AFLCMC/HBN C5ISR and IAMD Overarching System of Systems Construct (SoSC) Compendium - Volume 3

Secure Computing Environment (SCE)

30 May 2020

Prepared by:
International and Foreign Military Sales Division

AFLCMC/HBN

HANSCOM AFB, MA 01731

THIS PAGE INTENTIONALLY LEFT BLANK

RECORD OF CHANGES

Version	Date	Author	Change Comments

TABLE OF CONTENTS

1. PURPOSE

The purpose of this document is to describe and define AFLCMC/HBN's Command and Control, Communications, Computers, Cybersecurity, Intelligence, Surveillance and Reconnaissance (C5ISR) and Integrated Air and Missile Defense (IAMD) Overarching System of Systems Construct in the context of FMS Cases for the Air Force Life Cycle Management Center, Battle Management Directorate, International and Foreign Military Sales Division (AFLCMC/HBN).

This document supports:

IN PARTNERSHIP WITH OUR INTERNATIONAL FMS AND DEFENSE INDUSTRY PARTNERS; DELIVERING AND SUSTAINING WORLD-CLASS C5ISR and IAMD CAPABILITIES.

2. REFERENCES

The Compendium for C5ISR and IAMD Overarching System of Systems Construct is comprised of six specific volumes as referenced below.

a) AFLCMC/HBN C5ISR and IAMD SoSC Compendium Construct, 30 May 2020

1) AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume 1 – Concept of Operations (CONOPS), 30 May 2020

2) AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume 2 – System of Systems A-Specification, 30 May 2020

3) AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume 3 – Secure Computing Environment (SCE), 30 May 2020

4) AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume 4 – Cybersecurity Provisioning, 30 May 2020

5) AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume 5 – Integrated Logistics, 30 May 2020

6) AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume 6 – Embedded Interactive Training and Simulation, 30 May 2020

3. SCOPE

AFLCMC/HBN supports the 2018 U.S. National Defense Strategy (NDS) by delivering battle management capabilities to Partner Nations (PN) for conducting Joint Air Operations and Integrated Air and Missile Defense (IAMD). Using a digital engineering approach, AFLCMC/HBN has processes and artifacts that shorten the time to deliver capabilities and deepening interoperability. The approach requires

a coordinated effort with Secretary of the Air Force/International Affairs (SAF/IA), Defense Security Cooperation Agency (DSCA), Combatant Commanders and Industry. This Battle Management capability approach acknowledges that delivering a single material solution alone does not necessarily increase a Partner Nation's warfighting capability or deepen interoperability. The approach as depicted below, focuses on three main components that lead collectively to the optimization of a functional material solution set in accordance with the warfare missions delineated in the AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume 1 – Concept of Operations (CONOPS):

- Delivering and Maintaining an Effective C5ISR System,
- Developing Trained Personnel and
- Maturing Tactics, Techniques and Procedures (TTP).

The aforementioned components are integral supportive actions required to procure, install and/or upgrade an effective C5ISR and IAMD system and are formulated by compliance and guidance with additional components that effect operational capability/functionality as depicted in Figure 1 below.

Figure 1. Focus Areas that Formulate an Effective C5ISR and IAMD System

The document provides U.S. Government and Defense Industry Partnerships a Constructualization of Command & Control, Communications, Computers, Cybersecurity, Intelligence, Surveillance, Reconnaissance (C5ISR) capabilities and how they may be applied to future deliveries of international C5ISR/IAMD Systems and Sensors. The C5ISR and IAMD Overarching SoSC Compendium objective for supporting global warfare missions is achieved via the implementation of a secure, modular, and adaptive network-enabled systems architecture and tactical applications that facilitate and enhance successful "Sensor to Shooter" engagements.

A Secure Computing Environment (SCE) platform is the foundational capability required for successful weapons system(s) implementation and sustainment of C5ISR and IAMD systems and is inter-related and in some cases, even co-dependent upon other primary system capabilities as depicted below in Figure 2. Innovative Information Technology coupled with evolving cutting-edge, virtualized tactical applications and sub-systems transition, form the foundational construct of the C5ISR and IAMD Overarching Systems of System Construct.

