SAME
Pikes Peak Post

General Membership Meeting
November 10, 2020

Col Jim Brackett, PE, F.SAME (USAF Ret)
President

DISCOVER
YOUR ROLE
IN BUILDING
AMERICA'S
FUTURE.

Agenda

- Welcome & Pledge
- Housekeeping
- Welcome New Members
- Upcoming Events
- USAFA Engineering & Construction Camp Alumni Feedback
- Guest Speaker
  - William J. Beary, P.E. F.SAME
  - GS-15 DAFC, NORAD and USNORTHCOM/J42 Chief, Engineering Division

Housekeeping

- Please mute phones and turn-off webcams
- Submit all questions via chat
- Webinar will be recorded and available following program
- PDH Credit certification can be obtained by emailing Bob Fant
  - robert.fant.1@us.af.mil

New Members – Joined in October

CPT Matthew Riggs

Dr. John Carson, Neptune & Company

Carolyn Terrell

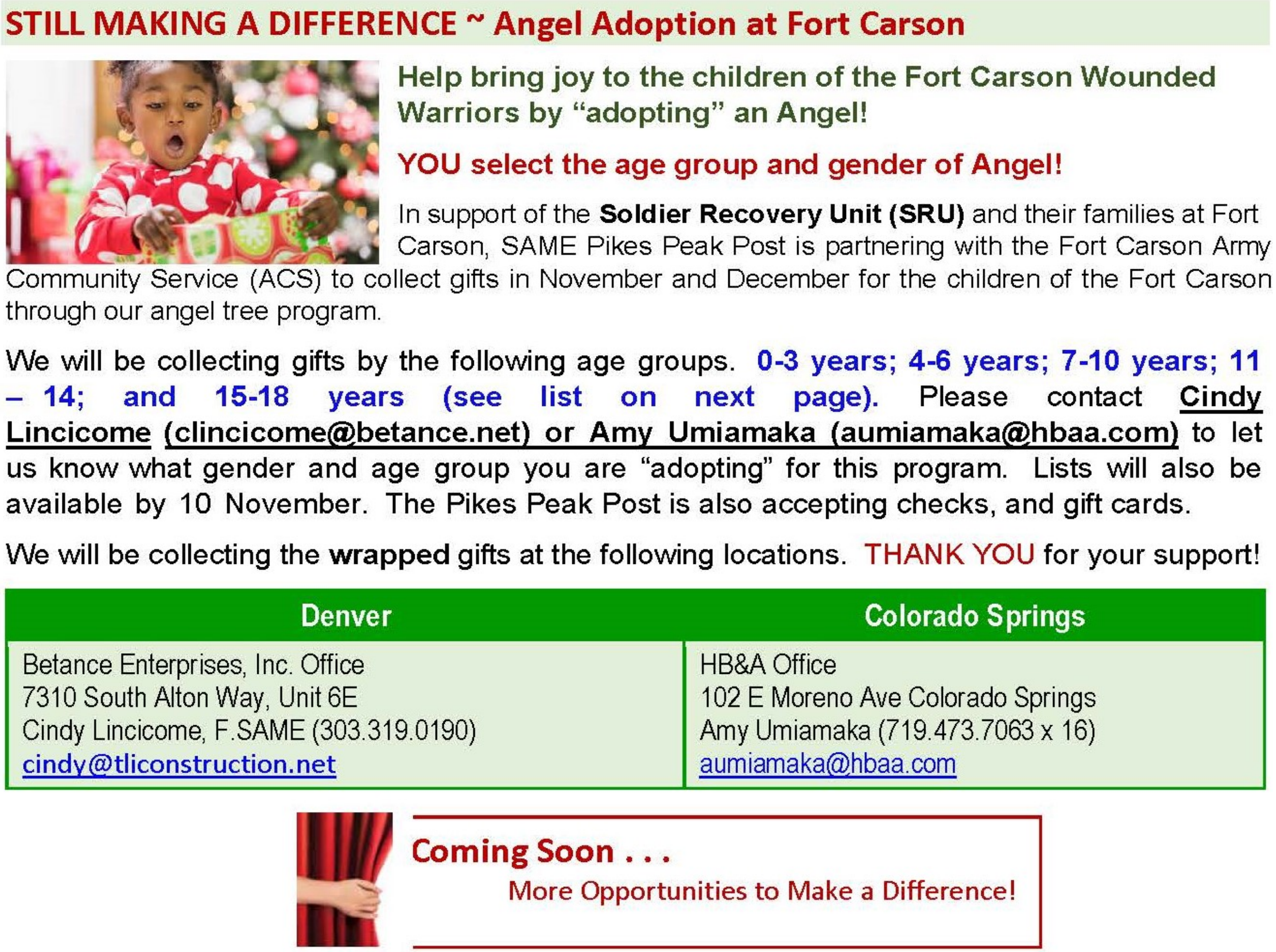
Capt Charles (Dirk) MacDonald, USAFA

Brian Best, HDR

Upcoming Events

- Joint Denver Metro & Pikes Peak Posts Membership Meeting
  - November 17, 2020 | 11:30am-1:30pm MT - 2020 Task Force Colorado COVID-19 Alternate Care Facility (ACF) Response
    - Bruce Gurney, USACE: Colorado Convention Center Alternate Care Facility
    - Joe Caracillo, USACE: The Range, Loveland, CO; Alternate Care Facility
- SAME Leader Development Program
  - Application for 2021-2022 program open now
  - Application period closes ***7 Dec 2020***
  - https://www.same.org/Grow-Professionally/Leader-Development-Program
  - Contact Zakary Payne Zakary.Payne@matrixdesigngroup.com if interested

Soldier's Recovery Unit Angel Tree



STILL MAKING A DIFFERENCE ~ Angel Adoption at Fort Carson

Help bring joy to the children of the Fort Carson Wounded Warriors by "adopting" an Angel!

YOU select the age group and gender of Angel!

In support of the **Soldier Recovery Unit (SRU)** and their families at Fort Carson, SAME Pikes Peak Post is partnering with the Fort Carson Army Community Service (ACS) to collect gifts in November and December for the children of the Fort Carson through our angel tree program.

We will be collecting gifts by the following age groups. **0-3 years; 4-6 years; 7-10 years; 11 – 14; and 15-18 years (see list on next page).** Please contact Cindy Lincicome (clincicome@betance.net) or Amy Umiamaka (aumiamaka@hbaa.com) to let us know what gender and age group you are "adopting" for this program. Lists will also be available by 10 November. The Pikes Peak Post is also accepting checks, and gift cards.

We will be collecting the **wrapped** gifts at the following locations. THANK YOU for your support!

Denver	Colorado Springs
Betance Enterprises, Inc. Office 7310 South Alton Way, Unit 6E Cindy Lincicome, F.SAME (303.319.0190) cindy@tliconstruction.net	HB&A Office 102 E Moreno Ave Colorado Springs Amy Umiamaka (719.473.7063 x 16) aumiamaka@hbaa.com

Coming Soon . . .

More Opportunities to Make a Difference!

