More Situational Awareness for Industrial Control Systems (MOSAICS)

USINDOPACOM Operational Manager, Mr. Ross Roley
USNORTHCOM Operational Manager, Mr. Bill Beary
DOD Technical Manager, Mr. Rich Scalco, Naval Information Warfare Center Atlantic
DOE Technical Manager, Dr. Bill Waugaman, Sandia National Laboratories
Transition Manager, Mr. Man Nguyen, Naval Facilities and Engineering Command

Non-Kinetic Threat

Timeline of Non-Kinetic Attacks on Critical Infrastructure

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

2010

Stuxnet identified

2011

Shamoon wiper destroys nearly 30,000 Saudi Aramco computers

2012

OASyS System files are collected

Havex watering hole-based ICS targeting

2013

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

2014

F-Secure notes 7 years of cyber espionage

2015

Cyber attack directed against utilities in Ukraine

2016

Cyber attack directed against Ukrainian transmission operator

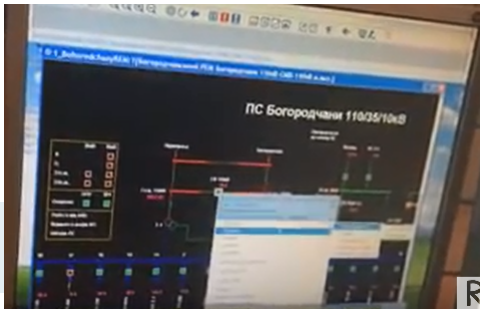
2017

WannaCry
CrashOverride
Petya-NotPetya
Nuclear 17…

2018

US Cert - Russian Targeting Energy & Critical Infrastructure

2019



THREATS ARE REAL AND EXPANDING

MOSAICS
Operational Requirement

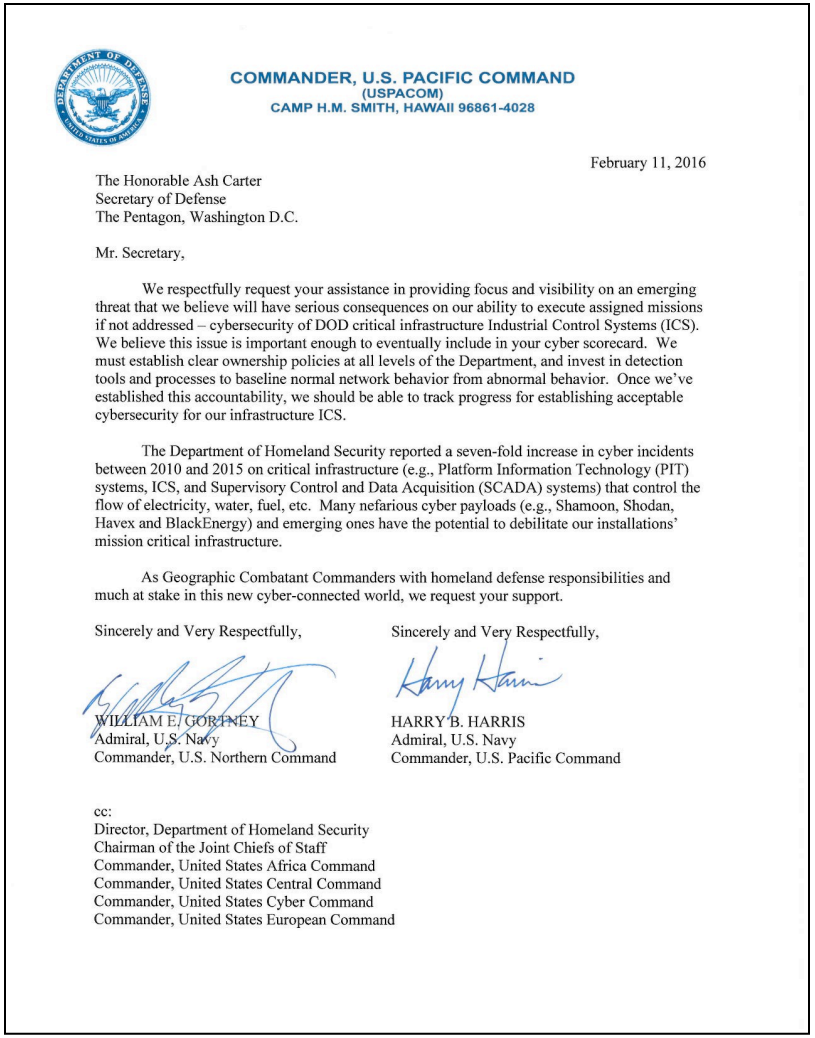
PACOM/NORTHCOM
"8-star" Letter to SECDEF

"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, USPACOM

FY20-24 Integrated Priority Lists

- USCYBERCOM
- USEUCOM
- USNORTHCOM
- USPACOM



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 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
Operational Problem Statement

Primary Focus Area: Information Operations and Analytics

Primary Operational Challenge: IOA 3 - analytic capability to provide cyber and asymmetric threat indications and warnings and intrusion detection, tracking, and defeat

Current Threat:

- Operational Problem:

  Adversaries have demonstrated non-kinetic means to disrupt critical warfighting infrastructure, denying our ability to project force. This threat was recently highlighted in a DHS technical alert detailing an ongoing Russian government cyber intrusion campaign targeting U.S government and commercial critical infrastructure. The need to mitigate such threats is prioritized in the National Security Strategy, National Defense Strategy, and the National Defense Authorization Act (2017) Section 1650. Currently, DOD lacks adequate cyber situational awareness and response capabilities to address this problem.

