

Headquarters U.S. Air Force

Integrity - Service - Excellence

WELCOME

Spring Update 2016

Information Dominance Forum



U.S. AIR FORCE

2016 Information Dominance Forum / Spring Update

Agenda

Mon, 25 April 2016			
		Travel Day	
Start Time	Stop Time	Tue, 26 April 2016 - Information Dominance Forum Smart Center, Andrews AFB	
MAJCOM A6 Briefings: (working lunch)			
		<i>Attended by: MAJCOM A6's and Chiefs, SAF/CIO A6 Directors, and Staff as needed UOD: Short Sleeve Blues/Business Attire</i>	
9:00	9:10	Opening Comments	Lt Gen Bender
9:10	10:10	BITI Acquisition Strategy	Lt Col Brad Panton
10:10	10:40	ACC Update	ACC/A6
10:40	10:50	Break	
10:50	11:20	AETC Update	AETC/A6
11:20	11:50	AFGSC Update	AFGSC/A6
11:50	12:00	Transition to Multi Function Room for working lunch	
12:00	12:30	AFMC Update	AFMC/A6
12:30	13:00	AFSPC Update	AFSPC/A6
13:00	13:30	AFRC Update	AFRC/A6
13:30	13:45	Transition back to Auditorium	
13:45	14:15	AFSOC Update	AFSOC/A6
14:15	14:45	AMC Update	AMC/A6
14:45	15:15	NGB Update	NGB/A6
15:15	15:30	Break	
15:30	16:00	PACAF Update	PACAF/A6
16:00	16:30	USAFE Update	USAFE/A6
16:30	16:45	Day in Review/Discussion	
16:45	18:00	Prep/Transit to Ice-breaker	
Start Time	Stop Time	Tue, 26 April 2016 JB Bolling-Anacostia	
18:00	20:00	ICE-BREAKER	
		<i>Attended by: MAJCOM A6's and SAF/CIO A6 Directors UOD: Smart Casual</i>	

Agenda

Start Time	Stop Time	Wed, 27 April 2016 - Information Dominance Forum Smart Center, Andrews AFB	
7:30	8:00	Continental Breakfast	
Morning Session			
		<i>Attended by: MAJCOM Personnel, Jt/USAF Cyber Personnel, SAF/CIO A6 Directors, and Staff as needed UOD: Short Sleeve Blues/Business Attire</i>	
8:00	9:00	AFSPC Brief	AFSPC
9:15	9:30	Break	
9:30	10:30	DISA Brief - NSCSAR - Classified	DISA
10:30	10:45	Break	
10:45	11:45	Operating In/Through/From Cyber - Classified	Brig Gen Kevin Kennedy
11:45	12:00	Break / Transition to working lunch (MPR)	
12:00	13:00	Defense Innovation Unit Experimental - AF Innovation Strategy	Lt Col Enrique Oti
Afternoon Session (SAF/CIO A6 Briefs)			
		<i>Attended by: MAJCOM Personnel, Jt/USAF Cyber Personnel, SAF/CIO A6 Directors, Staff as needed, and Retired GOs/SESs Open invite to SAF/CIO A6 Personnel UOD: Short Sleeve Blues/Business Attire</i>	
13:15	14:15	IMSC Brief	Col Robert Borja
14:15	14:30	Break	
14:30	15:30	Windows 10 Migration	Lt Col Michael Furman
15:30	18:00	Prep/Transit to Hall of Fame Dinner	
Start Time	Stop Time	Wed, 27 April 2016 - Hall of Fame Dinner JB Bolling-Anacostia	
17:30	18:00	Meet and Greet - Photos with HoF Inductees	
18:00	21:30	Banquet	
		<i>Attended by: Open to AFC4A Invitation UOD: Mess Dress or Semi-formal Dress Uniform (Military) / Formal or Business Attire (Civilian)</i>	

Agenda

Start Time	Stop Time	Thursday, 28 April 2016 - Senior Mentor Discussions, ID Forum (Cont.), Spring Update Smart Center, Andrews AFB	
7:30	8:00	Continental Breakfast	
8:00	8:30	Senior Mentor Discussion	
		<i>Attended by: Retired SAF/CIO A6s, Lt Gen Bender UOD: Short Sleeve Blues/Business Attire</i>	
8:30	8:35	Break	
8:35	9:30	Senior Officer/Enlisted Matters	Lt Col Jeff Blankenship / CMSgt Chip Campbell
		<i>Attended by: Retired SAF/CIO A6s, Retired GOs/SESs, Lt Gen Bender UOD: Short Sleeve Blues/Business Attire</i>	
Spring Update General Session			
		<i>Attended by: MAJCOM personnel, Jt/USAF Cyber Personnel, SAF/CIO A6 Directors, Staff as needed, Retired GOs/SESs, AFC4A members, FedBizOps respondents Open invite to SAF/CIO A6 Personnel UOD: Short Sleeve Blues/Business Attire</i>	
9:30	10:30	Task Force Cyber Secure Update	Col "Data" Bryant
10:30	10:45	Break	
10:45	11:45	Comm Squadron Next	Lt Col Reid Novotny
11:45	12:00	Transition to Andrews Golf Course	
12:00	13:30	AFC4A Lunch with Brief from Lt Gen Bender	Lt Gen Bender
		<i>Attended by: AFC4A Invite</i>	
13:30	13:45	Transition to Smart Center	
Information Dominance Forum (Concludes)			
		<i>Attended by: MAJCOM Personnel, Jt/USAF Cyber Personnel, SAF/CIO A6 Directors, Staff as needed, and Retired GOs/SESs Open invite to SAF/CIO A6 Personnel UOD: Short Sleeve Blues/Business Attire</i>	
13:45	15:00	Health of the Force (enlisted/officer)	Lt Col Christopher Schlak / CMSgt Chip Campbell
15:00	15:15	Break	
15:15	16:00	Deployable Comms and Future Efforts	Col Keith Mueller, 5 CCG
16:00	16:30	Lt Gen Bender's Closing Remarks	
Start Time	Stop Time	Friday, 29 April 2016 - AFC4A Golf Tournament Andrews Golf Course	
8:00	14:00	AFC4A Golf Tournament 07:00 Registration / 08:00 Shotgun Start	
		<i>Attended by: Open to AFC4A Invitation</i>	