Camp Alumni

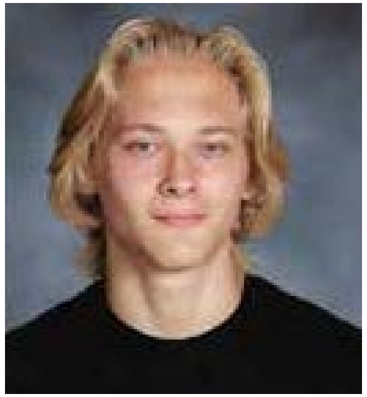
Jack Sewell

- **Camper 2014**
- **Camp Mentor and Loggie 4x = 2015-2019**

- Winner Camp Scholarship
- Louisiana State University
- LSU Petroleum Engineering GRAD! May 2020
- Enter MS program in Geology

- Sponsoring Post: Baton Rouge, LA

Camp Alumni

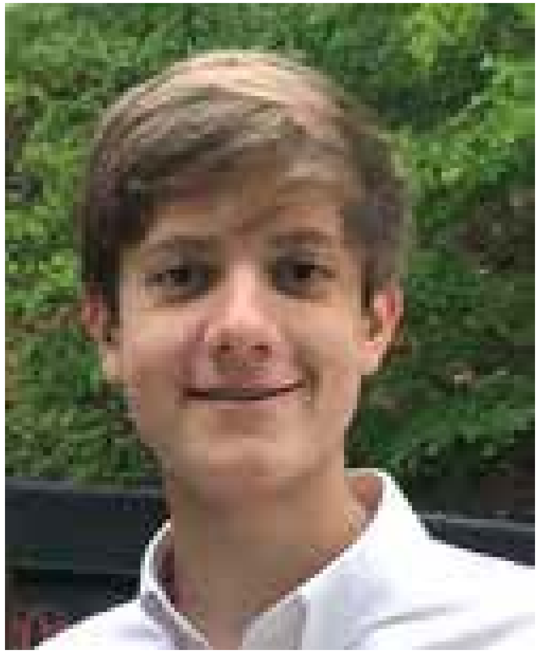


Alexander “Zander” Kitchen

- HS Sr
- Wrestling Tm Capt
- Band Drumline
- Math Team
- Top 1% of his class
- Interest – AFA and other service Academies

- Sponsoring Post: Lake Michigan

Camp Alumni



William Dyches

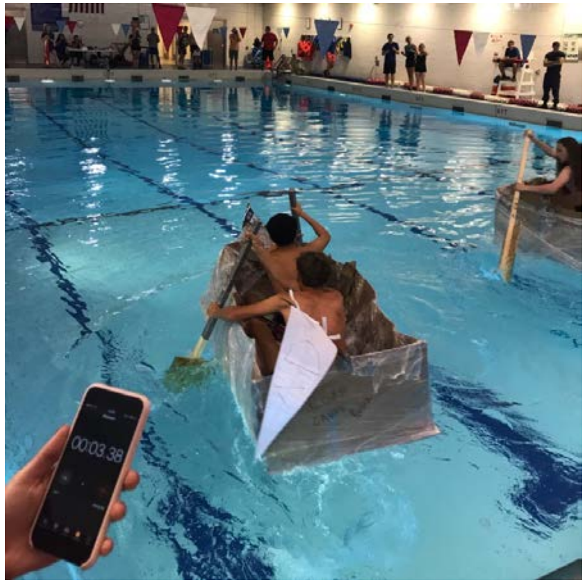
AFA Camp 2019

- HS Sr
- Varsity Basketball Center,
- Young Men’s Service League
- Philanthropy Chairman and Slating Committee
- Varsity Track
- Started / Leader HS STEM Program