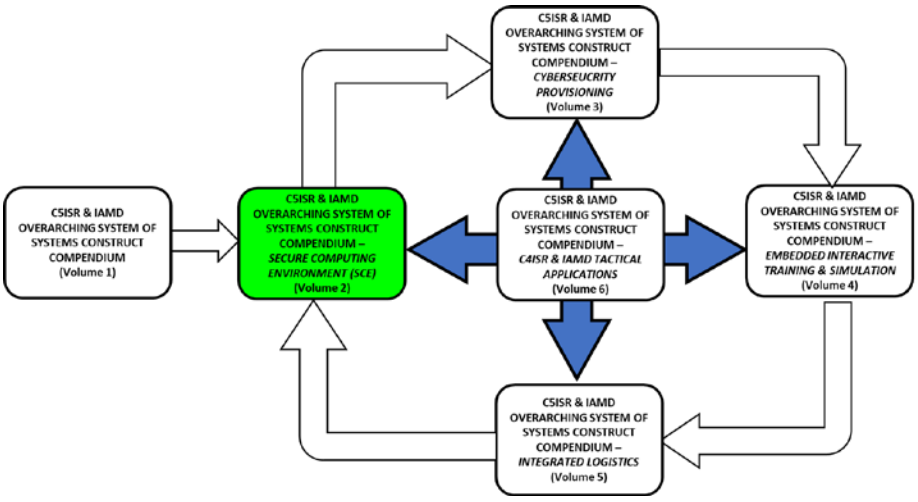

Figure 2. C5ISR & IAMD Overarching System of Systems Construct Compendium Inter-Dependencies

This document, Secure Computing Environment (SCE), specifically supports Partner Nation (PN) warfare missions and personnel by outlining the requisite SCE's IT infrastructure/architecture initiatives, concepts, practices and applications required, as one of the primary elements leading to effective C5ISR and IAMD system(s) implementation. Figure 3 below, depicts the SCE platform relationship associated with nominal warfare mission support. Requirements for a robust, stable and secure SCE supporting the tactical architecture (networks) extends across to all associated and interconnected applications.

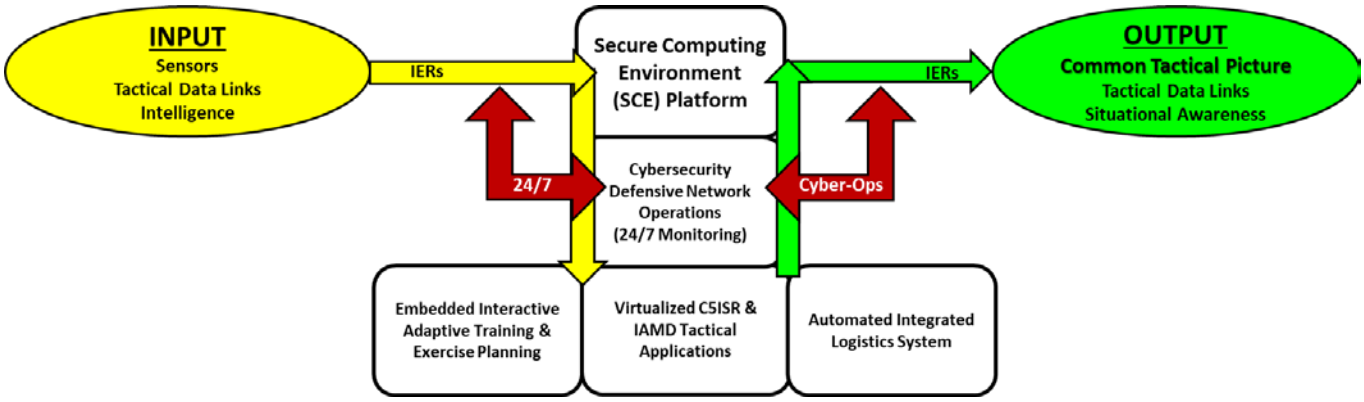

Figure 3. C5ISR & IAMD Overarching System of Systems Construct in Support of Nominal Warfare Mission Employment

4. C5ISR AND IAMD OVERARCHING SYSTEM OF SYSTEMS IMPLEMENTATION

The C5ISR and IAMD System of Systems Construct provide Partner Nations the collective capabilities required to support real-time warfare mission operations, cybersecurity defense, sustained logistical support and enduring enhanced training and simulation capabilities for C5ISR and IAMD architectures

and operating personnel. AFLCMC/HBN Overarching SoSC Compendium Volume 6 – Embedded Interactive Training and Simulation provides detailed information regarding SoSC training regimens.

The foundational bedrock of supporting an integrated system of systems architecture is the establishment of a secure computing environment (SCE) platform. The SCE platform ensures that C5ISR and IAMD applications and weapons systems conduct real-time tactical informational exchange of air and theater missile defense surveillance tracks coupled with effective and efficient Command and Control data elements (from initial detection to weapons engagement to battle damage assessment). It is imperative that real-time tactical data is transported via secure, stable dissemination conduits to all requisite echelon nodes and that the network infrastructure (components/systems) and architecture are vigilantly monitored, assessed and defended against all cybersecurity threats.

