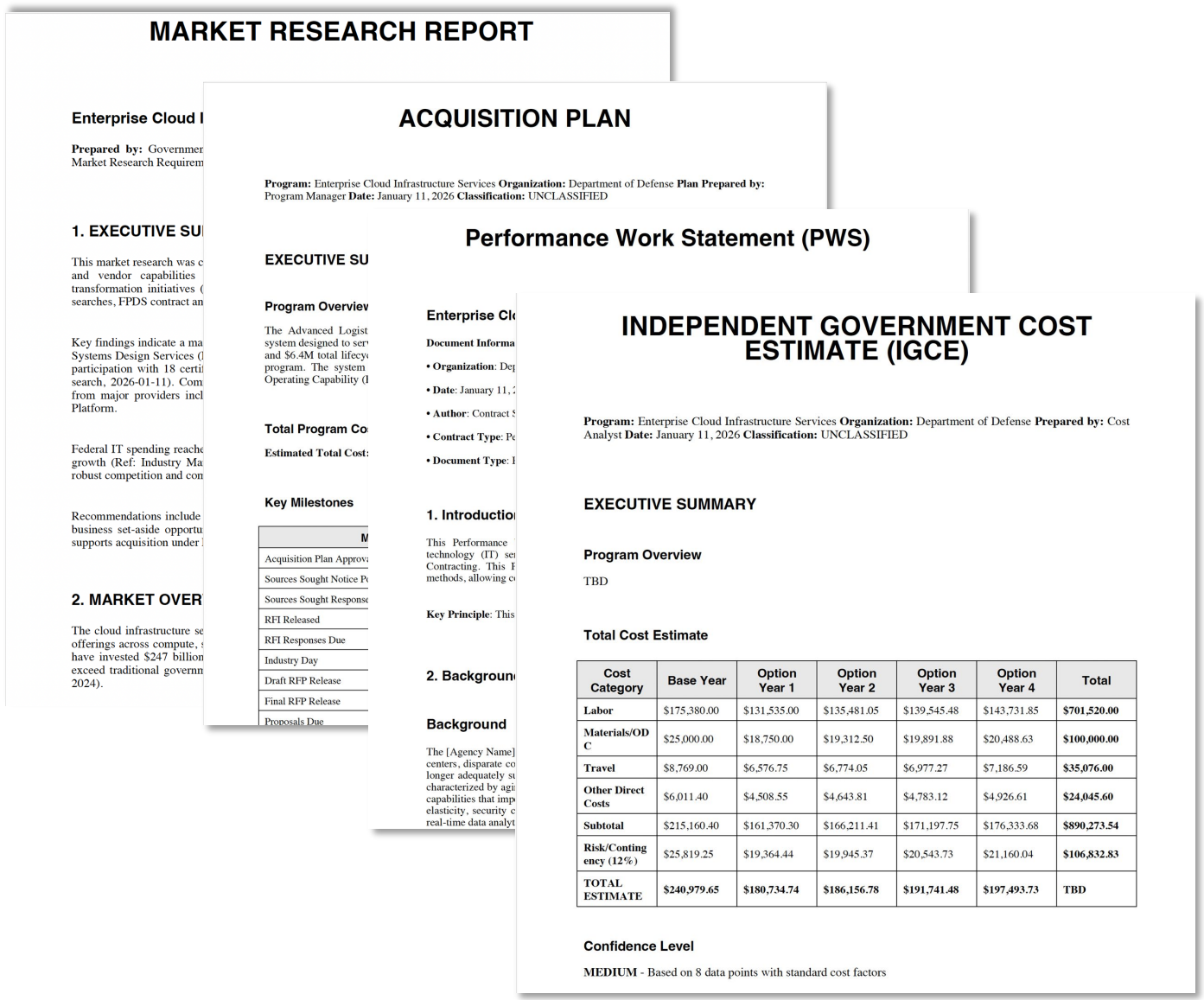
$195.75M Annual Savings

- DoW executes over **3,000,000+** contract transactions annually with the Navy and Air Force accounting for over **300,000** of those transactions
- 1% of contract actions = 3,000 acquisitions automated

3,000 × $65,250 = **$195.75M**

ACES transforms acquisition documentation **from a labor bottleneck into a scalable, AI-driven capability**—without changing FAR, DFARS, or workforce structure.

