



Forging a Future Fight: Shaping Cyber Phase 0

Colonel Adolph “Rocko” Rodriguez
Acting Deputy Principal Cyber Advisor
Office of the DAF Principal Cyber Advisor
29 August 2022



WHY ARE WE HERE?



THE DAF HAS DOCUMENTED EVIDENCE OF CRITICAL VULNERABILITIES TO INFORMATION, WEAPON, AND CONTROL SYSTEMS BEING DIRECTLY TARGETED BY OUR ADVERSARIES

FOUNDATIONS	PACAF TECH DEBT & COST		WHAT TFSS IS
Strategic Cybersecurity Program <i>Our adversaries are imposing cost on DAF <u>weapon systems</u> via cyber intrusions of weapon support systems and interdependencies (multi-billion) dollar investments</i>	Wide Area Network (AFINC) <i>PACAF core network devices that are end-of-life / end-of-service, with no failover, and unmitigated vulnerabilities</i>	\$10.5M	- Tailored to PACAF only - Cybersecurity & Cyber Defense Plan (CS&CD) for Information, Weapon, and Control systems - Defensive Countercyber capability for contested, degraded, and denied operating environments
	Base Area Network (CMAC) <i>Base-by-base modernization of wired and wireless networks</i>	\$200.0M	
	Physical Base Infrastructure (AFWP) <i>Unfunded cyber infrastructure requirements across PACAF critical to combat operations</i>	\$22.9M	
	AFNET Enterprise Core Services (CSCS) <i>Backend network management including authentication, patch management, scanning, and services for disconnected ops</i>	\$6.0M	
	End User Devices <i>#FixOurComputers</i>	\$43.4M	
	SIPR Components <i>Key devices for securing and operating SIPR</i>	\$6.6M	
NDA 1650 Control Systems Report <i>NDA Sec. 1650 highlighted <u>Critical Infrastructure/Control Systems</u> vulnerabilities in the sum of \$1.3B</i>	Cloud One IL-5 and IL-6 <i>Cloud services for information reaching CUI, National Security Systems, and Classified SECRET levels</i>	\$5.0M	WHAT TFSS IS <u>NOT</u> - Enterprise costed solution or Tech Debt - Steady state environment - DAF Data Fabric - Defense of enterprise-enabling solutions geographically separated from PACAF - Spectrum Management
DAF Crypto Modernization Action Group <i><u>Crypto Modernization</u> 1 & 2 effort is a \$10B delta for the DAF</i>			

LOGICAL, PRACTICAL SOLUTIONS—COORDINATED ACROSS STAKEHOLDERS—TO ENABLE COMBAT OPERATIONS!



FIVE FIGHTS
(AT RISK)

FIGHT FOR SPACE SUPERIORITY

- Cyber-enabled Space Architecture reachable by the adversary

FIGHT TO GET INTO THEATER

- Deficient SA of cyber terrain limits speed to counter cyber

FIGHT TO GET AIRBORNE

- Outdated cyber infrastructure cannot support Agile bases

FIGHT FOR AIR SUPERIORITY

- ABMS / JADC2 untenable in PACAF due to cyber infrastructure limitations

FIGHT TO REPEL THE INVASION

- C2 of fires dependent on vulnerable short- and long-haul cyber circuits



OV-1 CURRENT SITUATION

Lines of Effort

Data Strategy

IWN

TDC

SR Leader SA

Cyber C2

Sensor Implementation

Critical Enablers



Critical Enablers



Critical Enablers



Critical Enablers



Lines of Effort
(Enabling)

Data Strategy

Enable data-driven cyber SA for PACAF leadership & cyber C2 for operators

Integrated Warfighting Network (IWN)

Deliver solutions for resilient PACAF cyber architecture

Theater Deployable Comms (TDC)

Deliver defensible TDC construct for providing resilient warfighter comms

Lines of Effort
(CS&CD)

Senior Leader SA

Provide PACAF leadership real-time cyber status of key systems

Cyber Ops C2

Aligned and cohesive C2 across DODIN and DCO ops

Sensor Implementation

Design sensing solution aligned to "1-N" of PACAF critical assets



INFORMATION SYSTEMS

Information Technology backbone for computers, communications and C2



WEAPON SYSTEMS

Cyber-enabled Mission Design Series spanning Air and Space core functions



CONTROL SYSTEMS

Cyber-enabled operational technology critical to Air and Space power generation

Sensors

Deployed across the network reporting status and alerts.