Headquarters U.S. Air Force

Integrity - Service - Excellence

Opening Remarks Lt Gen Bill Bender



U.S. AIR FORCE



DEFENSE INNOVATION UNIT EXPERIMENTAL

Lt Col Enrique Oti
Managing Director, Air Force Element

This briefing is not for attribution or distribution.
Briefing represents the views of the author and do not necessarily represent DIUx.

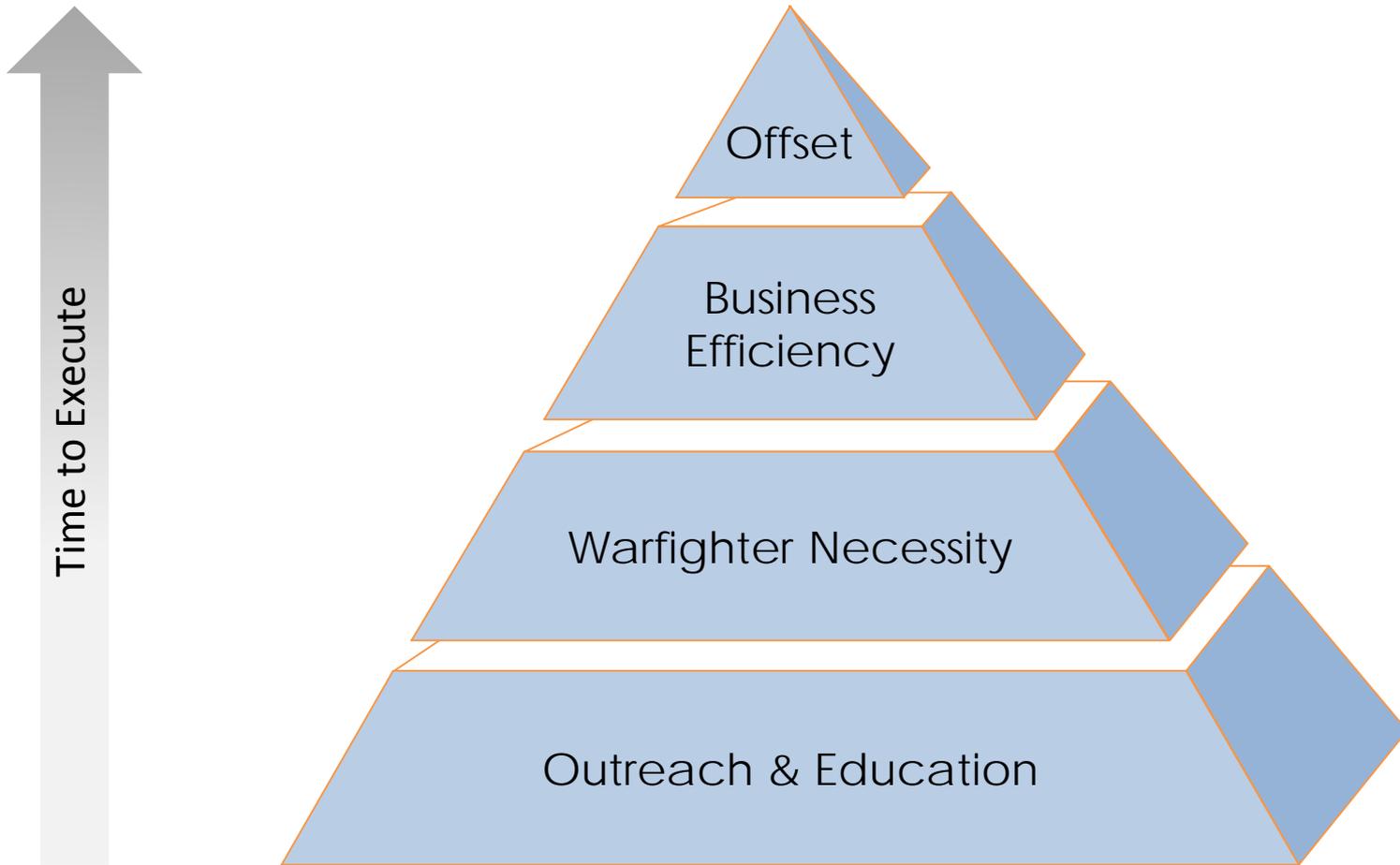
Why Innovate?