DEMO



MARKET RESEARCH REPORT

Enterprise Cloud I

Prepared by: Governmer
Market Research Requirem

1. EXECUTIVE SU

This market research was c
and vendor capabilities
transformation initiatives (
searches, FPDS contract an

Key findings indicate a ma
Systems Design Services (I
participation with 18 certi
search, 2026-01-11). Com
from major providers incl
Platform.

Federal IT spending reache
growth (Ref: Industry Ma
robust competition and con

Recommendations include
business set-aside opportu
supports acquisition under

2. MARKET OVER

The cloud infrastructure se
offerings across compute,
have invested $247 billion
exceed traditional governn
2024).

ACQUISITION PLAN

Program: Enterprise Cloud Infrastructure Services **Organization:** Department of Defense **Plan Prepared by:** Program Manager **Date:** January 11, 2026 **Classification:** UNCLASSIFIED

EXECUTIVE SU

Program Overviev

The Advanced Logist
system designed to ser
and $6.4M total lifecy
program. The system
Operating Capability (I

Total Program Co

Estimated Total Cost:

Key Milestones

M
Acquisition Plan Approva
Sources Sought Notice P
Sources Sought Response
RFI Released
RFI Responses Due
Industry Day
Draft RFP Release
Final RFP Release
Proposals Due

Performance Work Statement (PWS)

Enterprise Cl

Document Informa

- **Organization**: Dep
- **Date**: January 11,
- **Author**: Contract S
- **Contract Type**: Pe
- **Document Type**: I

1. Introductio

This Performance
technology (IT) se
Contracting. This P
methods, allowing c

Key Principle: This

2. Backgroun

Background

The [Agency Name]
centers, disparate co
longer adequately su
characterized by agi
capabilities that imp
elasticity, security c
real-time data analyt

INDEPENDENT GOVERNMENT COST ESTIMATE (IGCE)

Program: Enterprise Cloud Infrastructure Services **Organization:** Department of Defense **Prepared by:** Cost Analyst **Date:** January 11, 2026 **Classification:** UNCLASSIFIED

EXECUTIVE SUMMARY

Program Overview

TBD

Total Cost Estimate

Cost Category	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4	Total
Labor	$175,380.00	$131,535.00	$135,481.05	$139,545.48	$143,731.85	**$701,520.00**
Materials/ODC	$25,000.00	$18,750.00	$19,312.50	$19,891.88	$20,488.63	**$100,000.00**
Travel	$8,769.00	$6,576.75	$6,774.05	$6,977.27	$7,186.59	**$35,076.00**
Other Direct Costs	$6,011.40	$4,508.55	$4,643.81	$4,783.12	$4,926.61	**$24,045.60**
Subtotal	$215,160.40	$161,370.30	$166,211.41	$171,197.75	$176,333.68	**$890,273.54**
Risk/Contingency (12%)	$25,819.25	$19,364.44	$19,945.37	$20,543.73	$21,160.04	**$106,832.83**
TOTAL ESTIMATE	**$240,979.65**	**$180,734.74**	**$186,156.78**	**$191,741.48**	**$197,493.73**	**TBD**

Confidence Level

MEDIUM - Based on 8 data points with standard cost factors

ACES delivers acquisition documents and contracting packages, cutting delivery from weeks and months to minutes!

Thank You!

For more information, please contact:

Maj Alejandro Maldonado
GenAI Branch Chief, SAF/SQ
alejandro.Maldonado.3@us.af.mil

Questions?