The ***SCE Platform*** is based on a service-oriented architecture (SOA). Migration to a Secure Computing Environment (SCE) platform employs hyper-converged private multi-cloud SOA (services-based) systems supporting the ever-increasing demands for more agile C5ISR and IAMD systems. The evolution of DoD SOA processes are depicted in Figure 4 below. Concurrently this implementation provides cost effective systems with increased "speed-to-capability implementation" (fielding).

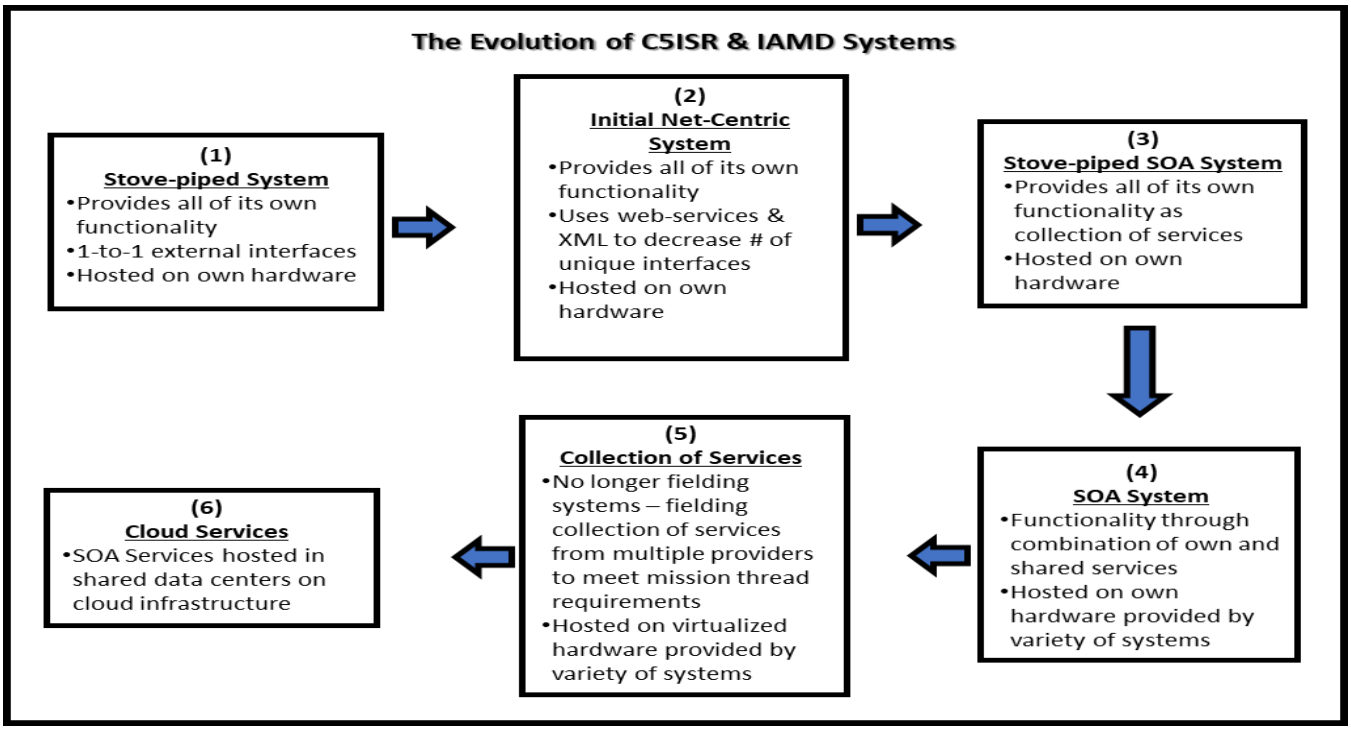

Figure 4. Service-Oriented Architecture Evolution in C5ISR and IAMD Systems

Transitioning to private cloud services implementation, collectively referred to as secure computing environment (platform), entails the implementation of a multi-cloud, hyper-converged system of systems that, in of itself provides the networked infrastructure enabling situational awareness, specifically, real-time depiction of a Single Integrated Air Picture (SIAP). The "system of systems" construct is enabled by a virtualized/containerized suite (set) of ***mission applications*** producing reliable sensor and

informational exchange of relevant data. The SoSC also supports interoperability with U.S. and Coalition forces operating on U.S. SECRET Releasable security domains. Many Partner Nations have systems that were not originally intended to operate at the U.S. SECRET Releasable level and as a result, cannot take full advantage of advanced weapons systems that generate U.S. SECRET Releasable data such as Link-16 and Mode 5. The Overarching SoSC encompasses High-Assurance Internet Protocol Encryption (HAIPE) when required, U.S. Keymat and fill devices when authorized and Foreign Cross-Domain Solution (FCDS) devices when approved for export.