- Solution:

  MOSAICS will provide cyber vulnerability baselining, enhanced asymmetric threat indications and warnings, anomaly detection, and information sharing capabilities within an automation framework that enables real-time response actions to disrupt attacker kill chains, timely recovery to restore normal operations, and machine-to-machine sharing of threat indicators and mitigations to degrade adversary re-use of attacks.

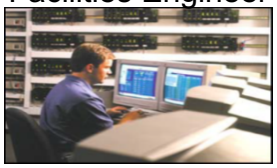
Prototype Model: Operational Prototype

Protect Task Critical Assets from Non-Kinetic Attacks

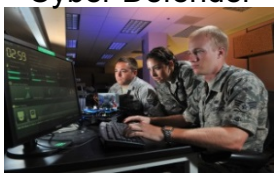
MOSAICS OV-1

ICS Protection

Facilities Engineer



Cyber Defender



Industrial Control Systems (ICS)

Joint Warfighter Operations

Operational Cyber Defense Capabilities

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

Smart Integration of Automation

Mission Assurance

Water

Electric Grid

Fuel

Building /Plant

Protect Critical Infrastructure Control Systems from Cyber Attacks

MOSAICS Description

What is it?

MOSAICS is an integration of COTS and GOTS technologies for enhanced situational awareness and defense of industrial control systems associated with task critical assets

What will project do?

Demonstrate the ability to baseline control system vulnerabilities and semi-autonomously identify, respond to, and recover from asymmetric attacks on critical infrastructure in mission-relevant timeframes

Operational value to the warfighter:

- Enhance understanding of risk to critical infrastructure and supported operational capabilities
- Detect control system threats faster – from months to minutes
- Improve situational awareness driving real-time decision aids to enable cyber defender response
- Disrupt adversary kill-chain in mission-relevant time
- Limit adversary re-use of attacks through enhanced sharing of indicators and mitigations
- Application of referenced open-system architecture across the Services

