688 Cyberspace Wing's

CENTERS OF EXCELLENCE (COE) INTEGRATION ELEMENT (CIE)

CIE Commanders:
Lt Col Jessica 'Jess' Perez (690 COS)
Lt Col Sidney 'Sid' Harris (691 COS)
Lt Col Jeremy 'Cookie' Cook (299 NOS-TFI)

Controlled by: Air Force
Controlled by: 690 COS
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC Lt Col Perez, 808-448-4830

WIRED FOR WAR

CIE Overview

- What is a Center of Excellence Integration Element (CIE)?
- Center Of Excellence (COE) Construct
- Center of Excellence Integration Element Functions
- Mission Growth
- Problem Resolution Teams (PRT)
- 33 COS Operating Locations E & F
- Cyberspace Awareness Dashboard (CAD)
- Questions?

CIE Mission

688 CW: America's First Cyberspace Wing…engineering, operating, extending, and defending the Air Force Information Network and warfighter communications…anytime, anywhere!

688 CW Vision: To be the Air Force's most *reliable* and *trusted* Wing.

CIE Mission (690 COS, 691 COS, 299 NOS):

- Integrate operations across all areas with the appropriate Functional Center of Excellence
- Maintain situational awareness of operational priorities to include: AFCYBER Cyber Tasking Order tasks,
- MAJCOM top 5 priorities, critical tickets and core service outages.
- Provide an initial response for critical cyber taskings when the appropriate Center of Excellence is unavailable.
- Identify training slot requirements to appropriate Functional CoE.

WIRED FOR WAR

CUI

CENTER OF EXCELLENCE INTEGRATION

688TH CYBERSPACE WING

Cyber Weapon Systems:

- Cyberspace Security & Control System (CSCS)
- Air Force Cyberspace Defense (ACD)
- Cyberspace Defense Analysis (CDA)
- Air Force Intranet Control (AFINC)

690 COS Operational Capabilities:

- Directory Services
- Storage & Virtualization
- Network Management
- Attack Surface Management

690 CYBERSPACE CONTROL SQ — INTEGRATE TO DOMINATE

Centers of Excellence (COE)

FOC: JULY 2024

690th CYBERSPACE OPERATIONS SQ — DEVELOP DEFEND DOMINATE
- COE Integration Element (CIE)

561st NETWORK OPERATIONS SQ
- Vulnerability Management
- Client Protection

38th ENGINEERING SQ — HONEY BADGERS NEVER QUIT
- Performance Monitoring
- Engineering

336 CYBERSPACE OPERATIONS SQ
- Security Operations
- GLOBAL AFIN SOC

26th NETWORK OPERATIONS SQ — ALWAYS ON ALWAYS READY
- Network Management
- Boundary Protection

5th COMBAT COMMUNICATIONS GROUP
- Global Expeditionary Communications

833 NETWORK OPERATIONS SQ
- Directory Services
- Messaging
- Network Monitoring
- Storage & Virtualization

IOC: SEPT 2024

690th CYBERSPACE OPERATIONS SQ — RESILIENT UNDER FIRE
- COE Integration Element (CIE)

CUI

CIE Functions

Directory Services
Assume maintenance responsibilities for all AFNET and AFNET-S Active Directory forests

- Policy Management
- Authentication Services – DNS, DHCP, DCs
- Change Request Management

Network Management
Ensures secure access through base boundary equipment out to DISA delivery point

- Enterprise Event Management
- Firewall Rules
- Network Analytics

Storage and Virtualization
Configures and manages the datacenter virtual environments hosting core services

- Change Request Management
- Virtualized Environment

Attack Surface Management
Consolidate maintenance, monitoring and operation of enterprise attack surface management capabilities

- Vulnerability Management
- Client Protection and Management
- Vulnerability Analysis and Mitigation
- Data Loss Protection Waivers

WIRED FOR WAR

CUI

MISSION GROWTH:

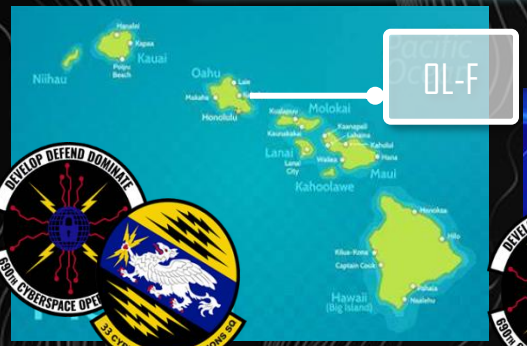
ADVANCING OPERATIONS IN SUPPORT OF GPC

Multi-Qualified Weapon System Operators

- Cyberspace Security & Control System (CSCS)
- Air Force Cyberspace Defense (ACD)
- Cyberspace Defense Analysis (CDA)
- Air Force Intranet Control (AFINC)