4.1. SECURE COMPUTING ENVIRONMENT (SCE) PLATFORM IMPLEMENTATION

An effective SCE includes all aspects of data dissemination, processing and storage components/systems associated with network enclaves and/or domains that extend to all required data end users (nodes). The SCE platform system of systems implementation is a modular, scalable, robust, and stable seamless integration of an IT infrastructure that operates on a continuous 24/7 basis. The SCE platform is defined by five (5) capability areas:

- Infrastructure
- Operating Systems
- Virtualization Software
- Container Software and
- Services.

Network data transport services are secured via High-Assurance, Internet Protocol, Encryptors (HAIPE)/Crypto devices and in the future, may also host or connect to Foreign Cross Domain Solutions (FCDS) devices as well. An SCE generally integrates and employs leading IT industries' complement of current and evolving Non-Developmental Items (NDI) and/or Commercial-Off-The-Shelf (COTS) Information Technology (IT) components and/or systems that are designed to function in the modern 21st Century cybersecurity environment.

The SCE platform has three primary functions providing:

- Mission Applications Framework
  - Hosts and integrates virtualized/containerized C5ISR and IAMD applications for direct optimized warfare mission support at the strategic, tactical and operational levels
- Cybersecurity Services
  - Defensive and counter cyber-threat protection for the C5ISR and IAMD network infrastructure and the associated information exchange dissemination conduits from malicious and adversarial cybersecurity attack
- Collaboration Services
  - Secure and stable dissemination conduits for C5ISR and IAMD information exchange data in direct support of the warfighters and leadership for conducting successful territorial defense against air breathing and theater missile threats.

A secure computing environment (platform) infrastructure coupled with an established tactical data network architecture is a foundational element required in order to provide a modern and effective secure C5ISR and IAMD system providing superior situational awareness by generation and maintenance of a single Common Tactical Picture (CTP) or also referred to as Single Integrated Air Picture (SIAP) or

Recognized Air Picture (RAP) or Common Operating Picture (COP). For effective and efficient C5ISR and IAMD networks the CTP needs to be disseminated for display and action at all echelon activities/units (nodes). Figure 5 depict a figurative IT Layer representation of an SCE capability/functionality construct and Figure 6 provides a representative depiction of containerized/virtualized NDI tactical mission applications integrated into a secure computing environment.

Figure 5. Secure Computing Environment Construct

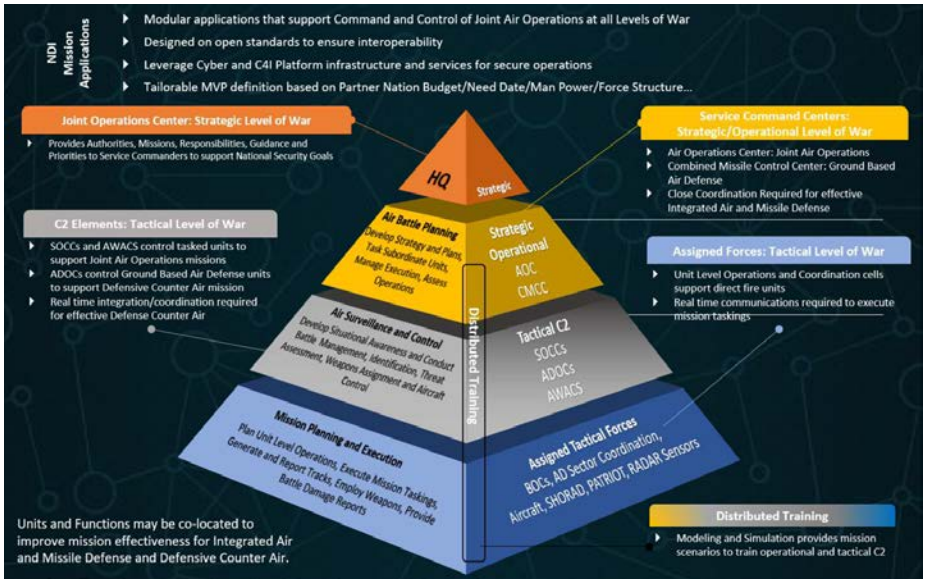

Figure 6. NDI Tactical Mission Applications Operating on a Secure Computing Environment