We are fighting 21st Century warfare with 20th Century technology and 19th Century manpower and processes



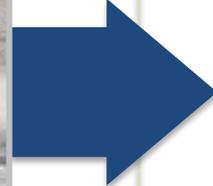
Approach





Strategic Offsets

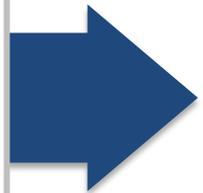
1st Offset



2nd Offset



3rd Offset



1950 1960 1970 1980 1990 2000 2010 2020

Offset = Asymmetric, technological advantage that scales

DIUx Mission

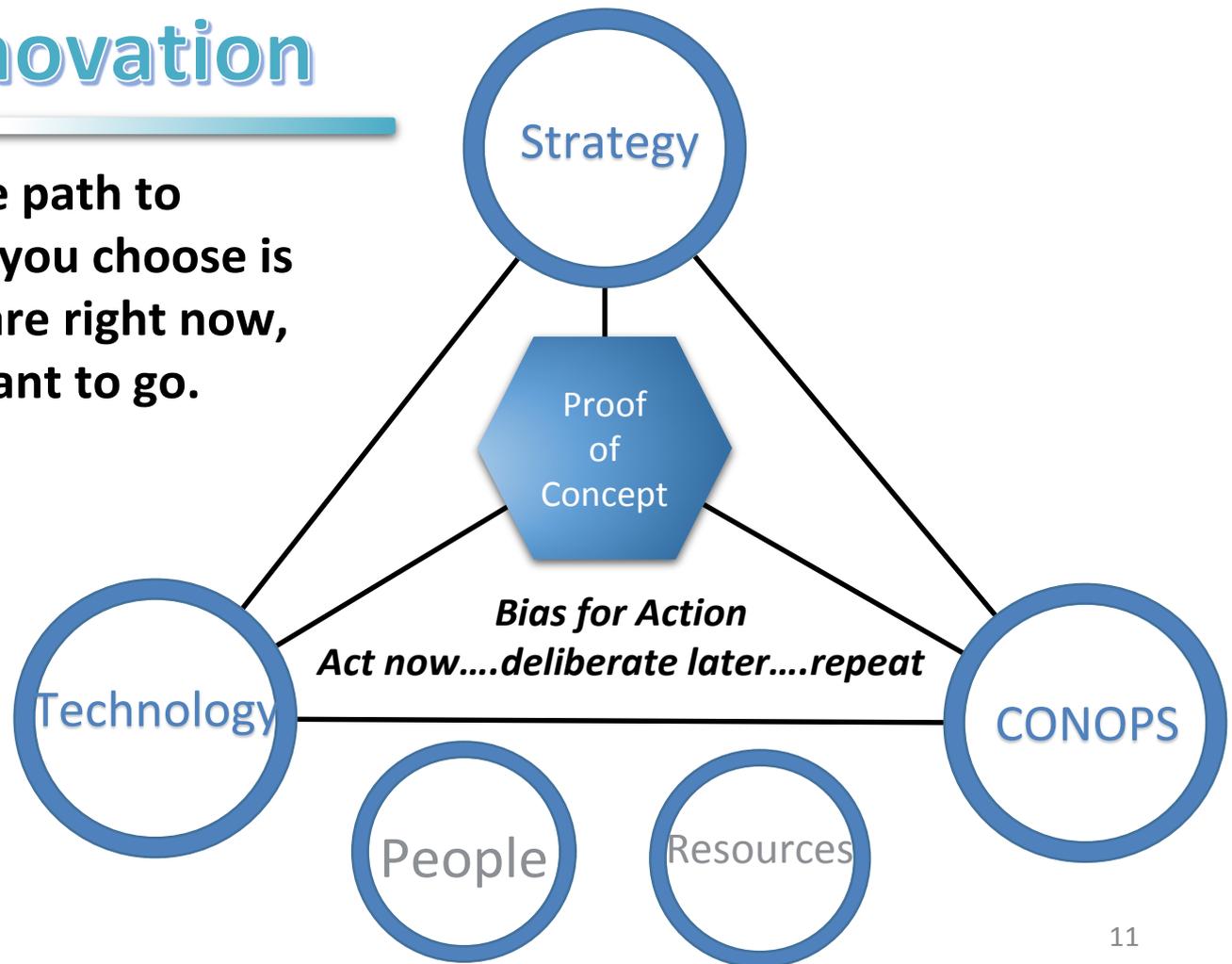
*Strengthen existing relationships
and build new ones.*

*Scout for breakthrough and
emerging technologies.*

*Serve as a local point of presence
for the Department of Defense in
Silicon Valley.*

Iterative Innovation

There is no single path to innovation; the route you choose is based on where you are right now, and where you want to go.