Data Transport

Reliability and resiliency dependent on geolocation.

Data

Centrally managed in ELICSAR BDP, accessible world-wide.

Cyber Ops C2

Disparate Defensive Cyber Forces unaligned to Air Operations.

Senior Leader SA

Limited to visibility by Senior Cyber Leaders. Disconnected to DAF.

Sensors

Nascent, not standardized.

Data Transport

Does not exist.

Data

Does not exist or is siloed, on-prem, and is inaccessible.

Cyber Ops C2

Limited to Mission Defense Teams below the threshold of IOC.

Senior Leader SA

Does not exist.

Sensors

Do not exist.

Data Transport

Does not exist.

Data

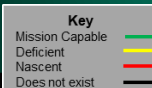
Does not exist or is siloed, on-prem, and is inaccessible.

Cyber Ops C2

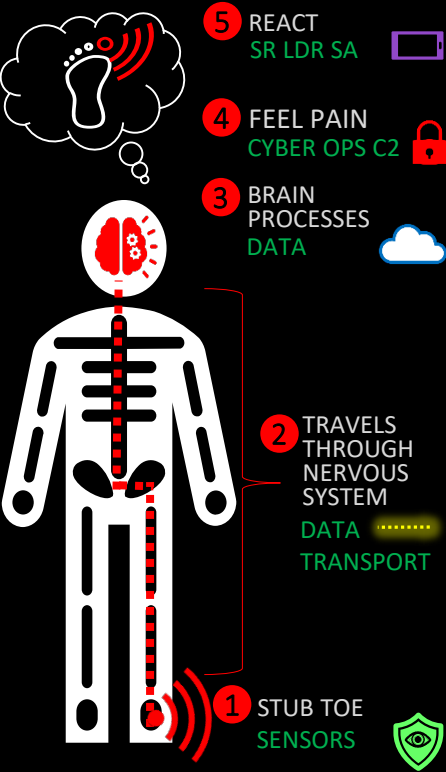
Does not exist.

Senior Leader SA

Does not exist.



"PAIN PATH" EXAMPLE



OV-1 CS & CD TAILORED SOLUTIONS

LINES OF EFFORT

DATA STRATEGY

IWN

TDC

SR LEADER SA

CYBER C2

SENSOR IMPLEMENTATION

CRITICAL ENABLERS



CRITICAL ENABLERS



CRITICAL ENABLERS



CRITICAL ENABLERS



BIG DATA
PLATFORM

SENIOR LEADER
SITUATIONAL
AWARENESS

COST (ROM)

Total	FY24	FYDP
FY22/23	FY24	FYDP
\$473.6M	\$409.0M	\$1,605.4M

Sensor Implementation

FY22/23	FY24	FYDP
\$51.0M	\$89.4M	\$419.1M

IWN

FY22/23	FY24	FYDP
\$37.4M	\$55.4M	\$238.7M

TDC

FY22/23	FY24	FYDP
\$43.4M	\$171.1M	\$359.5M

SR Leader Dashboard

FY22/23	FY24	FYDP
\$10.9M	\$13.6M	\$72.0M

Cyber Ops C2

FY22/23	FY24	FYDP
\$27.8M	\$24.8M	\$134.9M

Other Investments

FY22/23	FY24	FYDP
\$303.1M	\$54.7M	\$381.2M

INFORMATION SYSTEMS

Information Technology backbone for computers, communications and C2

WEAPON SYSTEMS

Cyber-enabled Mission Design Series spanning Air and Space core functions

CONTROL SYSTEMS

Cyber-enabled operational technology critical to Air and Space power generation

Sensors

A defensive cyber operations framework via VOLTRN+ and MOSAICS capabilities consisting of sensors and a common persona-based platform bringing all-system data to local and Enterprise instantiations of ELICSAR Big Data Platform (BDP).