2026 SSC CYBER EXPO

Stanford AI Accelerator

Lt Devrin (C-13) Chullanandana
HQ USSF
Founder, USSF AI Accelerator

Cyber Readiness at the Speed of Space

Stanford AI Accelerator

USSF

USSF AI Accelerator at Stanford

Who We Are

- SSC-stood-up USSF AI Accelerator, formally signed by Ms. Eberhardt; supported by Lt. Gen. Garrant
- Partnered w/ LLNL — already executing space-relevant work with NRO, SWAC, Mission Delta 9, and SYD 81 (OTTI)
- Provides operator and acquisition pull to de-risk and tech-transfer AI from labs/startups into USSF execution
- On-ramp for HQSF/S6 funding to support near-term OTTI-aligned efforts

Col. Jason Hansberger
Director, DAF AI Studio

Maj. John Alora
Stanford PhD Research Lead

Lt. Devrin Chullanandana
Founder, USSF AI Accelerator

Stanford AI Accelerator

Space Rendezvous Lab (SLAB) Roadmap Update

CAESAR
Center for Aerospace Autonomy Research

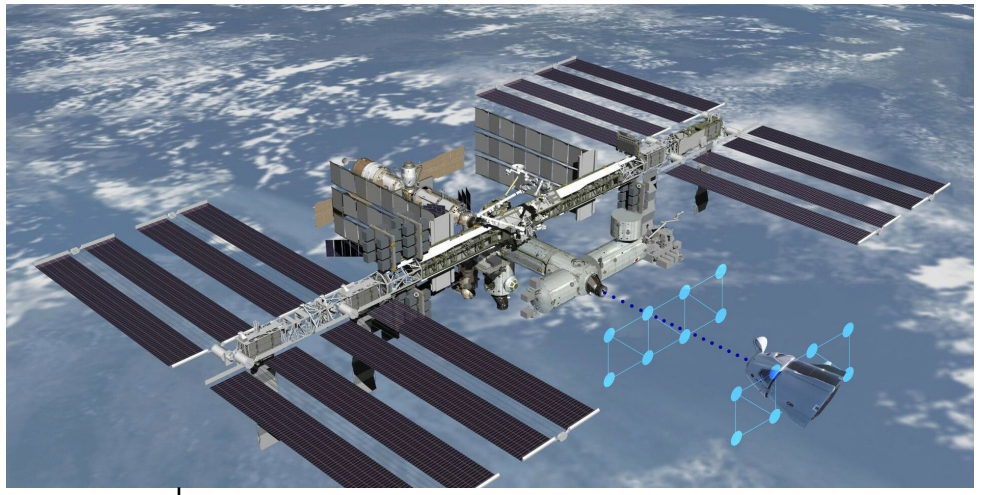
rendezvous Space
Space Rendezvous Laboratory