- Sponsoring Post: Atlanta

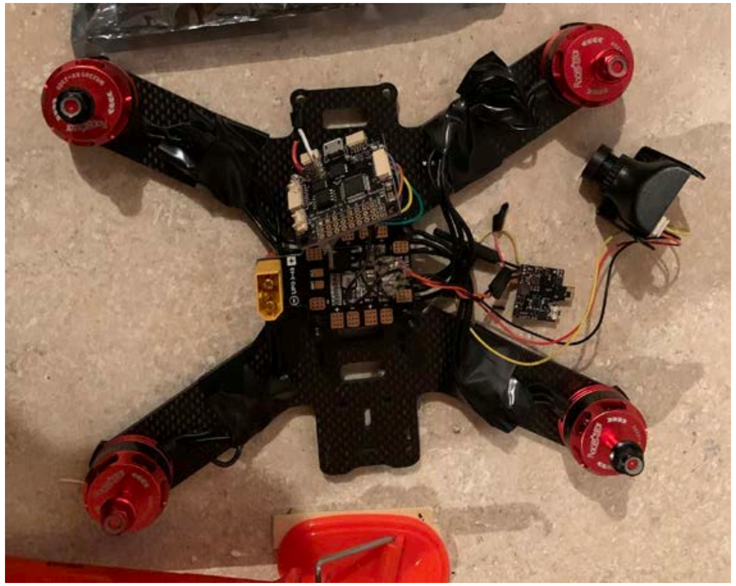
SAME Camp ‘19

My Experience

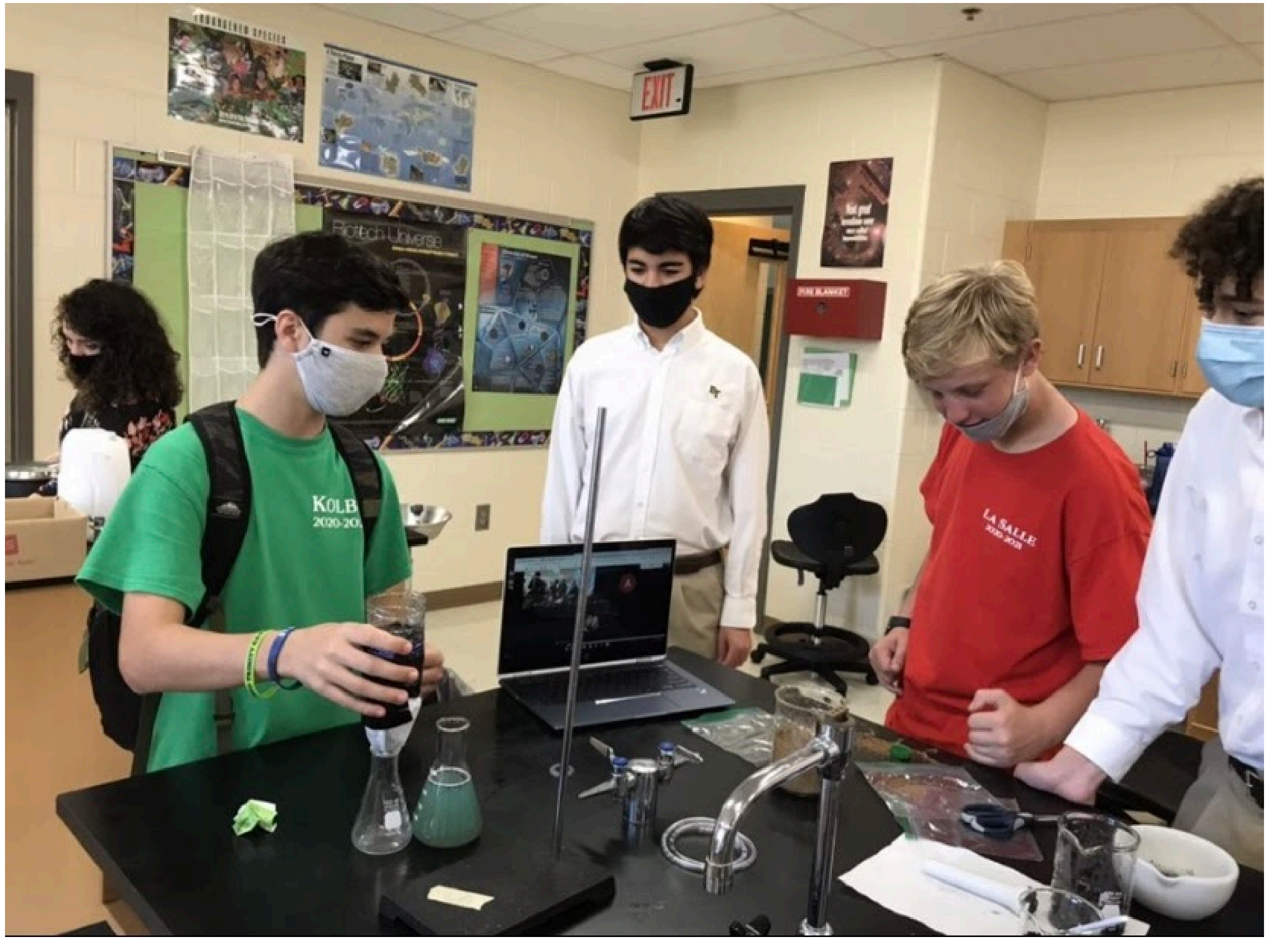


Where I am Now

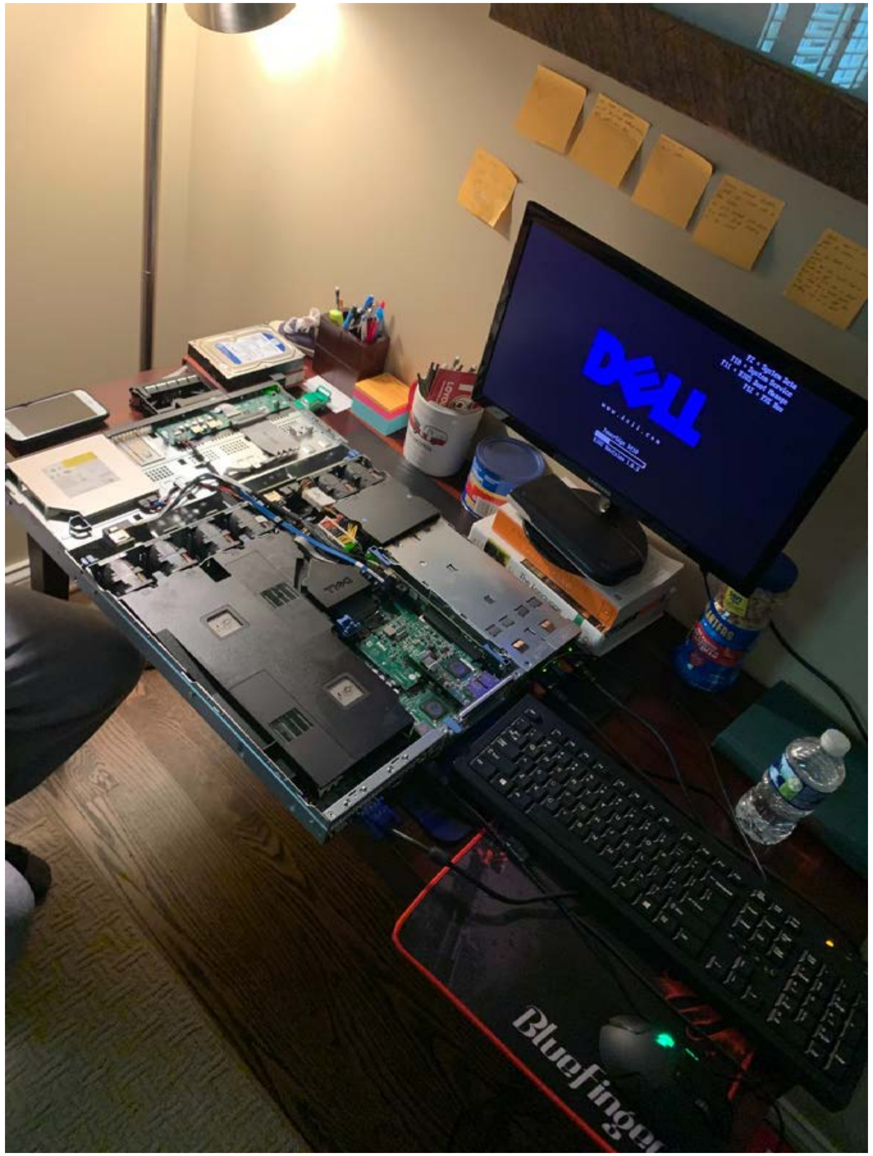
- Senior at Blessed Trinity Catholic High School
- Plan to study engineering in college
- Love doing random engineering projects



Engineering Club



- Electrical and Computer Engineering
- Contact Info:
  - wdyches21@btcatholic.org



William J. Beary, P.E.
GS-15 DAFC, NORAD and USNORTHCOM/J42
Chief, Engineering Division

More Situational Awareness for Industrial Control Systems (MOSAICS)

William J. Beary, CAPT USN (Ret), PE, F. SAME
Jeth A. Fogg, Lt Col USAF (Ret), Ph.D., PE, M. SAME

More Situational Awareness for Industrial Control Systems (MOSAICS)

- The Threat
- Joint Capability Technology Demonstration (JCTD)
- MOSAICS Description
- Current Status
- Stakeholders
- Question and Answer

Theater Security Challenges

Arctic Traffic

Resurgent Russia

Assertive China

Natural Disasters

Fiscal Constraints = Difficult Choices

Space & Cyber Security

North Korea

Iran

Networks

CBRN

The Threat

- Our Nation’s Critical Infrastructure is at risk both inside (Government owned) and outside the fence (Commercially owned)
  - 89% of US military installations lie within US States and Territories
  - 90% of Critical Infrastructure is privately owned
- Cyber Threats to Industrial Control Systems (ICS) are expanding
  - Per IBM: ICS Cyber attacks increased 2,000% in 2019!

The JCTD team effort is foundational to protecting critical infrastructure!