Example Prototype

elasticsearch

CISCO

kibana

NOZOMI NETWORKS

Microsoft System Center Configuration Manager

DEMISTO
A PALO ALTO NETWORKS® COMPANY

tenable®

CYNASH

McAfee

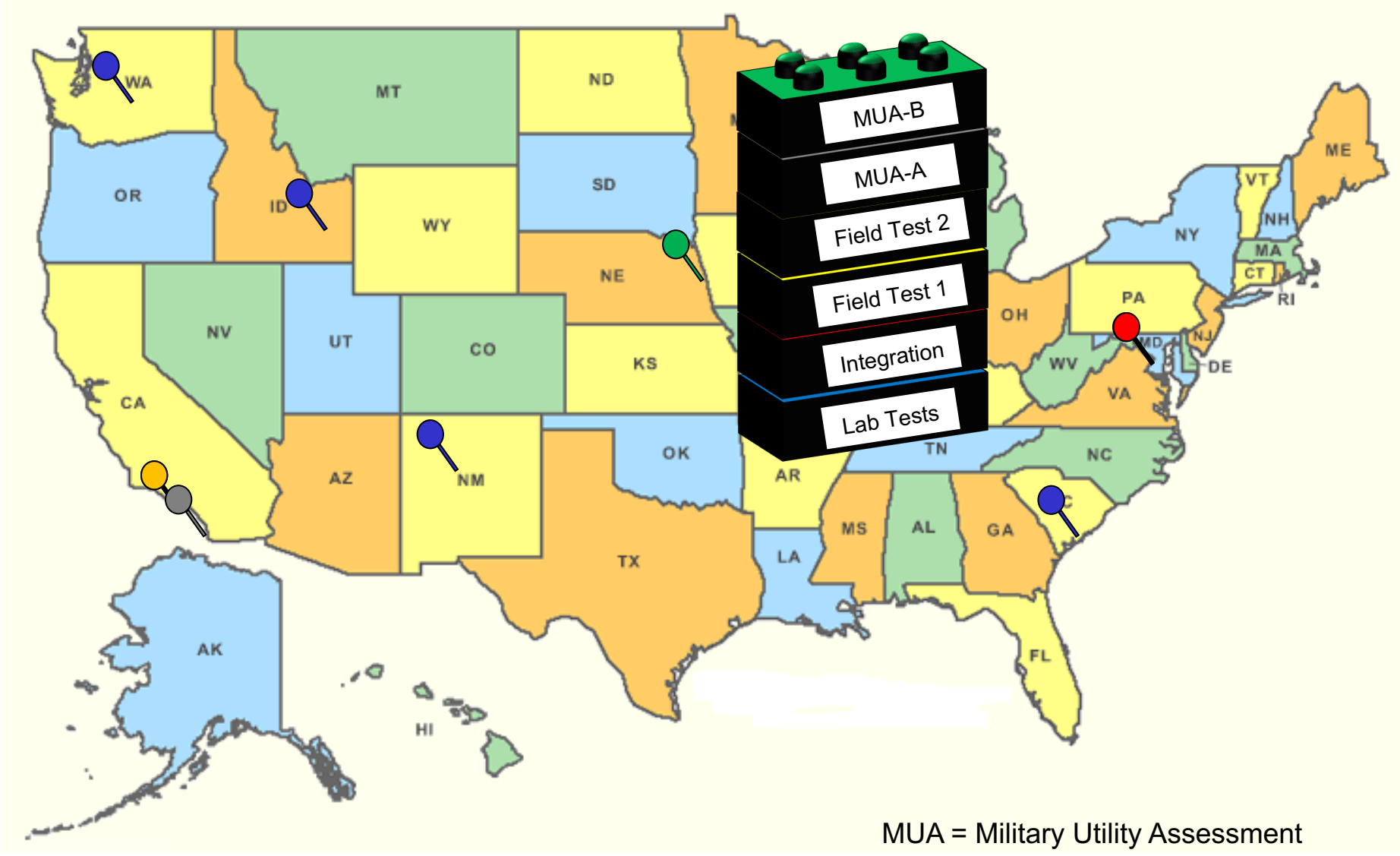
Technology Set Tailored to Site Needs

Field Test #1 Overview

- **Conducted by Air Force 47th Cyberspace Test Squadron**
  - Developmental Test Squadron focus on Offensive and Defensive Cyber Operations systems for the AF, Army, Navy, USCC, USSF
- **Run remotely from 24-28 August due to COVID-19**
  - Via the Sandia Research Network on SNL Heisenberg Lab servers
- **Five test cases executed, performed 250+ test runs**
- **Discovered 11 (Cat I-U) and 11 (Cat II-U) deficiencies**
  Cyber attack detection and alerts worked
  - Deficiencies primarily due to undelivered operator interface requirements
- **Results**
  - System significantly more mature than December 2019 test
  - More operationally representative evaluation than December 2019 test
    - real cyber-attack inputs, end to end evaluation, operator interface assessed
  - SNL range model (virtual) vs planned NAVFAC control system testbed environment (EXWC) increases operational live environment integration risk
    - FD#2 will be accomplished at EXWC In person to mitigate this risk

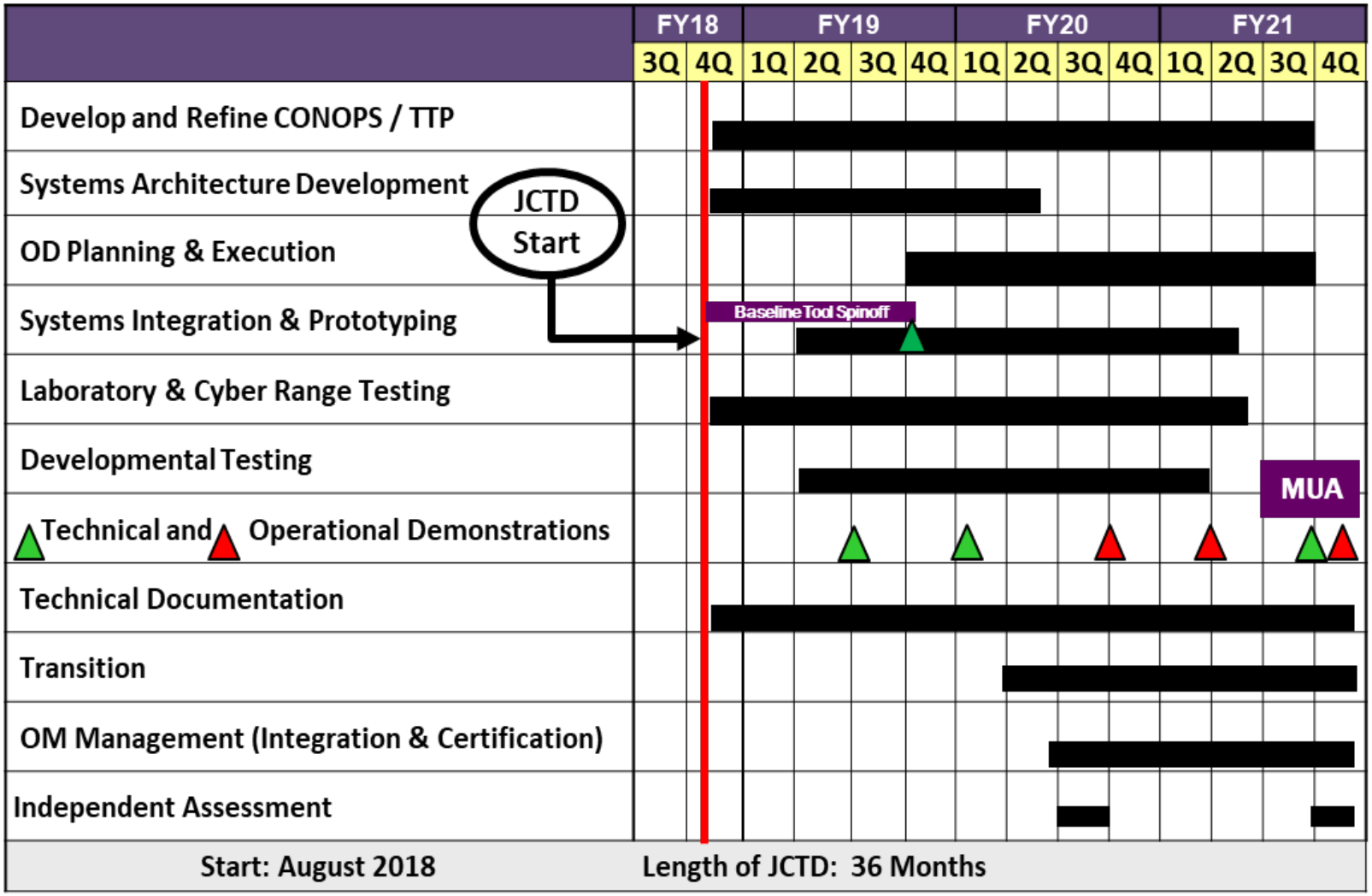
Substantial MOSAICS development progress