From Concept to Reality

Innovation requires failure....If you succeed 100% of the time, you are not trying hard enough

R&D

“Where do we need to partner or invest to drive technology forward to where we need it?”

Strategic Investment

“We saw an interesting technology, how do we shape it to meet our future needs?”

Quick Reaction Capability

“What can we do right now to make our existing technology work even better?”

Rapid AQ

“We saw an interesting technology that meets an immediate need, how do we buy it now?”

Questions/Comments

“We don't live in an era where all of the technology of importance to national security is going to come out of the Pentagon. Those days are gone.”

-- SECDEF, Apr 2015

Air Force Installation & Mission Support



AFIMSC Update

Col Robert Borja
HQ AFIMSC/IZS
27 Apr 2016



Purpose

***To update the SAF/CIO A6 Info Dominance Forum
on the transfer of communications capabilities
to the AFIMSC***



Overview

- **Why AFIMSC**
- **AFIMSC Communications Capabilities**
- **Capabilities Provided by Other Organizations**
- **AFIMSC Funding Transfer**
- **Milestones / Way Ahead**



Why AFIMSC?



“In this constrained budget environment, we will continue to look for ways to reduce overhead, improve efficiency and maximize combat power, but we must do so in a deliberate manner after careful consideration of how best to ensure this department is able to carry out its mission of defending the nation.”

**Honorable Chuck Hagel,
Secretary of Defense
December 2013**

Is there a more effective and efficient way to manage common, day-to-day, installation support/base operating support (BOS) and expeditionary support activities?



How are we building AFIMSC?

Capability Delivery Methods



What capabilities have to be done by someone with a MAJCOM patch?

Retain at MAJCOMs



What capabilities don't need someone with a MAJCOM patch, but need to be in theater?

Transfer to AFIMSC Dets



What capabilities don't need someone with a MAJCOM patch, can be done by reach back?