4.2. CYBERSECURITY SCE PROVISIONING IMPLEMENTATION

Cybersecurity a mandatory requirement directly supports a systems' implementation with active maintenance of its resident security posture and practices with respect to, the reliability and protection of any data element transported via a multitude of dissemination conduits. Positive cybersecurity initiatives and protection policies must be implemented in a C5ISR and IAMD systems to include the protection of system data and network operations that encompasses end-to-end connectivity. If nefarious cyber-attackers (hackers) gain access to an information technology network or system component there is a distinct possibility that the information residing on that network and or network data storage elements could be captured and/or maliciously manipulated. Critical data dissemination disruptions (denial of service / malicious logic / track identity / track reporting) could potentially create serious harm to a nation's air and theater missile defense activity thereby resulting in damage to defended assets and loss of personnel. Refer to AFLCMC/HBN C5ISR and IAMD Overarching SoSC Compendium Volume -4 – Cybersecurity for additional processes for maintaining adequate cybersecurity posture for an SCE platform.

A SCE platform implements technical security controls to mitigate risk based on the Partner Nation's risk acceptance level for the specific security domain. For security domains that include U.S. Classified Military Information (CMI), a SCE must implement the technical security controls specified by the U.S. Combatant Commander in accordance with U.S. policy which is implemented in accordance with U.S. DoD Risk Management Framework (RMF) security provisions.

This SCE platform provides the requisite containerized, hyper-converged, private –cloud foundational infrastructures that simultaneously furnishes support for virtualized C5ISR and IAMD applications and its tactical data network while simultaneously delivering an active and robust cybersecurity defensive capability that maintains 24/7 security operations and monitoring. The RMF process when employed will determine an IT system's resident information in terms of Confidentiality (rules limiting access to information), Integrity (information accuracy [trustworthy]) and Availability (guaranteed reliable access by authorized individuals) which in turn, dictate the level of security provisioning required to maintain adequate and proactive system cybersecurity.

Effective implementation of cybersecurity provisions requires an investment in a dedicated and manned, centralized Cybersecurity Network Operations Center (CNOC) that will provide 24/7 remote monitoring and active analyses of the network topology, health, security and capacity (traffic load balancing) in order to ensure optimal network and organizational performance and cybersecurity defense is maintained. The CNOC will provide cyber-threat detection and network cyber-threat alert notification for any cyber-threat incidents. CNOC technicians will initiate immediate actions to isolate the threat(s), reroute data paths as required to remain tactical and system availability while commencing remediation (addressing a breach and limiting the amount of damage to the IT system). Remediation countermeasures include agile actions such as isolation, data path rerouting, component/system re-configuration, and patching or software modifications. Remediation is the lynchpin of actions to avert secure tactical data loss and is an essential foundational required to effectively maintain a Continuity of Operations Plan (COOP). Concurrently the CNOC provides access to stored voice and video storage that can be archived for technicians to utilize in post-action forensic investigation applications and synchronized playback analyses.

An SCE platform is comprised of, but not limited to a hyper-converged, secure, modular, flexible and scalable platform for warfare mission application deployment. The SCE provides advanced capabilities to the warfighter by leveraging tailorable, and scalable "state of the art" C5ISR and IAMD Non-Developmental item(s) (NDI) vendor capabilities into a common C5ISR and IAMD product line options coupled with integrated cybersecurity services as depicted below in Figures 7 and 8. Some elemental and extended core cybersecurity services are depicted in Figure 9 below. Several leading IT/Cybersecurity SCE service providers, not all inclusive, are provided below in Figure 10.