MOSAICS Test Concept



MUA = Military Utility Assessment

MOSAICS Schedule



MOSAICS is a Solid Value Proposition

IT/OT Perspective Security Orchestration, Automation & Response (SOAR)

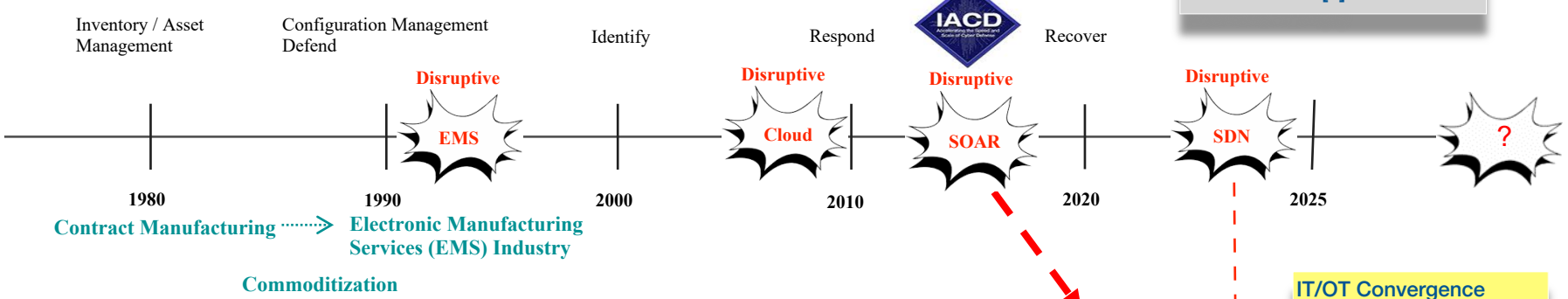
It has taken IT 50 years of investment, research, development, experience and commercial industry to "SOAR."
We are "seeding" an entire OT transformational industry to defend mission critical infrastructure in ~ 3 years with <$20M

BOTTOM LINE – We will accomplish in 3 years with $20M what has taken IT 50 years and $ Hundreds of Billions

IT Path to SOAR Near Real-time Solutions — 50 Years

Security Orchestration, Automation and Response (SOAR) IT Industry Segment Seeded by investments from DOD and DHS in partnership with JHU APL over 7+ years.

Global digital transformation market worth $3,294 Billion by 2025
22.7% CAGR [1]

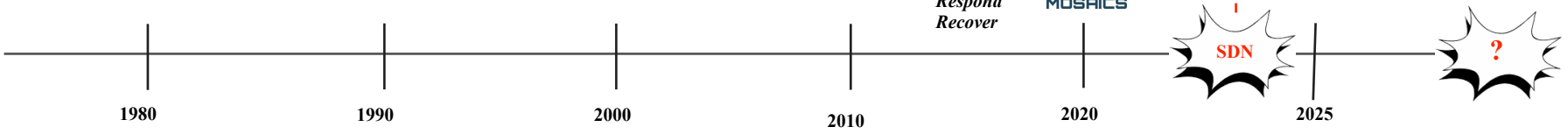


IT/OT Convergence
"Think Function & Effect"
Not Technology

OT Path to SOAR Near Real-time Solutions — 3 Years

Inventory
Asset Mgnt
Conf. Mgnt
Defend
Identify
Respond
Recover

MOSAICS



Global Critical Infrastructure Protection (CIP) market size projected to grow to $152.3 Billion by 2025
3.4% CAGR [2]