Transfer to AFIMSC HQ



AF Installation & Mission Support Center

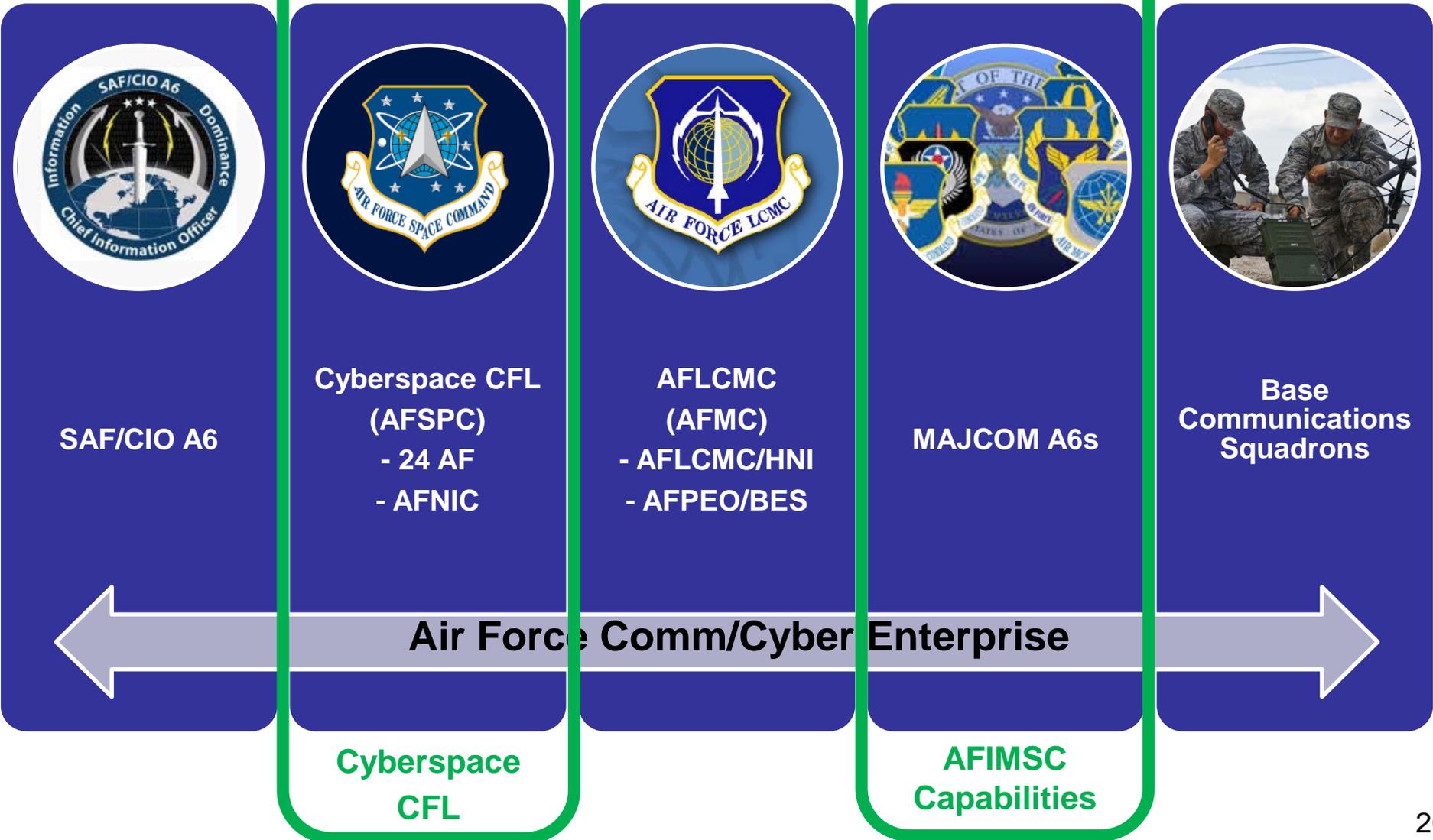


AFIMSC Defined: The Air Force Installation and Mission Support Center serves as the *single intermediate-level headquarters staff* supporting AF-wide installation and expeditionary support activities





Communications/Cyber Organizations Prior to the AFIMSC





PAD 14-04 Communications Capabilities Assignments

Transferred To AFIMSC (12 Capabilities)

COM.01	Functional Area Manager (FAM)	XZR
COM.03	Develop, Manage, & Maintain UTCs	XZR
COM.05	C&I System Maintenance	IZSS
* COM.06	Records/Pubs & Forms Management	IZSI
COM.07	Privacy Act	IZSI
COM.08	FOIA Services	IZSI
* COM.09	Long Haul Communications	IZSS
COM.11	Transmission Systems	IZSS
* COM.12	Cyber Force Tng Mgmt	XZT
* COM.13	Info Assurance Assessment	IZSS
* COM.14	IA-Command COMSEC Mgmt	IZSS
COM.15	E&I workplan	IZBT

* PAD 07-08 previously consolidated these capabilities under AFSPC

Transferred To AFIMSC Dets (8 Capabilities)

COM.02	MAJCOM Functional Manager (MFM)
COM.04	Officer/enlisted force development advice to DT and DDT
COM.18	E&I Contracting
COM.23	MAJCOM CONUS Official Mail & Postal Ops Manager**
COM.28	Advocates MAJCOM's resource needs
COM.29	Functional oversight of cyberspace workforce
COM.30	Cyber Infrastructure Planning System Mgt
COM.41	Resources (Specific to AFMC: HQ AFMC A6/7 Resources)

** Official Mail and Postal Ops are integrated capabilities/units.

Retained At MAJCOMs (20 Capabilities)

COM.16	AFFOR Support
COM.17	CIO responsibilities
COM.19	Certification & Accreditation
COM.20	Network Operations
COM.21	Spectrum Management
COM.22	NDO, GS, & NC3 mission support
COM.25	COCOM Support
COM.26	Contingency Ops planning and support (includes spectrum SMEs and MCCCs)
COM.27	Exercise planning and support
COM.31	Air Force NIPR/SIPR DAA/AFSPC Enterprise Network Operations/Cyber Security
COM.32	Overhead
COM.35	Overseas Postal & Official Mail Manager**
COM.36	Classified Message Incident Handling
COM.37	Cyber Modernization
COM.38	MAJCOM Unique applicator
COM.40	MAJCOM unique services
COM.42	Enterprise Info Systems Management
COM.43	Direct Support to CFL
COM.44	Airfield Systems
COM.45	Global Force Management (For ACC: GFM Ops Center Functional Area)

40 Total Capabilities

* NOTE: Reference #'s not consecutive due to 5 capabilities deleted by MAJCOMs from initial list



Communications Capabilities Assignments

Transferred To AFIMSC (7 Capabilities)

COM.01	Functional Area Manager (FAM)	XZR
COM.03	Develop, Manage, & Maintain UTCs	XZR
COM.05	C&I System Maintenance	IZSS
COM.07	Privacy Act	IZSI
COM.08	FOIA Services	IZSI
COM.11	Transmission Systems	IZSS
COM.15	E&I workplan	IZBT

Transferred To AFIMSC Dets (8 Capabilities)

COM.02	MAJCOM Functional Manager (MFM)
COM.04	Officer/enlisted force development advice to DT and DDT
COM.18	E&I Contracting
COM.23	MAJCOM CONUS Official Mail & Postal Ops Manager
COM.28	Advocates MAJCOM's resource needs
COM.29	Functional oversight of cyberspace workforce
COM.30	Cyber Infrastructure Planning System Mgt
COM.41	Resources (Specific to AFMC: HQ AFMC A6/7 Resources)

Retained at Cyberspace CFL/AFSPC* (5 Capabilities)

COM.06	Records/Pubs & Forms Management
COM.09	Long Haul Communications
COM.12	Cyber Force Tng Mgmt
COM.13	Info Assurance Assessment
COM.14	IA-Command COMSEC Mgmt

Retained At MAJCOMs (20 Capabilities)