USSF

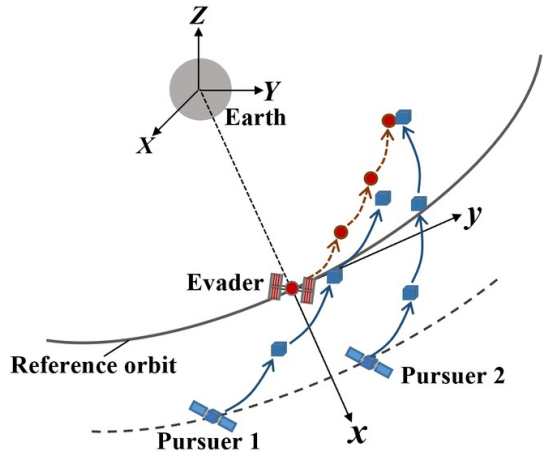
Intent-Conditioned Adversarial Autonomy

Project Overview

- Motivation: orbital warfare is a burgeoning mission area. Using machine learning and data at scale will aid not only in tactic development and operator training, but eventual capability deployment on-orbit.
- Research Description: orbital pursuit-evasion games (OPEGs) describe a class of warfighting scenarios where spacecraft maneuver against each other to achieve tangible, tactical objectives. By leveraging semantic language processing, machine learning, and convex trajectory optimization, there are potential ways to recognize adversarial intent and condition autonomous GNC for orbital warfare.
- Existing Literature: Chinese researchers have published 50+ research papers on OPEGs since January 2025. The vast majority leverage AI/ML.
- Reasoning-based Autonomous Guidance Engine for Space (RAGES): Stanford SLAB is developing a framework for reasoning-based semantic spacecraft guidance by integrating learning-based intent inference with optimization-based trajectory generation with safety guarantees.
- USSF Deliverables: Reasoning data for fine-tuning, AI tools, prototypes, representative M&S, laboratory demonstrations, and APIs for test & training environments
- Guardian Researcher: Capt Gordon McCulloh