Slide Source – A. Scalco. CSU 2020
[1] Global News Wire, Meticulous Market Research LTD, June 10, 2020, https://www.globenewswire.com
[2] Global News Wire, Report Linker, May 7, 2020, https://www.globenewswire.com
CAGR - Compound Annual Growth Rate

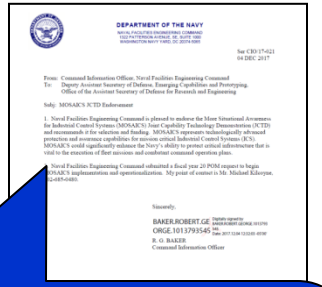
MOSAICS Transition Strategy

WHAT WILL BE TRANSITIONED?

- Control System Baselining Tool, Fielded Prototype, Updated ACI TTP, Automated Workflows, CONOPS, Integrators Open-System Architecture Design, Technology Assessment Data, Training plans, Lessons Learned, Guidance on System Interfaces, Transition Plans, Unified Facilities Criteria

WHERE WILL IT BE TRANSITIONED?

- Fielded prototype at Naval Air Station North Island, San Diego, CA
- NAVFAC will integrate MOSAICS at ten priority Navy installations
- Air Force AFCEC may integrate MOSAICS at Air Force installations
- Army IMCOM is assessing MOSAICS for baselining and implementation
- USCYBERCOM and ASD (EI&E) will publish updated ACI TTPs
- Industry transition via standards and regulatory organizations (i.e. APPA, EEI, NRECA, FERC, NERC, NERUC, NASEO, NIST)
- Industry transition via CRADAs


DEPARTMENT OF THE NAVY

"Naval Facilities Engineering Command submitted a fiscal year 20 POM request to begin MOSAICS implementation…"

Robert Baker
Command Information Officer

WHO WILL BE RESPONSIBLE FOR MAKING IT HAPPEN?

- NAVFAC EXWC with transition partners including ASD (EI&E), HAF/A4, AFCEC, IMCOM and USCYBERCOM

WHEN WILL THE TRANSITION OCCUR?

- Spiral spinoffs will transition incrementally as technologies mature, beginning on completion of phase one

WHAT ARE THE EXPECTED COSTS OF TRANSITION AND FUNDING SOURCES?

- Navy - $25M over the FYDP (NAVFAC included in FY20 POM specifically for MOSAICS)

Industry Day #1
4-5 November 2020

- **Intent it to start a conversation with industry to:**
  1. Share MOSAICS requirements, playbooks, concepts, and lessons learned
  2. Encourage public-private and private-private collaboration and teaming
  3. Ultimately establish a commercial industry of MOSAICs-like capabilities
- **Agenda is a combination of MOSAICS and vendor presentations**
  - First session establishes the DOD demand signal and business case
  - 22 vendor presentations in 6 deep dive sessions
    - Security automation and orchestration
    - Sensors
    - Decision support and visualization
    - Data and forensics
    - Protection
    - Miscellaneous
  - Final session is an open discussion on how to achieve the goals above
- **First of 3 planned MOSAICS Industry Days**
  - 2nd will be 14-16 Jun 2021 in Austin, TX in conjunction with TechConnect World
  - 3rd will be Fall/Winter of 21/22 on the east coast TBD

MOSAICS Stakeholders

OSD & CSA

CCMDs

National Labs & UARC

Air Force

Army

Navy

Industry

Back-Ups
Additional

MOSAICS
Comparison of Related Projects

→ J-BASICS →

MOSAICS

	Microgrids	CONOPS/TTP	Operational Cyber Defense
Mission Assurance	✓	✓	✓
Infrastructure	✓		
Software			✓
CONOPS/TTPs		✓	✓
Leave Behind	✓		✓
Automation			✓
Sensing			✓
Orchestration			✓
Detection		✓	✓
Analysis			✓
Visualization			✓
Decision Support			✓
Mitigation		✓	✓
Recovery		✓	✓
Info Sharing			✓