COM.16	AFFOR Support
COM.17	CIO responsibilities
COM.19	Certification & Accreditation
COM.20	Network Operations
COM.21	Spectrum Management
COM.22	NDO, GS, & NC3 mission support
COM.25	COCOM Support
COM.26	Contingency Ops planning and support (includes spectrum SMEs and MCCCs)
COM.27	Exercise planning and support
COM.31	Air Force NIPR/SIPR DAA/AFSPC Enterprise Network Operations/Cyber Security
COM.32	Overhead
COM.35	Overseas Postal and Official Mail Manager
COM.36	Classified Message Incident Handling
COM.37	Cyber Modernization
COM.38	MAJCOM Unique applicator
COM.40	MAJCOM unique services
COM.42	Enterprise Info Systems Management
COM.43	Direct Support to CFL
COM.44	Airfield Systems
COM.45	Global Force Management (For ACC: GFM Ops Center Functional Area)

40 Total Capabilities

* NOTE: Reference #'s not consecutive due to 5 capabilities deleted by MAJCOMs from initial list

* PAD 07-08 previously consolidated these capabilities under AFSPC



AFIMSC Capability Delivery

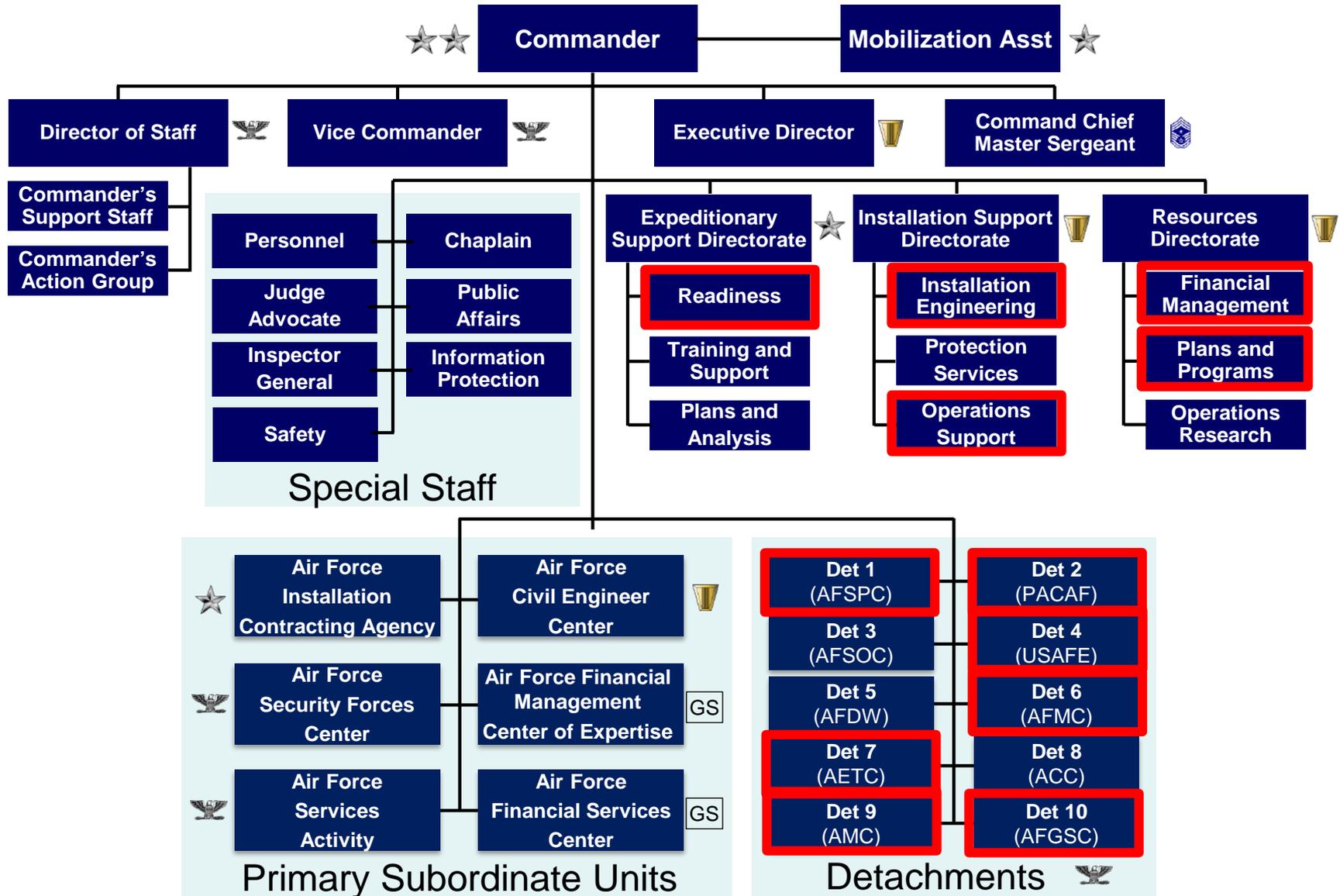
The capability areas are comprised of common services and are the focus areas for AFIMSC's BPR activities

AFIMSC Capability Delivery

AFIMSC Enterprise Operations	Installation Management	Protection Services	Installation Operations	Expeditionary Support
Resourcing	Planning	Integrated Defense	Communications	AEF & Readiness
Center Operations			Logistics (Deployments & Distribution)	
Audit	Execution	Emergency Services (Fire, EOD, & EM Career Field)	Support for Airmen & Families	
Assessment				