Re-cast Autonomous **Intent-Conditioned GNC** for **Orbital Pursuit Evasion**



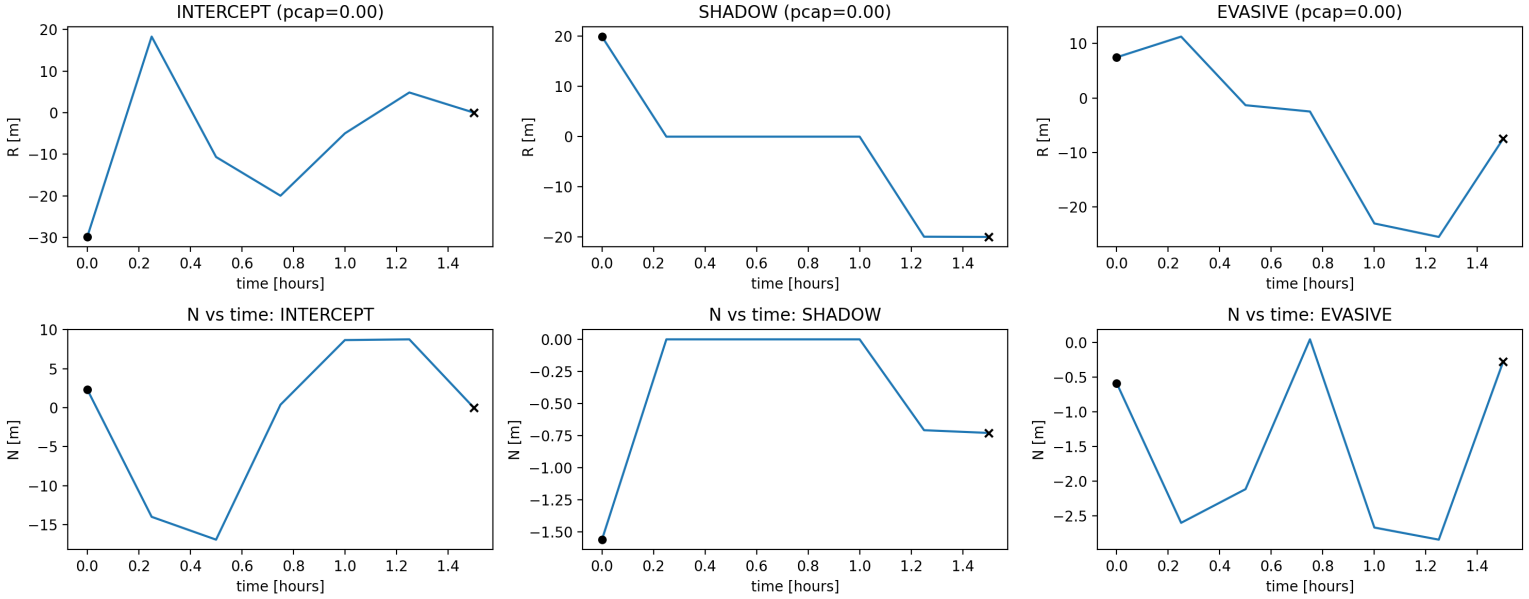
CAO: 27 Mar 26

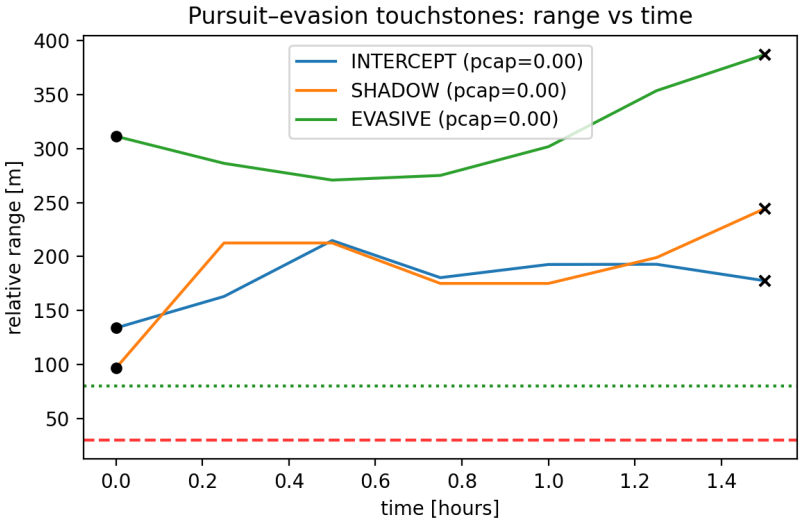
Topic Collaboration

- Academia
  - Stanford (Space Rendezvous Lab) – research hub for trajectory optimization via Reasoning-based Autonomous Guidance Engine for Spacecraft (RAGES)
  - New Mexico State University – research on intent classification under AFRL
- Space Operations
  - CFC 3 SOPS/CDET 3-1 – adapting Tactical Standard Operating Procedures for rapid-reaction orbital warfare to spacecraft pursuit-evasion behaviors
  - Delta 9 – actively developing the Mission Planning Guide for Space Domain Awareness
- Laboratories
  - Lawrence Livermore National Lab – adapting multi-agent RL 2v1 pursuit-evasion simulator for intent recognition
  - Sandia National Lab – using different RL methods to solve 1v1 pursuit-evasion games
  - AFRL/RVSW – collaborating with the Space Warfighting Directorate on state-of-the-art intent classification algorithms
  - AFRL/RYA – concept development for training TALOS (Slingshot Aerospace) for operational deployment
- Intelligence Community
  - NRO – developing taxonomy for spacecraft relative motion and out-of-distribution behaviors

Progress

- RAGES Shell
  - Data Flywheel – created a pursuit-evasion game environment that acts as a shell to the existing reasoning-based autonomous guidance engine for synthetic data generation at scale
  - Behavioral Primitive Modeling – expanded the set of semantic behavioral primitives available to spacecraft according to strategic intents and generalized tactical SOPs from the space ops community
  - Domain physics – incorporating critical domain information such as camera-angle-target-sun to the RPO codebase to enable sensor-based adversarial intents