Non-Kinetic Threat

Timeline of Non-Kinetic Attacks on Critical Infrastructure

Chinese hackers target 23 U.S. gas pipeline companies collecting sensitive information

TELVENT

OASyS System files are collected

Havex watering hole-based ICS targeting

havex

The Dukes

F-Secure notes 7 years of cyber espionage

Cyber attack directed against Ukrainian transmission operator

WannaCry
CrashOverride
Petya-NotPetya
Nuclear 17…

INDUSTROYER

US Cert - Russian Targeting Energy & Critical Infrastructure

MOSAICS Technology Approach

2010 · 2011 · 2012 · 2013 · 2014 · 2015 · 2016 · 2017 · 2018 · 2019

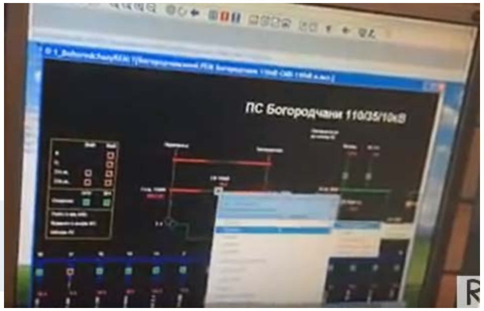
Stuxnet identified

Shamoon wiper destroys nearly 30,000 Saudi Aramco computers

أرامكو السعودية
Saudi Aramco

Energetic bear collects data from energy companies in U.S. and Europe

Cyber attack directed against utilities in Ukraine



THREATS ARE REAL AND EXPANDING

JCTD Program

RAPIDLY DELIVERING CAPABILITIES
JCTD
JOINT CAPABILITY TECHNOLOGY DEMONSTRATION

Created in 1995, the Advanced Concepts Technology Demonstration Program (precursor to JCTDs) emerged from the Packard Commission as a way to reduce cost and risk of entering full-scale acquisition

Mission

- **Address Combatant Command (CCMD) and Joint warfighting gaps through prototyping and demonstration of innovative and game-changing technologies**

Objectives

- **Demonstrate solutions within 2-4 years (from the identification of a warfighting gap)**
- **Deliver meaningful military utility and refine CONOPS / TTP**
- **Provide effective leave-behind capabilities when required**
- **Facilitate technology transition to acquisition programs**
- **Leverage open architectures to enhance interoperability and promote affordability**

Unique Project Structure

- **Oversight provided by an integrated management team of key stakeholders (CCMD OM, Service TM, Service XM)**
- **Dedicated funding to commence work in the year of selection**
- **Relief from some JCIDS requirements**
- **Opportunities for a truncated acquisition process (post JCTD)**

CONOPS – Concept of Operations, TTP – Tactics, Techniques, and Procedures
OM – Operational Manager, TM – Technical Manager, XM – Transition Manager
JCIDS – Joint Capabilities Integration and Development System

A long history of accelerating the transition of affordable, leap-ahead capabilities

MOSAICS
Operational Requirement

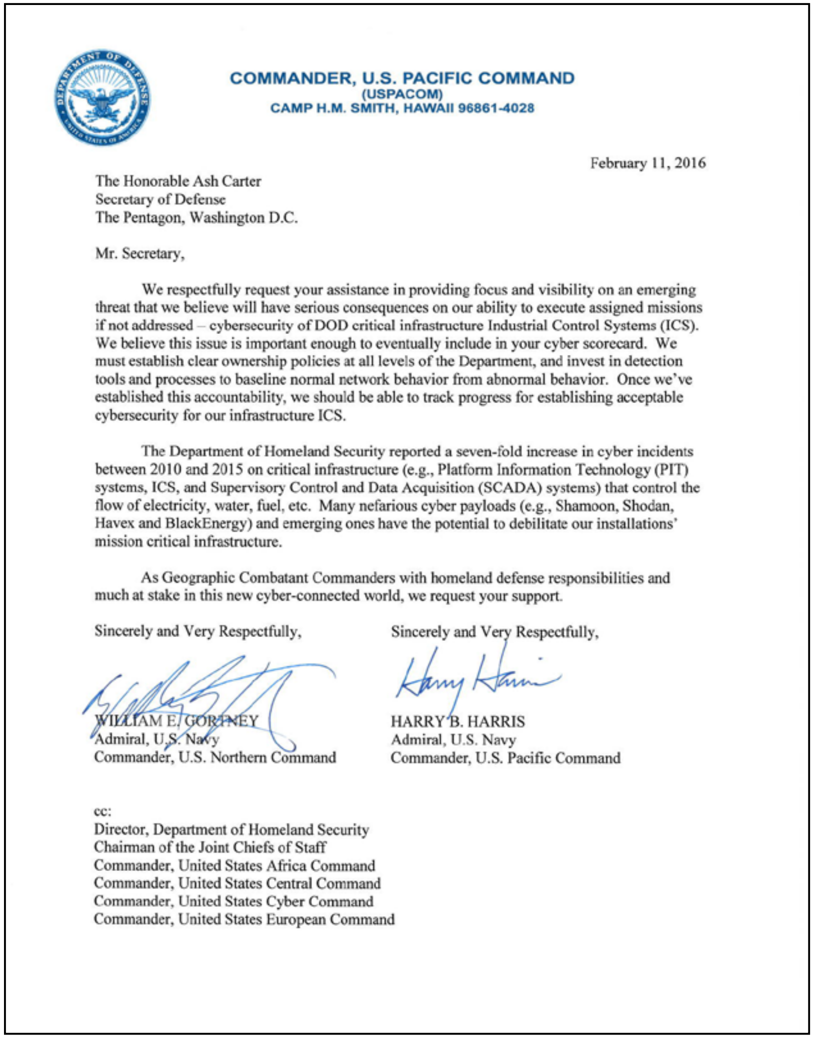
INDOPACOM/NORTHCOM
"8-star" Letter to SECDEF

"We respectfully request your assistance in providing focus and visibility on an emerging threat we believe will have serious consequences on our ability to execute assigned missions if not addressed – cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS)."

11 Feb 2016
Admiral William Gortney, USNORTHCOM
Admiral Harry Harris, USINDOPACOM

FY20-24 Integrated Priority Lists

- USCYBERCOM
- USEUCOM
- USNORTHCOM
- USINDOPACOM



COMMANDER, U.S. PACIFIC COMMAND
(USPACOM)
CAMP H.M. SMITH, HAWAII 96861-4028

February 11, 2016

The Honorable Ash Carter
Secretary of Defense
The Pentagon, Washington D.C.

Mr. Secretary,

We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS). We believe this issue is important enough to eventually include in your cyber scorecard. We must establish clear ownership policies at all levels of the Department, and invest in detection tools and processes to baseline normal network behavior from abnormal behavior. Once we've established this accountability, we should be able to track progress for establishing acceptable cybersecurity for our infrastructure ICS.

The Department of Homeland Security reported a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure (e.g., Platform Information Technology (PIT) systems, ICS, and Supervisory Control and Data Acquisition (SCADA) systems) that control the flow of electricity, water, fuel, etc. Many nefarious cyber payloads (e.g., Shamoon, Shodan, Havex and BlackEnergy) and emerging ones have the potential to debilitate our installations' mission critical infrastructure.

As Geographic Combatant Commanders with homeland defense responsibilities and much at stake in this new cyber-connected world, we request your support.