MOSAICS Builds Upon Past Successes

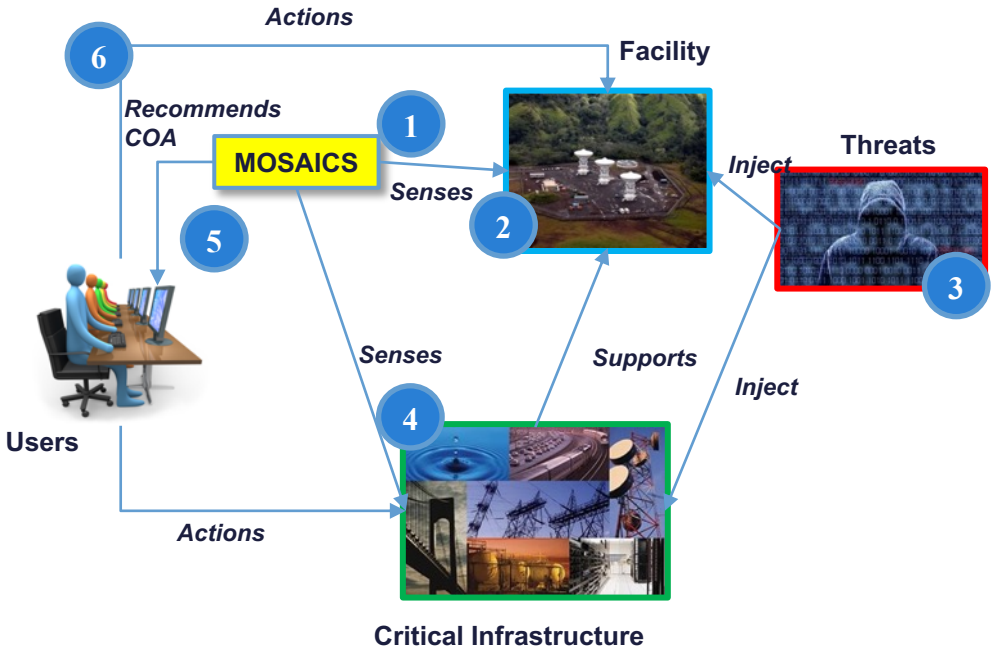
MOSAICS CONOPS

Purpose: Describe how situational awareness capabilities for ISC may be employed to

- Provide cyber and asymmetric threat I&W and intrusion detection, tracking, and defeat
- Increase dissemination and data sharing

Includes:

- Warfighting gaps addressed and expected operational outcomes;
- facility descriptions and operations;
- administrative and operational organization;
- threat actors ,vectors and TTPs;
- scenarios;
- overview of core capabilities;
- and plans to address DOTMLPF



1. Establish baseline
2. Monitor for changes in equipment, network, or status
3. Threats inject malicious activity
4. MOSAICS senses the disruption, provide alerts
5. MOSAICS provides available COA
6. Users take action based on recommendations

Structured Spiral Development

*Structured Technical Management using Spiral Development Methodology and Identified EPICS and Tasks are underway:

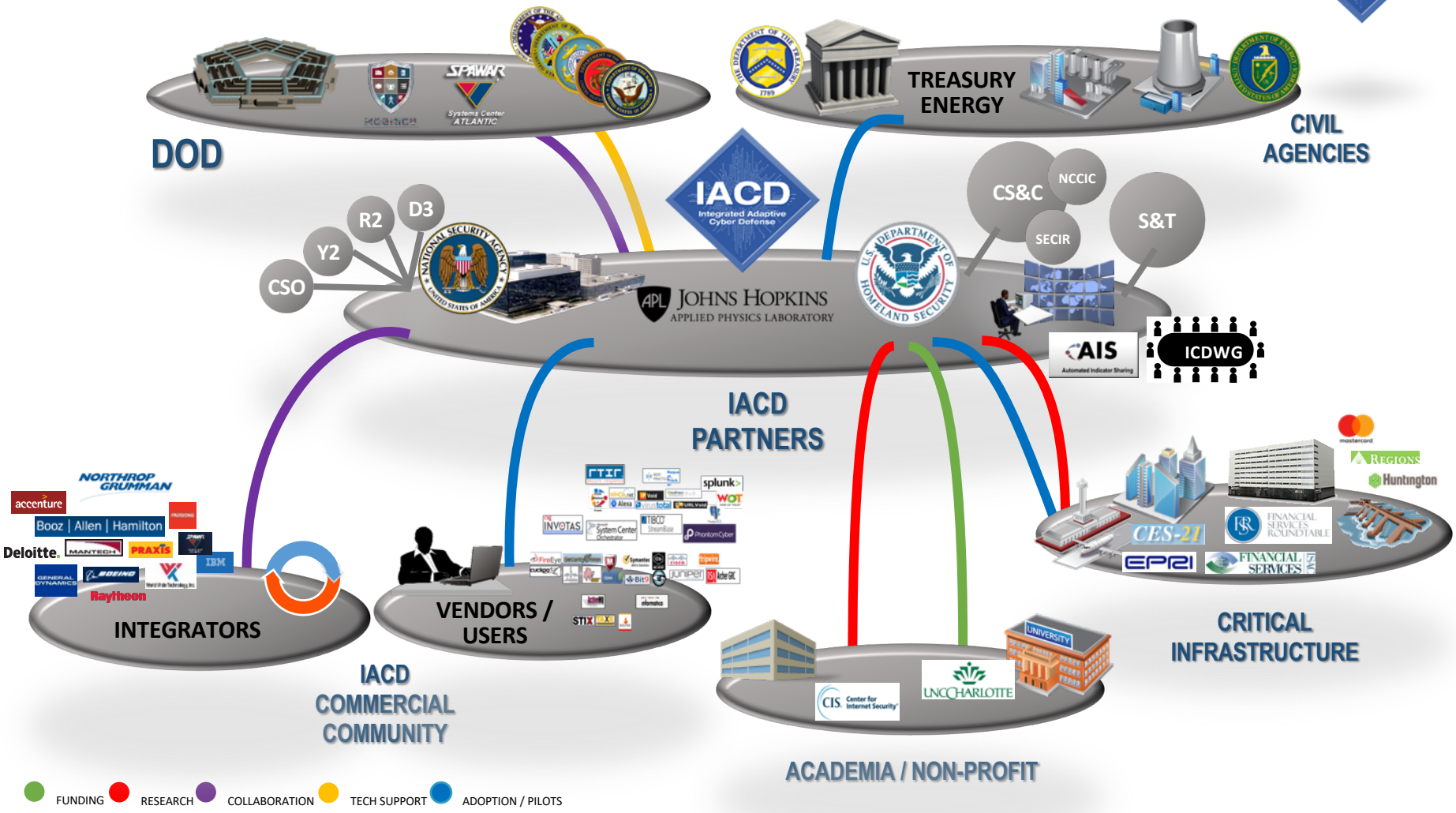
Number	Epic/Chapter(s)
1	Operational Requirement Development
1.1	CONOP Vision
1.2	Context Diagram
2	GOTS/COTS Survey
2.1	GOTS/COTS Quantitative Tool Selection
3	Technical Requirement Development
4	Range Demonstration/Event Connectivity
5	Architecture
6	Data Availability
7	Site Survey Characterization
8	TM Risk Management Framework (RMF) Conduit to Transition Management (XM)