Figure 7. SCE Hosting Mission Applications

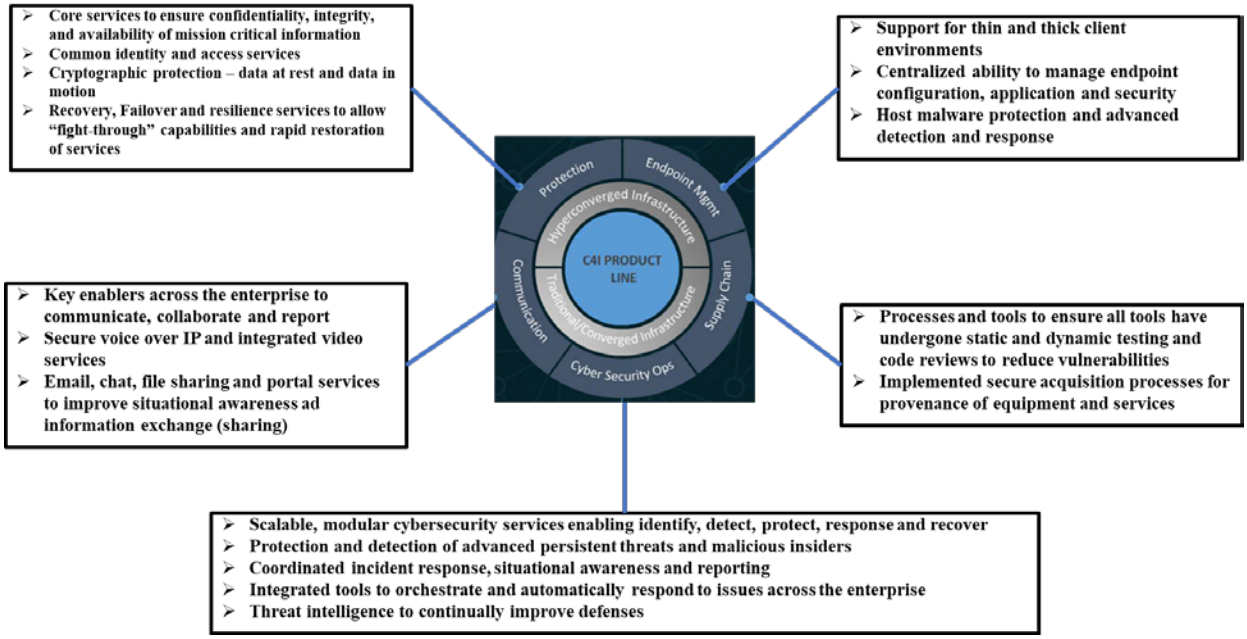

Figure 8. Sample Representation of SCE Integrated Cybersecurity Services

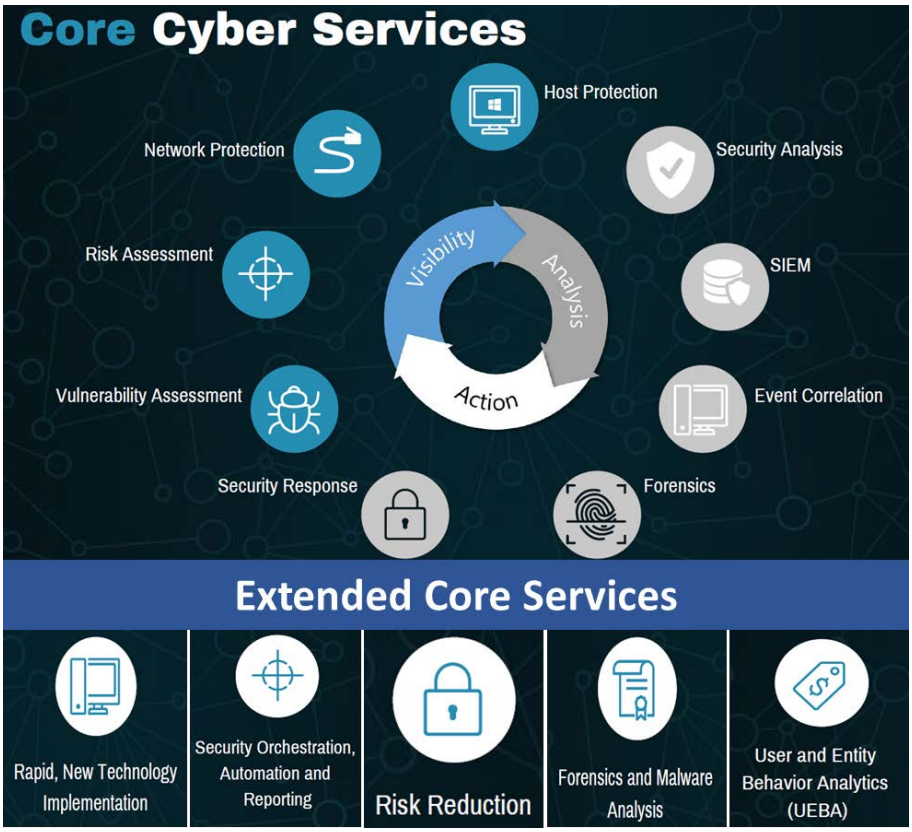

Figure 9. Core Cybersecurity Services

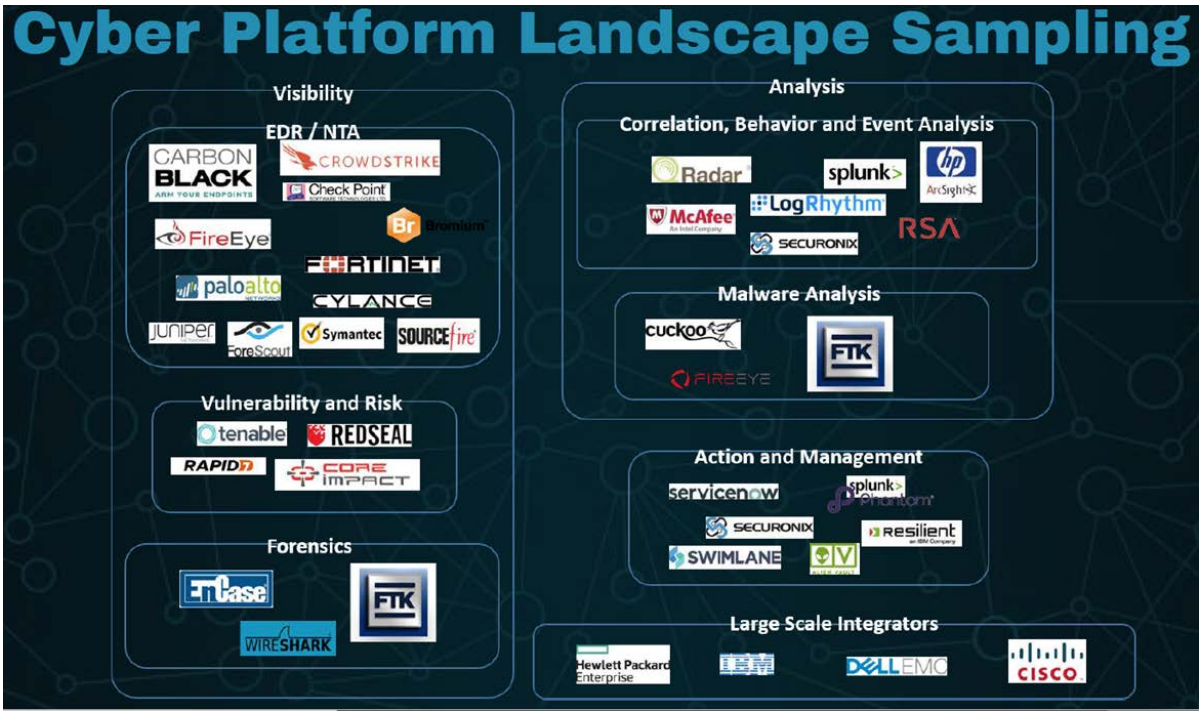

Figure 10. Sampling of Cybersecurity Platform Contractors

5. TIME-PHASED IMPLEMENTATION

Contract administration, production schedules, delivery periods, installation, initial training and testing events all impact operationalization of new or upgraded C5ISR and IAMD components and systems. Procurement, contractor and warfare representatives are to develop a schedule that delivers a fully operational and integrated capability at the completion of acceptance testing. Time-phased implementation plans can efficiently schedule integrated installations of capability sets, be it individual, or set (group) of capabilities. However, integrated installation stages (phases) must be fully supported by system/component tactics, techniques and procedures (TTP), established training regimens, cybersecurity, provisioning and logistical support interval installations and enable a viable operational capability enhancement. Appendix B below, provides a simple form to support development of Time-Phased Installation schedules. Identification of co-dependencies from other components, systems, source inputs, and associated capabilities must be captured and identified by implementation date to have a successful system installation. This activity will preclude the installation of components that must sit at idle capacity, awaiting the installation of another component or capability set.