Sincerely and Very Respectfully,

WILLIAM E. GORTNEY
Admiral, U.S. Navy
Commander, U.S. Northern Command

Sincerely and Very Respectfully,

Harry Harris

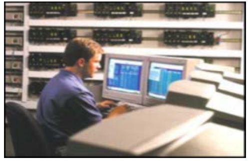
HARRY B. HARRIS
Admiral, U.S. Navy
Commander, U.S. Pacific Command

cc:
Director, Department of Homeland Security
Chairman of the Joint Chiefs of Staff
Commander, United States Africa Command
Commander, United States Central Command
Commander, United States Cyber Command
Commander, United States European Command

MOSAICS OV1

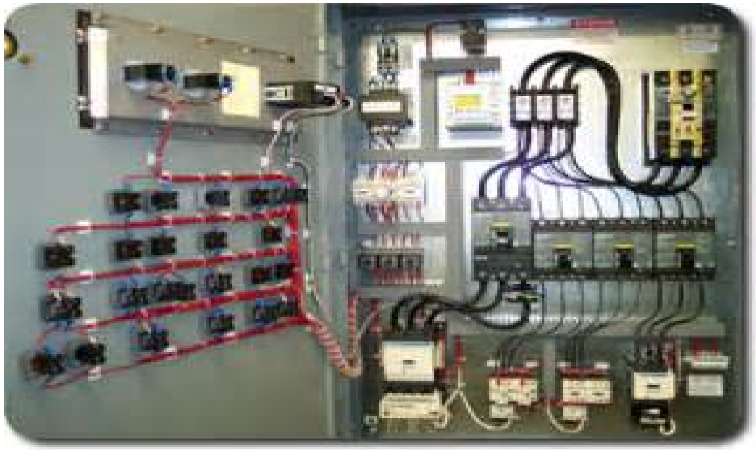
ICS Protection

ICS Operator



Cyber Defender

Industrial Control Systems (ICS)



Joint Warfighter Operations

Improved Situational Awareness and Speed to Decision

Detect → Analyze → Visualize → Decide → Mitigate → Recover → Share

Smart Integration of Automation

Higher Mission Assurance

Water

Electric Grid

Fuel

Building /Plant

Protect Critical Infrastructure Industrial Control Systems from Non-Kinetic Attacks

More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD)

MOSAICS is the first effort demonstrating the Initial Operating Capability for cyber defense of Critical Infrastructure

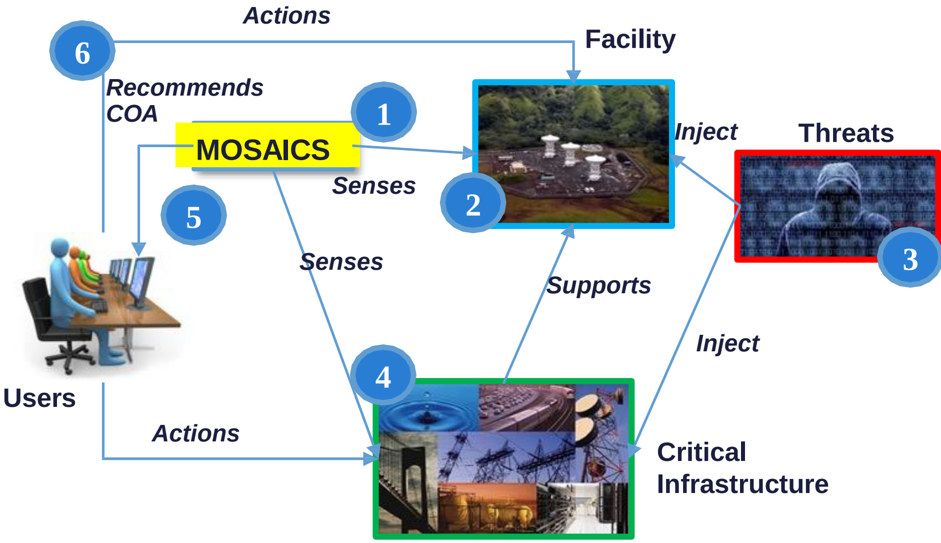
More Situational Awareness for Industrial Control Systems (MOSAICS) JCTD

Operational Objective: Resolve cybersecurity risks to Industrial Control Systems (ICS) supporting Department of Defense (DOD) critical infrastructure identified in the USINDOPACOM, USNORTHCOM, USEUCOM, and USCYBERCOM FY20-24 integrated priority lists (IPL). Baseline the ICS vulnerabilities and semi-autonomously identify, respond to, and recover from asymmetric attacks on critical infrastructure in mission-relevant timeframes.

Links to NDS, R&E Priorities, DOD Modernization Priorities: **NDS:** Resilient, survivable, federated networks and information ecosystems; **(R&E)** CYBER Strategy; **(DOD MP)** Cyber Security/Cyberspace

Project Description:

- **Applies automated tools to ICS to provide:**
  - o ICS Baseline and vulnerabilities
  - o Cyber & asymmetric Indications & Warnings (I&W)
  - o Cyber & asymmetric intrusion detection
  - o Semi-autonomously identify, respond to and recover from asymmetric attacks on critical infrastructure in mission-relevant timeframes (months to minutes)
- **Combatant Commands' (CCMD) and Military Services' Cyber Defenders and ICS operators will integrate MOSAICS alerts into analytic and collection workflows**



1. Establish baseline
2. Monitor for changes in equipment, network, or status
3. Threats inject malicious activity
4. Senses disruption, provide alerts
5. Provides available mitigation COA's
6. Users take action based on recommendations

MOSAICS Technology Focus

- **MOSAICS: Only DOD ICS Cyber Infrastructure Demonstration based on Integrated Adaptive Cyber Defense (IACD) technologies**
- **Start with Commercial Off-the-Shelf (COTS) technologies**
  - Minimize long-term costs and logistics support
- **Supplement with Government Off-the-Shelf (GOTS) to fill gaps**
  - The industrial control system space has unique requirements and only recently has become a focus of information security vendors
- **Foundation for application of Industrial Control Systems (ICS) security enhancements**
  - The platform and partnership foundation built by the MOSAICS JCTD has led to the prototyping of new technologies that monitor, analyze, and/or mitigate attacks
- **Expedite new technologies to enter the market**
  - Gap analysis and need to advance beyond the state-of-the-art have pushed the envelope to address the national need for ICS cybersecurity