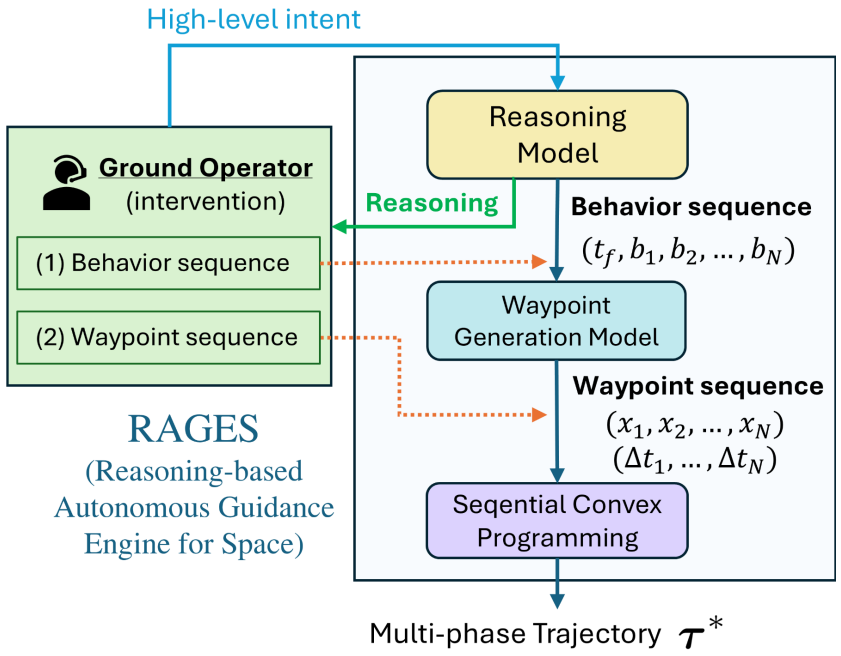




- **RL Dynamics**
  - **PPO** – testing proximal policy optimization as the basic heuristic for pursuit spacecraft against intent-conditioned evader
  - **Discrete impulse** – deliberately choosing a non-continuous thrust strategy to constrain the training of orbital warfare agents

Integration Efforts and Mission Impacts

- ## Current Work
  - Refining RAGES wrapper for OPEG gym environment with varying RL approaches
  - Model training and scaling
  - Investigation of intent conditioning as a valid training approach
  - Laying the groundwork for multi-agent RL for distributed space system or “swarm” engagements
- ## Integration
  - Short term: SWORD environment (LLNL)
  - Long term: on-orbit deployment with human operator orchestration
- ## Mission Impact(s)
  - Semantic decision support for scalable training and enhanced aggressor realism
  - Safety supervision



Objective: Apply semantic autonomous spacecraft guidance to adversarial intent recognition and pursuit-evasion games

Problem Scoping	Literature Review	Code Development	Research Paper	Model Training	Fine Tuning	Model Validation	Publish to USSF Community
Jan-Feb ‘26	Jan-Mar ‘26	Feb-Jun ‘26	Mar-Jun ‘26	Mar-May ‘26	May-Jun ‘26	Jun ‘26	Jul-Sep ‘26

Adversarial intent reasoning & autonomous engagement

- Safety-critical oversight
- Threat reaction
- Tactic generation per doctrine
- Distributed systems

Stanford AI Accelerator

Autonomous Systems Lab (ASL)
Adversary Intent Runtime Monitor

Brandon Kim, 1st Lt, USSF
Guardian Researcher
brandon.kim.9@spaceforce.mil

USSF

Problem Statement

- **Orbital Pursuit-Evasion Games (OPEGs):** Adversarial scenarios where satellites engage in maneuver-based competition to achieve proximity, execute intercepts, or evade capture under orbital constraints.
- **Zero Trust in Space:** High-stakes autonomy demands “Zero Trust” framework, requiring rigorous offline verification and runtime uncertainty quantification to prevent failures.
- **Doctrinal North Star:** Leverage established military doctrine and Standard Operating Procedures (SOPs) as high-level semantic signals to interpret agent maneuvers.
- **ASL Publications:** FORTRESS is a multi-modal framework that synthesizes semantically safe fallback plans for Out-of-Distribution (OOD) failures and hazards in real-time.