APPENDIX A

ACROYMNS

ABT	Air Breathing Threat
AC	Alternating Current
ACL	Access Control List
ACO	Air Control Order
ADOC	Air Defense Operations Center
AFB	Air Force Base
AMD	Air and Missile Defense
AOC	Aerospace Operations Center
ATC	Air Traffic Control
ATO	Air Tasking Order
AFLCMC	Air Force Life Cycle Management Center
AFLCMC/HBN	AFLCMC International and Foreign Military Sales Division
ASTERIX	All Purpose Structured Eurocontrol Surveillance Information Exchange
°C	Centigrade
C2	Command and Control
C4ISR	Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
C5ISR	Command and Control, Communications, Computers, Cybersecurity, Intelligence, Surveillance and Reconnaissance
CAOC	Coalition Aerospace Operations Center
CENTCOM	(USCENTCOM) U.S. Central Command
CI&A	Confidentiality, Integrity and Availability
CMI	Classified Military Information
CNOC	Cybersecurity Network Operations Center
CNSSAM	Committee on National Security Systems Advisory Memorandum
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operations Procedures
COP	Common Operational Picture
COTS	Commercial Off the Shelf
CPU	Central Processing Unit
CTP	Common Tactical Picture
CU	Controlling Unit (Link 16)
Db	Decibel
DC	Direct Current
DCN	Document Control Number
DCOE	Defense Centers of Excellence
DCS	Data Communications System
DERG	Data Extraction and Reduction Guide (TDL)
DISA	Defense Information Systems Agency (U.S)
DoD	U.S. Department of Defense
DoDI	DoD Instruction
DSCA	Defense Security Cooperation Agency
ESD	Electrostatic Discharge
FIPS	Federal Information Processing Standard (U.S.)
FCDS	Foreign Cross Domain Solution (device)
FMS	Foreign Military Sales
FPC	Full Packet Capture
GHz	Gigahertz