Data Transport

Theater Deployable Communications (TDC) paired with Integrated Warfighting Network (IWN) provides an organic, resilient expeditionary communications capability at the Wing level to enable Agile Combat Employment.

Data

ELICSAR BDP will broker cyber-based information, weapon, and control system data in Unclassified, Secret and Top Secret domains. This central repository will enable decision advantage across the spectrum.

Cyber Ops C2

A defensive countercyber force apportioned at echelon with mission threat response at Wing level, Cyber Defense Correlation Cell (CDCC) at MAJCOM, and the AFIN SOC at enterprise level with battle management and situational awareness integrated by JCC2.

Senior Leader SA

The Senior Leader Dashboard supports the visualization of cyber data from ELICSAR using the C2IE capability. Already approved by PACOM, the dashboard will enhance senior leader awareness of risk to cyber-enabled combat and supporting systems.



CRITICAL PATH TO DEFENSIVE COUNTERCYBER

CRITICAL MISSION THREADS

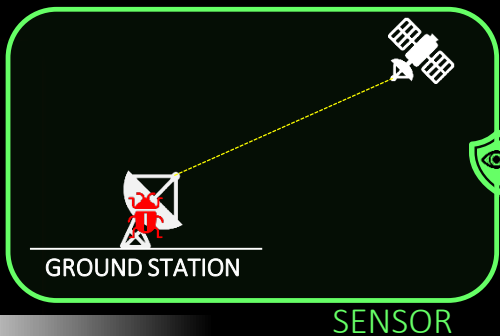
MISSION THREAT
RESPONSE FORCE

LONG-HAUL KILL CHAIN

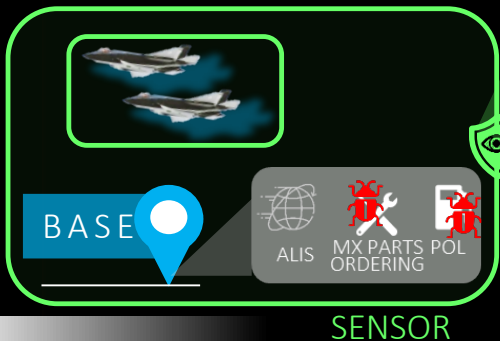
COMBAT OPERATIONS



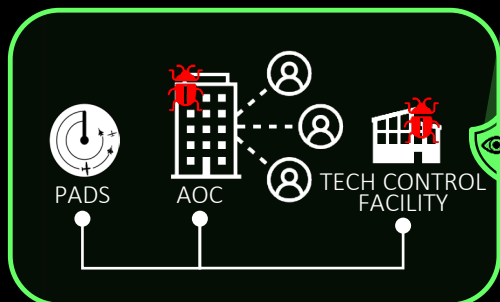
SPACE OPERATIONS



AIR OPERATIONS



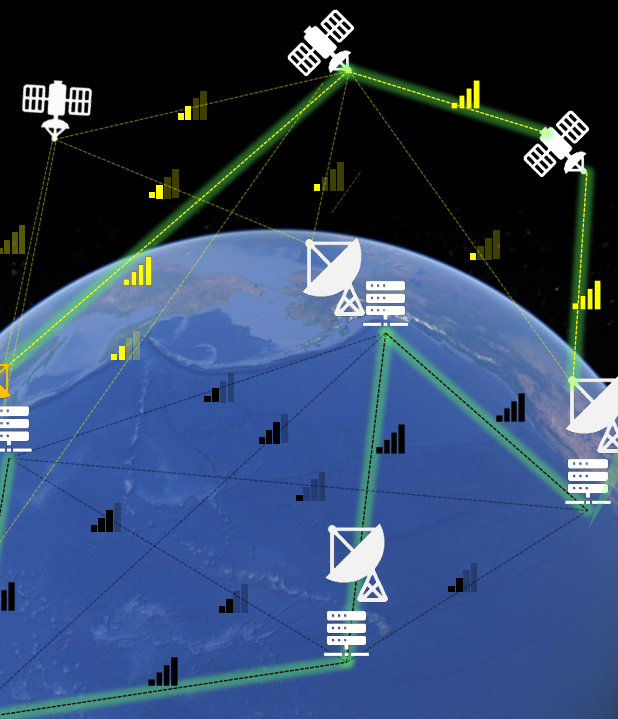
C2/GROUND OPERATIONS



INCIDENT RESPONSE



*Risk-informed
Operational
Decisions for Critical
Mission Threads*



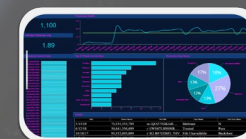
LONG-HAUL COMMUNICATIONS
"DIVERSE ROUTING"