Communications at AFIMSC





Comm Capabilities at AFIMSC HQ

COM.01	Functional Area Manager (FAM)	Provides functional area management of the GFM process in direct support of ACC's GFM responsibility.	Expeditionary Spt Div Readiness Branch (XZRR)
COM.03	Develop, Manage, & Maintain UTCs	Oversees aggregate deployment capabilities for MAJCOM units/bases.	Expeditionary Spt Div Readiness Branch (XZRR)
COM.05	C&I System Maintenance	Consolidates, develops, interprets, and disseminates system management and guidance.	Comm/Cyber Spt Branch (IZSS)
COM.07	Privacy Act	Establishes policies necessary to implement and enforce the Air Force privacy program.	Information Access Branch (IZSI)
COM.08	FOIA Services	Provides assistance in the coordination of the release or denial of records requested under the Freedom of Information Act (FOIA).	Information Access Branch (IZSI)
COM.11	Transmission Systems	Performs radio frequency (RF)-related workload (e.g., execution of Personal Wireless Communications Systems [PWCS], cable and antenna activities).	Comm/Cyber Spt Branch (IZSS)
COM.15	E&I Workplan	Consolidate, validate, prioritize, manage and advocate for AF, MAJCOM and Installation EI WP requirements. Establish EIGS approved EI Work Plan for the execution of EI funds annually.	Technical Analysis Branch (IZBT)



Comm Capabilities at AFIMSC Dets

COM.02	MAJCOM Functional Manager (MFM)	Interfaces with Cyberspace Support Squadron (CYSS) on equipment and training status and issues affecting bases within the MAJCOM
COM.04	Officer/Enlisted Force Development Advice to DT and DDT	Provides advice on force development matters
COM.18	E&I Contracting	Provides oversight of EI implementation plan, including reach back and response to RFIs. (Includes some project management for Det 2).
COM.23	MAJCOM CONUS Official Mail and Postal Ops Manager	Provides CONUS Official Mail guidance to the Installation Official Mail Manager (OMM) who oversees all aspects of official mail, to include postage, public law (PL), base-wide distribution.
COM.28	Advocate's MAJCOM's resource needs	Plans and advocates for funding for needed capabilities/updates/modernizations
COM.29	Functional oversight of cyberspace workforce	Manages billets and manning/qualifications of workforce
COM.30	Cyber Infrastructure Planning System Mgmt	Ensure and validate base generated EI Work Plan requirements are documented properly in CIPS and included as part of the AF EI Work Plan.
COM.41	Resources (Specific to AFMC)	POM, ACS, Manpower, HR, Awards, PEC Managers (Specific to AFMC includes CFLI)



Capabilities Provided by Other Organizations

Capability	Organization / POC
DoD-level Functions/Systems (e.g., DTS, DEERS)	System PM/EA
AF-level Policy Creation	SAF/CIO A6
Leadership of JIE or Pathfinder Efforts	SAF/CIO A6 & Cyber CFL
Cyber Operations (e.g., OCO, DCO-RA)	AFSPC, USCYBERCOM
AFWAY	AFPEO/BES
BITI	AFLCMC/HNI
Life Cycle Management	AFLCMC
MAJCOM-Specific Systems / Functions (e.g., NC3 systems, satellite control systems, RPA systems, AOC, etc.)	MAJCOM/A6, NAF/A6
Base-level Communications Support (e.g., help desk, touch maintenance, asset management)	Base Comm Squadron



AFIMSC Funds Transfer

- **A6 Tiger Team determined 6 capabilities & associated x550 funding to transfer to AFIMSC in FY18 POM**
 - LMR/ELMR, Microwave Systems, Cable Antenna Systems, Back-up power Environmental Systems, Voice Systems, and Mail Management
 - All other communications capabilities remain at MAJCOMS
- **ZBT transfers \$173M across FYDP of Active O&M – Non Civ-Pay dollars (FY18-23)**
 - Base COMM is broken program, 50% disconnect across FYDP
 - Proposed ZBT does not fix any programs
- **AFIMSC will need to work with MAJCOM/A6s to address FY17 C&I requirements**



Milestones / Way Ahead

- 25 Feb 2015 PAD 14-04 Approved by SecAF/CSAF
- 5 May 2015 AFIMSC Activation
- 1 Oct 2015 AFIMSC Initial Operational Capability
- 2 Dec 2015 PAD 14-04 Annexes Approved
- **May 2016 PPLAN Functional Coordination**
- **Jun 2016 PPLAN HAF 3-Itr/MAJCOM 2-Itr Coord**
- **1 Oct 2016 AFIMSC Full Operational Capability**