GPS	Global Positioning System
GPU	Graphic Processing Unit
HAIPE	High-Assurance Internet Protocol Encryption
HERP	Hazards of Electromagnetic Radiation to Personnel
Hz	Hertz
IAMD	Integrated Air and Missile Defense
IAW	In Accordance With
IDM	Intrusion Detection Monitoring
IDS	Intrusion Detection System
ILS	Integrated Logistics Support
IP	Internet Protocol
IT	Information Technology
ITSM	IT Service Management
JREAP	Joint Range Extension Protocol
KHz	Kilohertz
KVM	Keyboard, Video and Mouse
LAN	Local Area Network
MA	Massachusetts
MAN	Metropolitan Area Network
MIDS	Multi-functional Informational Distribution System
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
NDI	Non-Developmental Item
NDS	U.S. National Defense Strategy
NIST	National Institute of Standards and Technology
NMS	Network Management System
NOC	Network Operations Center
NOS	Network Operating System
NSI	National Security Information
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memoranda
PDS	Protection Distribution System or Power Distribution System
PDU	Protocol Data Unit
PEO	Program Executive Officer
PKI	Public Key Infrastructure
PN	Partner Nations
POP	Point of Presence or Period of Performance
PPLI	Precise Participant Location and Identification
QoS	Quality of Service
R2	Reporting Responsibility (link 16)
RAM	Random Access Memory
RAP	Recognized Air Picture
RCC	Radio Communications Committee of the IEE or Regional Communications Center
RF	Radio Frequency
RMF	Risk Management Framework
SA	Situational Awareness
SAASM	Selective Availability, Anti-Spoofing Module
SAF/IA	Secretary of the Air Force/International Affairs
SCE	Secure Computing Environment
SIAP	Single Integrated Air Picture
SIEM	Security Intrusion and Event Management
SNMP	Simple Network Management Protocol
TBM	Theater Ballistic Missile
TDL	Tactical Data Link
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions
TTP	Tactics, Techniques and Procedures
UHF	Ultra-High Frequency

UPS	Uninterruptible Power Supply
U.S.	United States
USCOCOM	U.S. Combatant Command
USCENTCOM	U.S. Central Command (Combatant Command)
USMTF	U.S. Message Text Format
UTC	Universal Time Coordination
V	Volt
VCP	Voice Control Panel
VCS	Voice Control System
VHF	Very-High Frequency
vLAN or VLAN	Virtual Local Area Network
VM	Virtual Machine
VMF	Variable Message Format
VoIP	Voice over Internet Protocol
VTC	Video Tele-Conference
VTE	Virtual Training Environments
VULOS	VHF/UHF Line of Sight
W/S	Work Station
WAN	Wide Area Network
XMPP	Extensible Messaging and Presence Protocol

APPENDIX B

Time-Phased Implementation of C5ISR and IAMD System Requirements

Time-Phased Implementation of C5ISR and IAMD Systems Requirements				
Requirement	**Capability Component**	**Phase 1 Capabilities Delivery (Years 1-2)**	**Phase 2 Capabilities Delivery (Years 3-5)**	**Phase 3 Capabilities Delivery (Years 6-10)**
Secure Computing Environment	System	☐	☐	☐
	Training	☐	☒	☐
	TTP	☐	☐	☐
	Dependencies			
	Date			
Mission Applications	System	☐	☐	☐
	Training	☐	☐	☐
	TTP	☐	☐	☐
	Dependencies			
	Date			
Cybersecurity	System	☐	☐	☐
	Training	☐	☐	☐
	TTP	☐	☐	☐
	Dependencies			
	Date			
Intelligence Applications	System	☐	☐	☐
	Training	☐	☐	☐
	TTP			
	Dependencies			
	Date			
Logistical Operations	System	☐	☐	☐
	Training	☐	☐	☐
	TTP	☐	☐	☐
	Dependencies			
	Date			
Embedded Integrated Training and Simulation	System	☐	☐	☐
	Training	☐	☐	☐
	TTP	☐	☐	☐
	Dependencies			
	Date			
Encryption	System	☐	☐	☐
	Training	☒	☐	☐

	TTP	☐	☐	☐
	Dependencies			
	Date			
FMS CDS	System	☐	☐	☐
	Training	☐	☐	☐
	TTP	☐	☐	☐
	Dependencies			
	Date			