Functional Requirements

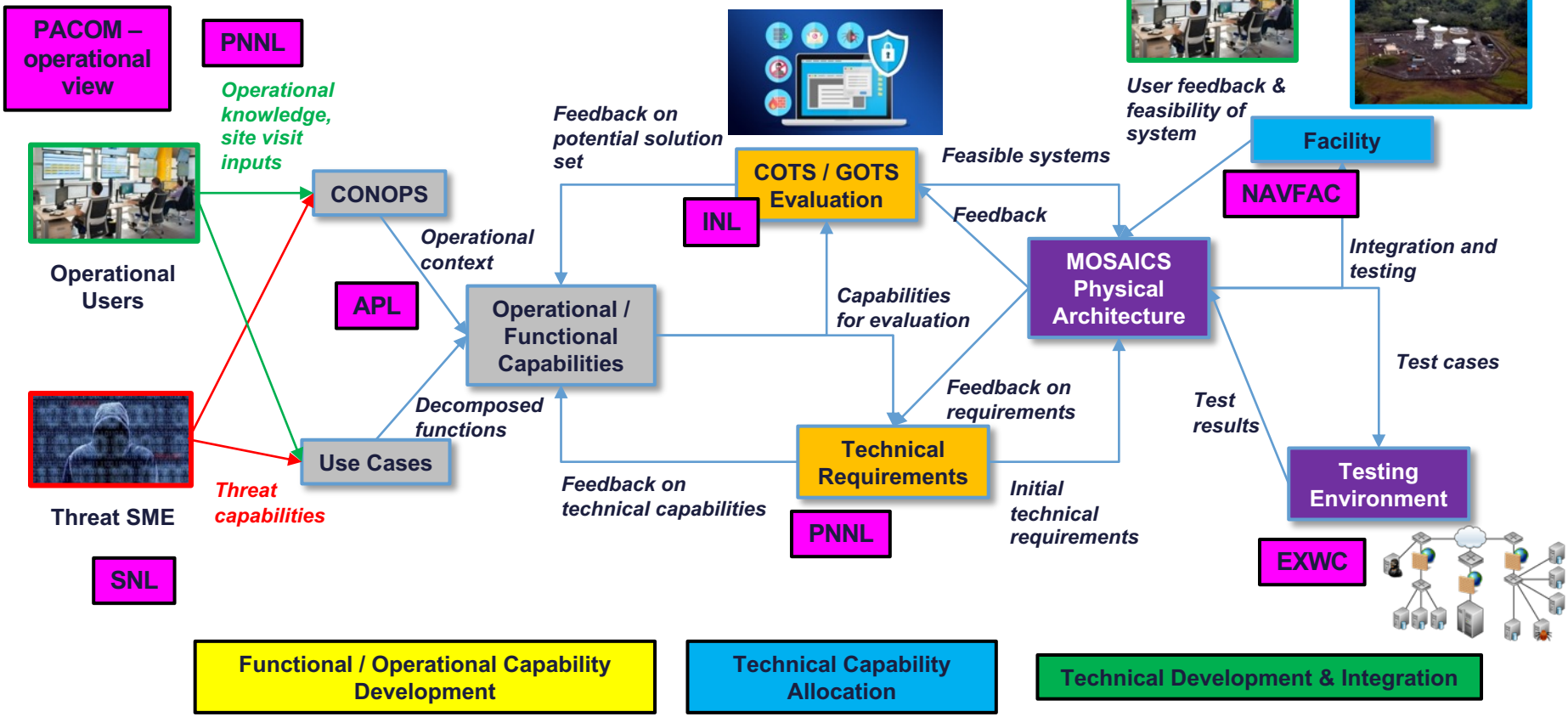
Identify → Protect → Detect → Analyze → Visualize → Decide → Mitigate → Recover → Share