Problem Resolution Teams (PRTs)

33 COS Operating Locations



Advancing AFIN Security

Cyber Awareness Dashboard

WIRED FOR WAR

CUI

MISSION GROWTH:

Problem Resolution Team Operations (TFI)

Server 2012
(02 Oct 23 – 17 Nov 23)

End of Life Enterprise Domain Controller upgrades

SIPR REL
(26 Oct 23 – 18 Dec 23)

Created SIPR Five Eye solution at Hickam AFB

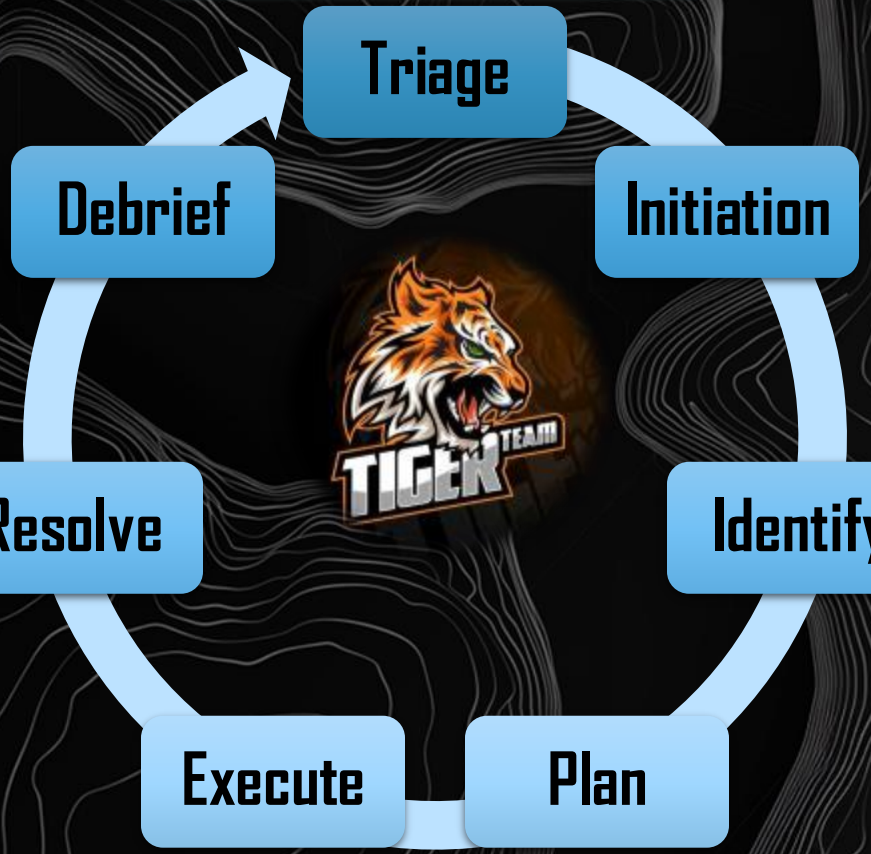
Hickam Degradation
(05 Feb 24)

Hickam DHCP degradation during exercise KEEN EDGE 2024

SIPR ISN
(14 Nov 23 – Current)

Flattening of SIPR Domains

Disciplined PRT Execution



"So-Called CISCO"
(15 May 24 – 05 Aug 24)

Identified counterfeit CISCO devices across the AFIN

Anderson AFB
(10 Dec 23 – 23 Dec 23)

Base Wide SIPR degradation

WIRED FOR WAR

33 COS Operating Location-E & F

Peacetime Operations & Enterprise-level Security

- Conduct security operations at the enterprise level.
- Deepen knowledge of Cyber terrain and mission partner systems.
- Co-located with 690 COS and 691 COS

Adaptability and Focus during Conflict

- Adapt and tailor operations to address specific regional threats.
- Rapid, targeted incident response via local expertise

Geographic Alignment and Collaboration

- Enterprise services are collocated during disconnected ops.
- Enhances COCOM strategic planning for OPLAN execution

Personnel

- OL-E (10) : Capt x1, MSgts x2, TSgts x2, SSgt x2, SrA x3
- OL-F (10) : Lt x1, MSgt x2, TSgt x2, SrA x5

Cyberspace Awareness Dashboard (CAD)

ENDPOINT VISIBILITY

- First time in history the enterprise has achieved 98% ACAS access rates

ACCOUNTABILITY

- Provides mechanism to standardize and enforce how we harden the AFIN against our adversaries
- Promotes advocacy amongst the PMO community

SITUATIONAL AWARENESS

- Provides Senior Leaders with real time SA into the AFIN cyber hygiene

SCALABLE SECURITY

- Operational only on NIPR
- 688 CW is posturing to expand to additional networks

How can we help?
Questions?