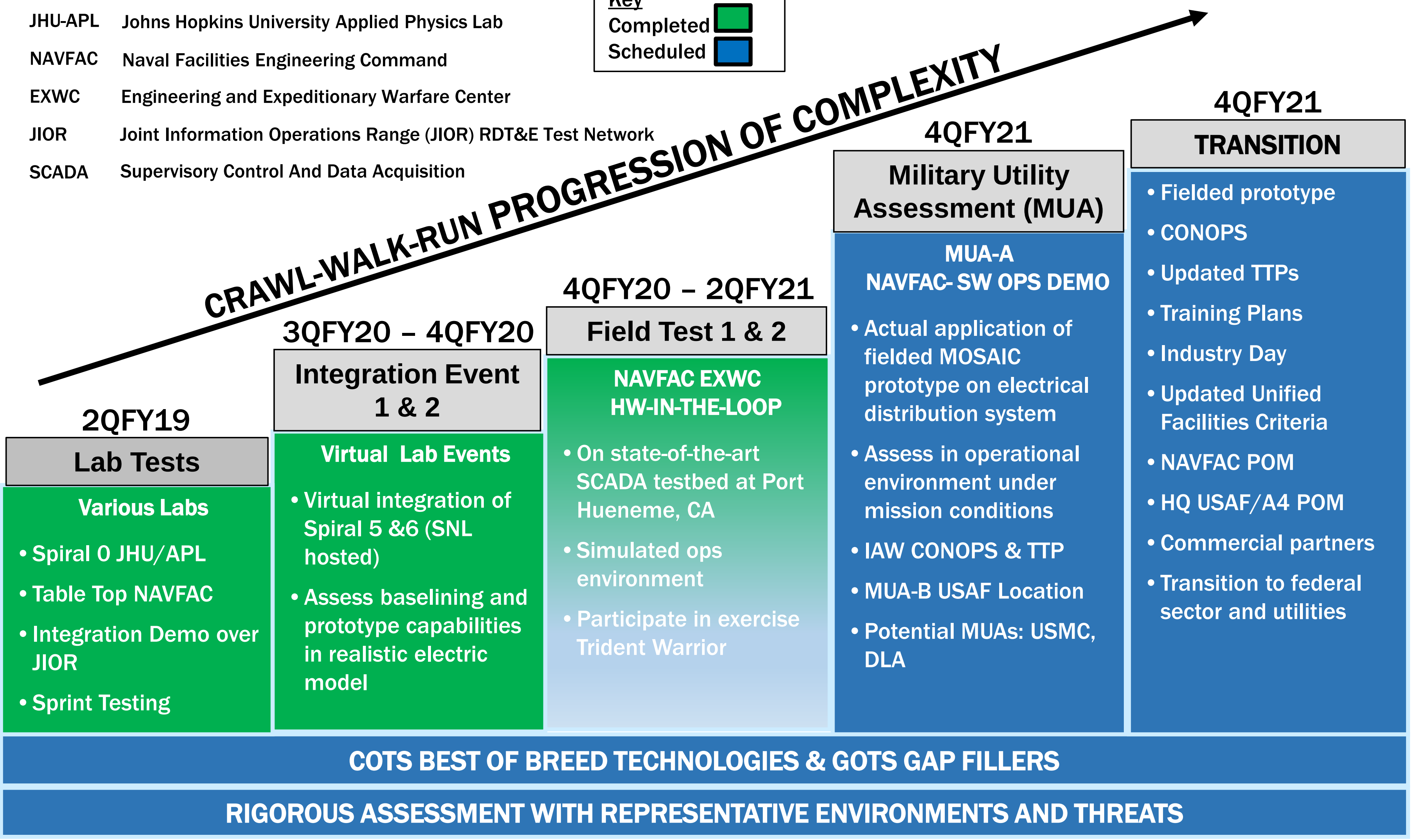
Systems Security Engineering / Risk Management Framework (RMF)

- As a system designed to monitor other systems for cyber attacks, the development of MOSAICS involves "building in" security features using the DOD's Risk Management Framework (RMF)
- The MOSAICS JCTD Systems Security Engineering (SSE/RMF) Team is supporting the following efforts:
  - An Interim Approval to Test (IATT) instance was initiated and is being maintained in the DOD's eMass system
  - The IATT Instance produced a set of security controls required to be implemented into the MOSAICS design
  - Conducts regular self assessments evaluating security control implementation
  - Collects and maintains all MOSAICS system artifacts, such as hardware software lists, topologies and ports/protocols and services
  - The completed IATT package will be submitted to the NAVFAC Functional Approving Authority for approval
- The MOSAICS IATT package serves as the foundation for all future Approvals to Operate and provides stakeholder assurances that MOSAICS integrated a security architecture within the design of MOSAICS

MOSAICS Technology Approach

JHU-APL	Johns Hopkins University Applied Physics Lab
NAVFAC	Naval Facilities Engineering Command
EXWC	Engineering and Expeditionary Warfare Center
JIOR	Joint Information Operations Range (JIOR) RDT&E Test Network
SCADA	Supervisory Control And Data Acquisition

Key
Completed 🟩
Scheduled 🟦



CRAWL-WALK-RUN PROGRESSION OF COMPLEXITY

2QFY19
Lab Tests

Various Labs

- Spiral 0 JHU/APL
- Table Top NAVFAC
- Integration Demo over JIOR
- Sprint Testing

3QFY20 – 4QFY20
Integration Event 1 & 2

Virtual Lab Events

- Virtual integration of Spiral 5 &6 (SNL hosted)
- Assess baselining and prototype capabilities in realistic electric model

4QFY20 – 2QFY21
Field Test 1 & 2

NAVFAC EXWC HW-IN-THE-LOOP

- On state-of-the-art SCADA testbed at Port Hueneme, CA
- Simulated ops environment
- Participate in exercise Trident Warrior

4QFY21
Military Utility Assessment (MUA)

MUA-A NAVFAC- SW OPS DEMO

- Actual application of fielded MOSAIC prototype on electrical distribution system
- Assess in operational environment under mission conditions
- IAW CONOPS & TTP
- MUA-B USAF Location
- Potential MUAs: USMC, DLA

4QFY21
TRANSITION

- Fielded prototype
- CONOPS
- Updated TTPs
- Training Plans
- Industry Day
- Updated Unified Facilities Criteria
- NAVFAC POM
- HQ USAF/A4 POM
- Commercial partners
- Transition to federal sector and utilities