- OPEGs require discerning novel adversarial threats from benign doctrinal maneuvers.
- ***How can a system detect Out-of-Distribution (OOD) adversarial behavior and initiate a safe recovery before a collision or intercept occurs?***

USSF

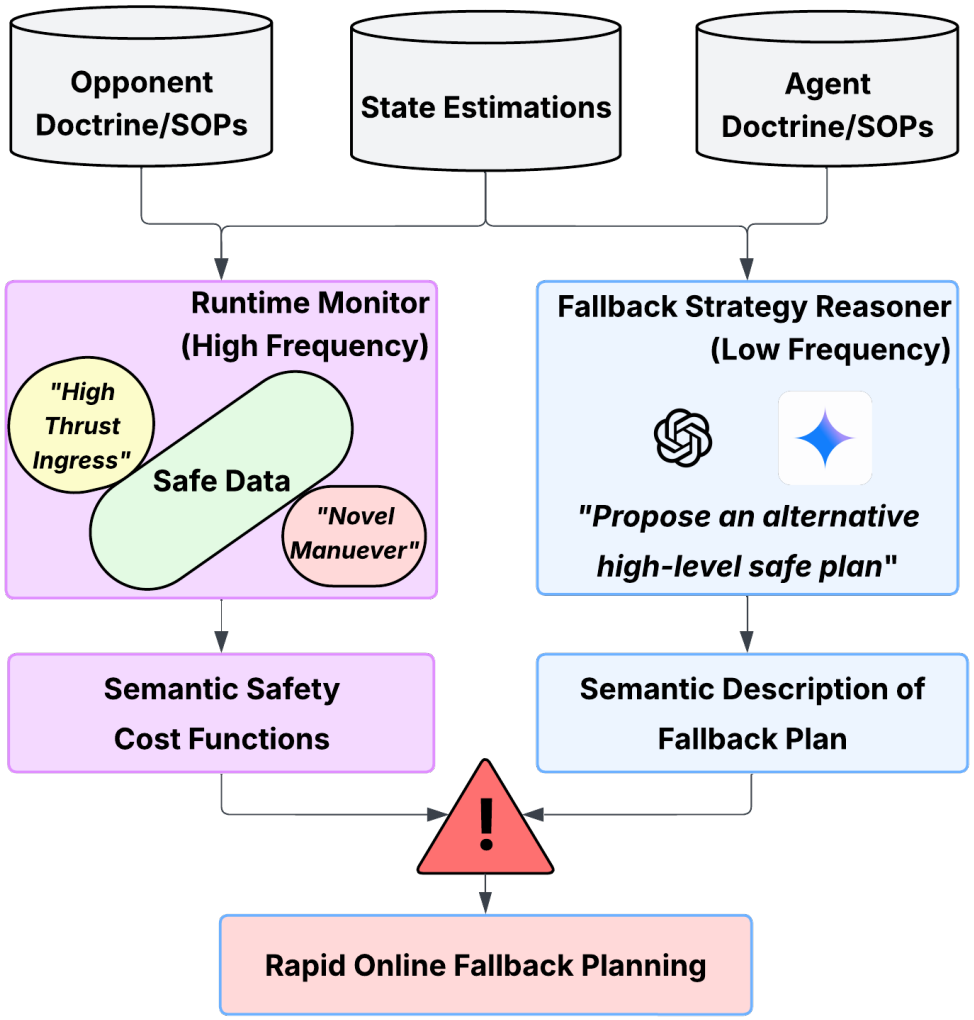
Stakeholders

- MD 2, 18 Space Defense Squadron (18 SDS)
- Combined Space Operations Center (CSpOC)
- Joint Commercial Operations (JCO)
- MD 9, National Space Defense Center (NSDC)
- Department of Commerce

USSF

Solution Architecture

- Module 1: Runtime Monitor
  - Calibrate shared latent space for trajectories and doctrine/SOPs
  - Monitor and flag for OOD adversarial intent and hazards
- Module 2: Fallback Strategy Reasoner
  - Foundation Model proposes semantic description of alternate safe plans
- Module 3: Fallback Plan Execution (SAGES)
  - Trigger alert for operator
  - Synthesize the fallback path in real-time
  - Execute dynamically feasible maneuvers



Integration Efforts and Mission Impacts

- **Current Work**
  - Curate dataset with trajectory-semantics pairings
  - Develop runtime monitor for uncertainty quantification
- **Integration**
  - Short term: SWORD environment (LLNL)
  - Long term: On-orbit deployment with human operator orchestration
- **Mission Impact**
  - Supervision and alert of failure modes
  - Rapid online fallback response

USSF

Roadmap

HIGH

Objective: Create Failure Mode Assistant for adversary runtime monitoring and strategic fallback reasoning, in collaboration with Stanford Autonomous Systems Lab (ASL) and Center for Aerospace Autonomy Research (CAESAR).