F1.0 Identify System Components	F2.0 Protect from Threats	F3.0 Monitor / Detect threats	F4.0 Analyze detected events	F5.0 Visualize status	F6.0 Decide on COA	F7.0 Perform mitigation actions	F8.0 Perform recovery actions	F9.0 Share data
F1.1.1 Inventory physical devices	F2.1.1 Protect data at-rest	F3.1 Monitor facility status	F4.1 Profile networks and systems	F5.1 Collect system status	F6.1 Generate available COA	F7.1 Select mitigation technique	F8.1 Determine desired end state for recovery	F9.1 Select data to share
F1.1.2 Inventory software components	F2.1.2 Protect data in-transit	F3.2 Monitor critical infrastructure status	F4.2 Compare against normal behaviors	F5.2.1 Display top-level view of facility capability	F6.2 Determine automated COAs	F7.2 Select equipment / node to apply mitigation	F8.2 Determine recovery timeframe	F9.2 Collect data
F1.1.3 Map communication and data flows	F2.2 Manage facility ICS assets	F.3.3.1 Detect changes from baseline configuration	F4.3.1 Perform system analysis	F5.2.2 Display affected network elements	F6.3 Display COA to user	F7.3.1 Protect / harden	F8.3 Consider list of recovery COA	F9.3 Receive data from external sources
F1.2 Categorize system components based on criticality and vulnerability	F2.3 Establish operational availability goals for ICS data capacity	F.3.3.2 Monitor system components	F4.3.2 Perform malware analysis	F5.2.3 Display affected devices	F6.4 Consider facility priorities	F7.3.2 Diversify	F8.4 Select recovery COA	F9.4 Store data
F1.3.1 Manage credential access	F2.4 Protect against ICS data leaks	F.3.3.3 Detect malware	F4.3.3 Perform network analysis	F5.4 Display identity of event	F6.5 Consider threat severity	F7.3.3 Segment	F8.5 Preserve data for forensic analysis	F9.5 Set access permissions
F1.3.2 Manage physical access	F2.5 Protect communications and control networks	F.3.3.4 Detect anomalous behavior	F4.4 Categorize event	F5.5.1 Display functional impact	F6.6 Consider CI availability	F7.3.4 Stop	F8.5.1 Restart	F9.6 Verify identify / access from requester
F1.3.3 Manage remote access	F2.6 Perform integrity checks for software, hardware, firmware information integrity	F.3.3.5 Detect rule/policy violations	F4.5 Perform event correlation	F5.5.2 Display information impact	F6.7 Consider mission priorities	F7.3.5 Restart	F8.5.2 Reinitialize	F9.7 Enable / deny access to data
F1.3.4 Manage access and authorization	F2.7.1 Develop a system baseline	F3.4.1 Monitor state of physical barriers	F4.6 Record events	F5.6 Receive operator acknowledgement		F7.3.6 Switch to manual control	F8.5.3 Reset permissions / access	F9.8 Send data
F1.3.5 Manage network integrity	F2.7.2 Maintain system baseline					F7.4 Observe system reaction to mitigation actions	F8.5.4 Replace	
F1.4 Utilize identity credentials in facility operations	F2.7.3 Implement a configuration control process to update system inventory						F8.5.5 Reconnect	
F1.5 Authenticate components	F2.8 Test recovery and protection systems and plans						F8.5.6 Test operation of system component	
	F2.9 Maintain ICS protection / monitoring systems						F8.7 Observe recovery progress	
	F2.10 Perform routine maintenance on ICS components (local or remote)							
	F2.11 Maintain audit logs for ICS protection / monitoring systems							
	F2.12 Protect against cyber threats							

IACD: *Breadth of Collaboration* signals positive progress for Cyber Defense at Speed and Scale.



MOSAICS Products



MOSAICS
Points of Contact

Partner	Senior Point of Contact (others key contacts)
688th Cyberspace Wing	Mr. Mike Kretzer (Rob Kaufman)
AFCEC	Col Tim Dodge
ARCYBER	Mr. Ron Pontius
ASD(A) C3CB	Mr. John Garstka (John Choi)
ASD(EI&E)	DASD Lisa Jung (Daryl Haegley)
COMPACFLT	Mr. Bob Stephenson (LT Nick Ward)
DOE	Mr. Joe Hagerman
DOT&E	Mr. Steve Gates
HAF/A4	Mr. Ed Oshiba
IMCOM/G4	Mr. Greg Kuhr
NAVFAC	Mr. Rob Baker
Southern Cal Edison	Mr. Glenn Haddox (Joy Weed)
SSC LANT	Mr. Rich Scalco
USCYBERCOM	RADM Ross Myers (Bob Leverton)
USNORTHCOM	Brig Gen Stan Sheley
USPACOM	Dr. George Ka'iliwai
USTRANSCOM	TBD (Marty Ledington, Aaron Harris)
10th Fleet	TBD