COTS BEST OF BREED TECHNOLOGIES & GOTS GAP FILLERS

RIGOROUS ASSESSMENT WITH REPRESENTATIVE ENVIRONMENTS AND THREATS

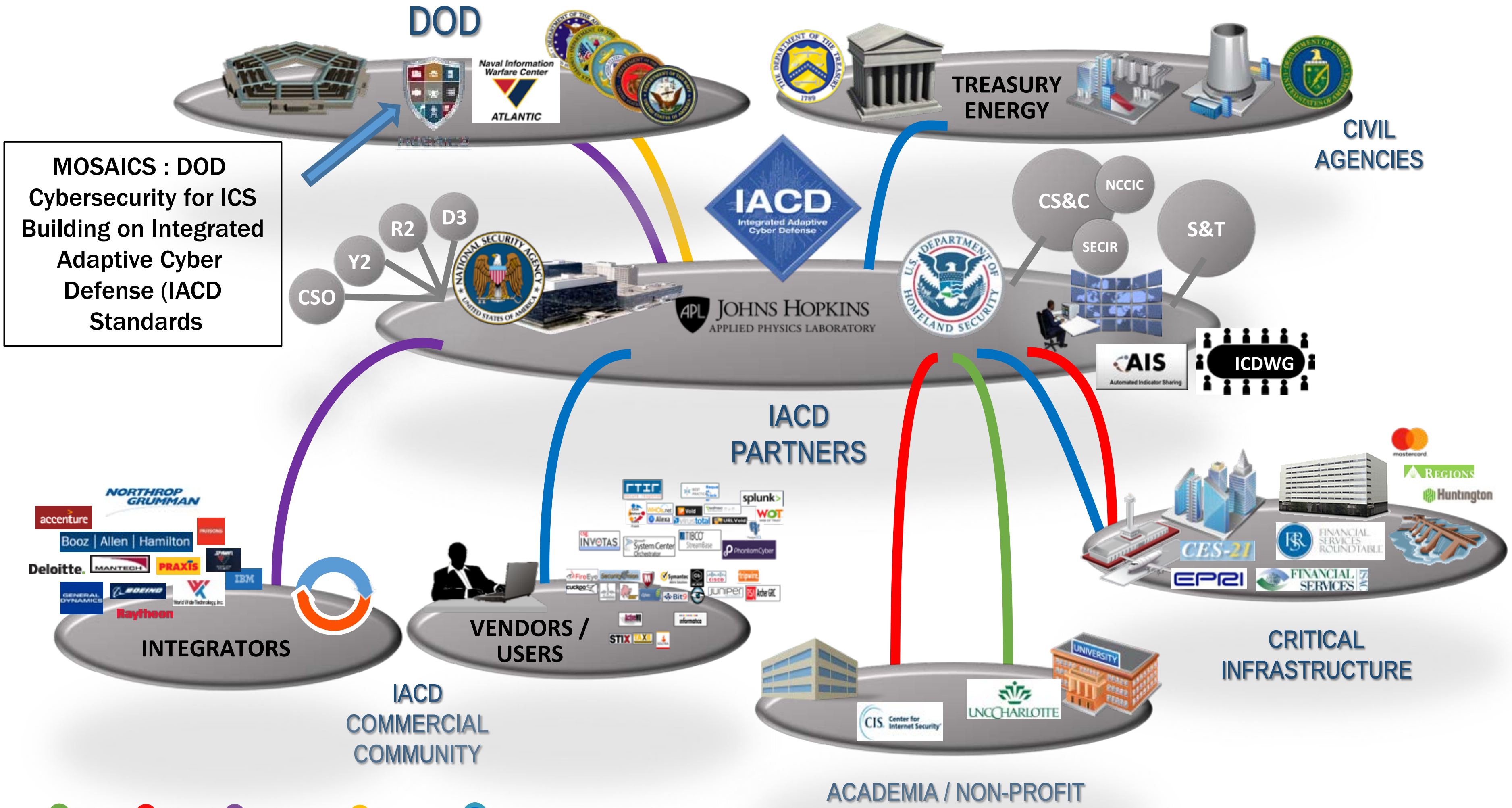
COTS Evaluation Efforts

- **COTS Survey**
  - A detailed feature categorization was used to document technology capabilities
  - More than 200 technologies were reviewed, which included company representative interface where possible
  - A process for the initial down-select weighting was developed
  - Gaps were identified in end point sensing, analytics, and visualization
  - GOTS technologies were identified from the labs to fill some gaps
  - A social media release was also issued to seek additional gap-filling technologies from the vendor community
- **Evaluation and down-select of COTS**
  - Each lab took a portion of the effort for the survey
  - Team evaluations performed using same criteria for consistency
  - Several hundred technologies narrowed to less than 50
  - The labs also parsed the effort for the hands-on testing for functional demo
  - DOE national labs, DOD, and NSA

MOSAICS JCTD Leverages IACD Standards

Integrated Adaptive Cyber Defense (IACD)

Breadth of Collaboration signals positive progress for Cyber Defense at Speed and Scale



MOSAICS : DOD Cybersecurity for ICS Building on Integrated Adaptive Cyber Defense (IACD Standards

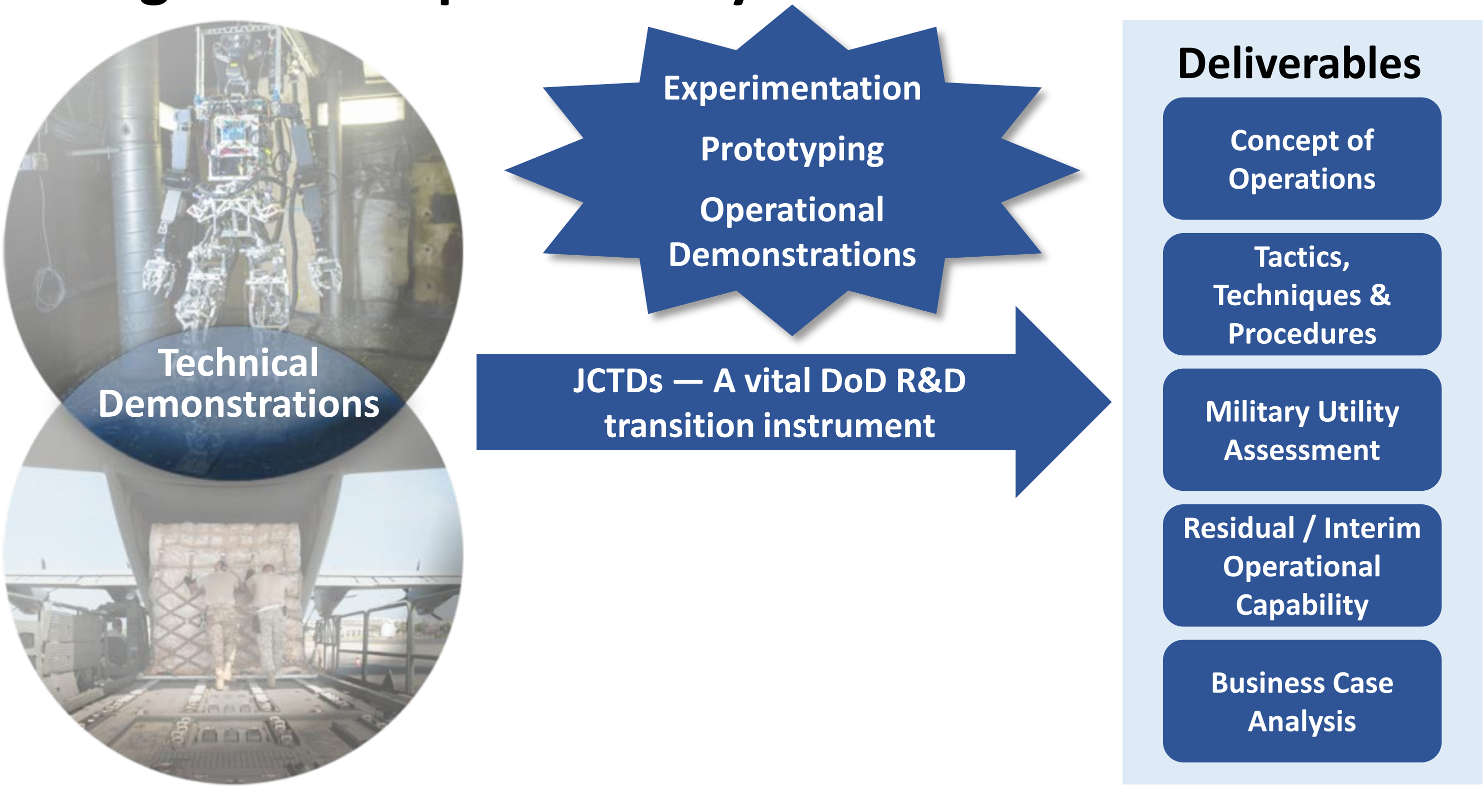
● FUNDING ● RESEARCH ● COLLABORATION ● TECH SUPPORT ● ADOPTION / PILOTS

Status

- ✓ Completed two major integration events
  - ✓ Re-planned and held virtually despite COVID19 impacts
- ✓ Technology Transition Agreement (TTA) completed pending NAVFAC signature
- ✓ First Operator Training Dry Run held week of 10 Aug 2020
- ✓ Virtual Field Test #1 (Tech Demo) held week of 24 Aug 2020
- ✓ Resolving Field Test #1 (Technical Demo) watch items
- ✓ Virtual Industry Days, 4-5 Nov 2020, 1st of 3
- Field Test #2 (Operational Demo) Port Heuneme, CA
  - Operator Training 18-22 Jan 2021
  - Dry Run 25-29 Jan 2021
  - Field Test #2 1-5 Feb 2021
- MUA San Diego CA Jul-Aug 2021

JCTDs Bridge to Acquisition

Provide opportunity for technical community to demonstrate technologies in an operationally relevant environment.