Attend CAESAR Annual Event & ACT4AERO	Generate Synthetic Trajectory- TTP Corpus	Build Doctrinal Vector Store (i.e., RAG Database)	Develop Online Failure Mode Assistant	Present Deliverables to DAF-AI Studio, CAESAR, and S6
Mar '26	Apr '26	Apr '26	May '26	Jun '26

End States

- ❑ Failure Mode Assistant capable of aligning satellite trajectories with automated doctrinal justifications.

MED

Objective: Integrate system feature into the Space Warfighter Operational Readiness Domain (SWORD) environment to enhance the Thinking Agent for Logical Operations and Strategy (TALOS) agent with explainable, failure mode detection capabilities.

Meet with OTTI and other stakeholders	Establish access to SWORD via OTTI	Generate SWORD-based Trajectory-TTP Corpus	Integrate SWORD-based TACTS to TALOS	Develop user-informed tools (e.g., automated debrief reporting)	Present Deliverables to DAF-AI Studio, OTTI, and S6
Feb '26	May '26	May '26	May '26	Jun '26	Jul '26

- ❑ Prototyped Failure Mode Assistant integrated into TALOS and SWORD with specific features.

What is the Genesis Mission?

Executive Order (Nov 24, 2025) launched a DoE-led national initiative to transform science & national security with AI

Origin

El Capitan (LLNL): 2.79 exaflops — the most powerful supercomputer in the world, purpose-built for national security science

Compute

Unified data + HPC + manufacturing + AI ecosystem connecting national labs, enabling "text-to-X" for rapid design and discovery

The Platform

25+ challenge problems spanning materials science, nuclear, quantum, manufacturing — and national security applications

Scope

DoE-led initiative transforming science and national security with AI across 25+ challenge problems — referenced during SecWar's speech at Starbase

Partners

LLNL, LANL, SNL, PNNL, Argonne, Oak Ridge + private sector (initial collaborators announced)

Referenced during SecWar's speech at Starbase — this is the administration's flagship AI initiative.

Why USSF Must Move First

The Strategic Case for Early Engagement

THE OPPORTUNITY

Massive compute — minimal cost to USSF

DoE funds the hardware. Early engagement with existing problems costs nothing; **DoW is already investing in Genesis.**

USSF problems shape the models

Embedded operators inject SDA, battle management, fire control, and object tracking problems directly into the research pipeline.

Research-to-acquisition pipeline

SAF/SQ engagement ensures outputs flow from lab research → prototypes → acquisition pathways.

White House visibility

Genesis is the administration's flagship AI initiative. USSF being first-in earns strategic positioning at the national level.

THE RISK OF WAITING

Compute is a war of resources

Every service and IC agency is competing for time on national lab HPCs. Services that embed first get priority scheduling.

Someone else's priorities get trained

If USSF isn't at the table when models are being built, those models get optimized for other domains.

Growing waitlist is real

LLNL has flagged that demand for Genesis slots is accelerating. Delay risks losing placement entirely.

Window closes fast

Genesis is moving at startup speed. The platform architecture is being set NOW. Influence requires presence, not memos.

Bottom Line: This is not a nice-to-have. The service that shows up first gets its problems prioritized. USSF needs to be that service.

2026 SSC CYBER EXPO

Closing Remarks

Col Brian Mihalko
SSC/S6 Director

Feedback Survey

Cyber Readiness at the Speed of Space