ELIC SAR
BIG DATA
PLATFORM

ANALYZE / EXECUTE



CYBER READINESS POSTURE





DECISION POINT

TFSS Roll Up: Cybersecurity and Cyber Defense Plan (PACAF)

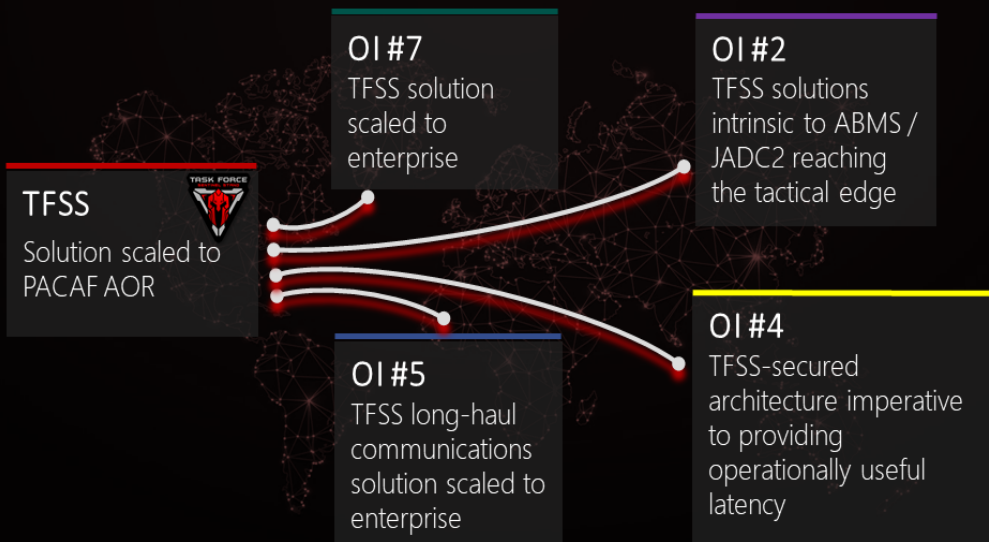
NEXT STEPS

1. Develop a 1-N stratification of mission enabling systems (POL, PADS, environmental, etc) supporting associated 1-N major weapon systems
2. Develop a 1-N stratification (with supporting analysis) of cyber risks across the relevant weapon systems and mission enabling systems
3. Build a phased plan to manage identified cyber risks until they are addressed
4. Draft solutions execution plan to match FYDP, and assign to appropriate stakeholders
5. Use CS&CD EXCOM for plan oversight

SOLUTIONS TO FUND

- Sensor Implementation: A defensive cyber operations framework via VOLTRN+ and MOSAICS capabilities bringing all-system data to ELICSAR.
- Data: ELICSAR BDP will broker cyber-based information, weapon and control system data in Unclassified, Secret and Top Secret domains.
- Data Transport: Theater Deployable Communications (TDC) paired with Integrated Warfighting Network (IWN) provides organic, resilient communications.
- Cyber Ops C2: A defensive counter cyber force apportioned at echelon with battle management and situational awareness integrated by JCC2.
- Senior Leader Dashboard: Presentation of cyber-driven Mission Risk Posture across PACAF systems.

CONVERGENCE: OPERATIONAL IMPERATIVES



Decision Points

FY24 POM

Disconnect:

FY22/23 Reprogramming:
FY24 Requirement:

CONCUR

☐

NON-CONCUR

☐

FYDP Outlook

Disconnect:

Currently Funded:

CONCUR

☐

NON-CONCUR

☐

FRANK KENDALL
Secretary of the Air Force

Questions?