Technical Demonstrations

Experimentation

Prototyping

Operational Demonstrations

JCTDs — A vital DoD R&D transition instrument

Deliverables

- Concept of Operations
- Tactics, Techniques & Procedures
- Military Utility Assessment
- Residual / Interim Operational Capability
- Business Case Analysis

Provide Transition Opportunity Serving S&T/Warfighting Community

Reference – See Joint Capabilities Integration Development System (JCIDS) manual which defines role JCTDs play in accelerating acquisition.

MOSAICS Stakeholders

KEY: ✦ Providing Funds

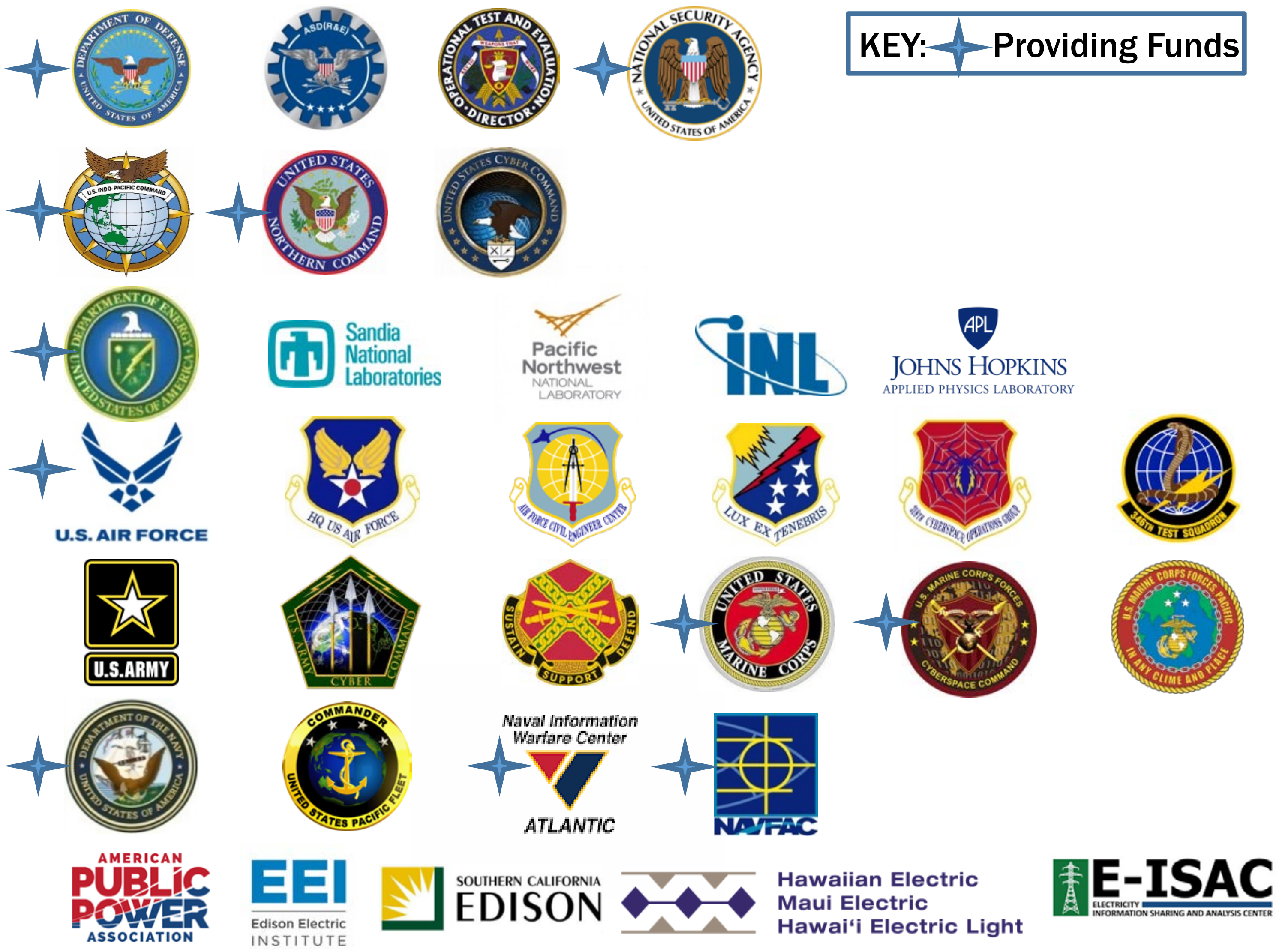
OSD & CSA

CCMDs

DOE, National Labs & UARC

Services

Industry



DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA
ASD(R&E)
OPERATIONAL TEST AND EVALUATION · DIRECTOR
NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA
U.S. INDO-PACIFIC COMMAND
UNITED STATES NORTHERN COMMAND
UNITED STATES CYBER COMMAND
DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA
Sandia National Laboratories
Pacific Northwest NATIONAL LABORATORY
INL
APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY
U.S. AIR FORCE
HQ US AIR FORCE
AIR FORCE CIVIL ENGINEER CENTER
LUX EX TENEBRIS
CYBERSPACE OPERATIONS GROUP
346th TEST SQUADRON
U.S.ARMY
U.S. ARMY CYBER COMMAND
SUSTAIN SUPPORT DEFEND
UNITED STATES MARINE CORPS
U.S. MARINE CORPS FORCES CYBERSPACE COMMAND
U.S. MARINE CORPS FORCES PACIFIC · IN ANY CLIME AND PLACE
DEPARTMENT OF THE NAVY · UNITED STATES OF AMERICA
COMMANDER UNITED STATES PACIFIC FLEET
Naval Information Warfare Center ATLANTIC
NAVFAC
AMERICAN PUBLIC POWER ASSOCIATION
EEI Edison Electric INSTITUTE
SOUTHERN CALIFORNIA EDISON
Hawaiian Electric
Maui Electric
Hawai'i Electric Light
E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Conclusion

- US Critical Infrastructure and force projection is at risk
- An ICS attack is a likely precursor to an adversary action in an attempt to pre-empt the dynamic sourcing of US military capability
- MOSAICS Mitigates the Risk demonstrating the IOC for cyber defense of DOD, Federal Government, and private sector critical infrastructure
- Even with the COVID delays the JCTD is on a path for success
- **The Nation needs this capability!**

More Situational Awareness for Industrial Control Systems (MOSAICS)

Questions?

"We Have the Watch"