Base Comm Items Transferring

■ Annex H: Command, Control, Communications, and Computers

Capabilities Transferring to AFIMSC	Related Base Comm Items per Tiger Team	EEICS
LMR/ELMR	Enterprise LMR, LMR Trunking Systems, ELMR Zone Core (hand helds not included)	44300
Microwave Systems	Microwave Systems	44200
Cable/Antenna Systems	Cable Infrastructure	44200
Cable/Antenna Systems	Base Cable Plant Repair	63770
Cable/Antenna Systems	Outside Plant Contract	44200
Cable/Antenna Systems	Cable & Antenna Maintenance	63780
Back-up Power and Environmental Systems	Uninterrupted Power Supplies (UPS) Maintenance	53390
Voice System (Legacy Voice/TDM)	Legacy Voice (TDM)	44200
Official Mail Management (note:Annex H, 5.4.18 includes Postal Service Centers (PSC) contract oversight).	All CONUS Postal funding (Official Mail and PSC mail) [Does not apply to PACAF or USAFE]	44600
Supports the other Comm Items on this list	Benchstock and Maintenance Items (for which AFIMSC is responsible)	63770



MAJCOM Retained Capabilities

- Tiger Team derived these capabilities from PAD 14-4 Communications Capability Library

Capabilities Retained at MAJCOMS
Network Operations
Help Desk
Cyber Incident Management
Storage Networks / Data Centers
Unified Capabilities (UC)
Voice over IP (VoIP)
Joint Information Environment (JIE)
Video Teleconferencing
SharePoint
Software Development and Maintenance
Task Management Tool (TMT)
Emergency Management Notification Systems
Toll Charges, Cellphones, Mobile Satellite Services, Cable TV
Overseas Postal



AFIMSC

Organizing purpose & principles

- **HQ AFIMSC provides**
 - Analytical support for evaluating cross-functional, enterprise-wide I&MS effectiveness/efficiency
 - I&MS resources through PPBE processes
 - Senior expert guidance and policy interpretation
 - Clear communications and accountability control
 - Coordination and integration of I&MS activities across the AF
- **Detachments provide**
 - Responsive synchronization and management of AFIMSC assets to address MAJCOM-specific I&MS priorities/concerns
 - Proactive solutions to emergent requirements
 - Issue resolution at the lowest level
- **PSUs provide**
 - Project and program management
 - Subject Matter Expertise and services

* NOTE: There is no PSU for Communications at this time

Organizational design principles: Minimize pass-throughs, drive decision making to lowest appropriate level to maximize responsiveness, operate at speed of trust



U.S. AIR FORCE

UNCLASS

Headquarters U.S. Air Force

AF-Wide Deployment of Windows 10

**Lt Col Michael Furman
JIE Action Officer
SAF/CIO A6SE
27 April 2016**

Integrity - Service - Excellence



U.S. AIR FORCE

Win 10 Requirement

- **Maintenance upgrade to Win 10 across AF Info Network (AFIN)**
- **DEPSECDEF-directed effort to improve cybersecurity on all clients**
 - **Protects internal storage of passwords and credentials**
 - **Eliminates malware on client start up**
 - **Ensures only trusted device drivers are used**
- **Win 10 mandate covers the entire DoD**
 - **Covers all classifications (intel owners cover intel clients)**
 - **Includes office workstations, tablets, platform IT, special access programs and standalone systems across every functional area**



U.S. AIR FORCE

AF Win 10 Solution

- **SECAF direction is to “Transform AF for Mobility/Security” by Jan 18**
 - **Replace most non-compatible systems with laptops & tablets**
 - **Upgrade existing systems capable of accepting Win 10**
 - **Field virtual desktop infrastructure on AF classified domain first**
 - **Expand on existing unclassified virtualized infrastructure**
- **PROS:**
 - **Strategic opportunity to put AF on a transformational path**
 - **Fixes existing issues with classified domain**
 - **More cost effective over long term (4+ years); most flexible option**
 - **Aligns with DoD CIO Data Center Consolidation Initiatives**
- **CONS:**
 - **Relies heavily on scaled robust infrastructure**

Integrity - Service - Excellence



U.S. AIR FORCE

Functional and Program Management Systems

- **Partner with acquisition and functional communities on process for addressing greatest need first**
- **SAF/AQ sent out a data call to assess magnitude across PMO systems**
 - **Applicability of Win 10 SHB and cost**
 - **System and Mission risk of Win 10 security features**
- **Develop Mitigation Strategy**
 - **Develop risk-based prioritization grounded on data call**
 - **Work through system waiver process**
 - **Program managers develop Win 10 plan of action and milestones**



U.S. AIR FORCE

Way Ahead

- **Implementation of Win 10 upgrade for unclassified and classified networks is underway**
- **Strategic opportunity to improve mission effectiveness by making Airmen more mobile and through innovation**
- **Proceeding with virtualization for Win 10 migration**
 - **CIO A6, AF Space Command, Financial Management and AF/A5-8 working trades for FY16/17 funding**
 - **Technical team continuing to architect transformation**
- **Need MAJCOM assistance for remainder of AF network migration:**
 - **Acquisition and program offices must rapidly identify what needs to be upgraded and can be upgraded**
 - **Leaders must approach solutions using risk analysis framework**

Integrity - Service - Excellence



Headquarters U.S. Air Force

Integrity - Service - Excellence

Task Force Cyber Secure Spring Update 2016



**Colonel Bill “Data” Bryant
Task Force Cyber Secure
Deputy Director**

U.S. AIR FORCE

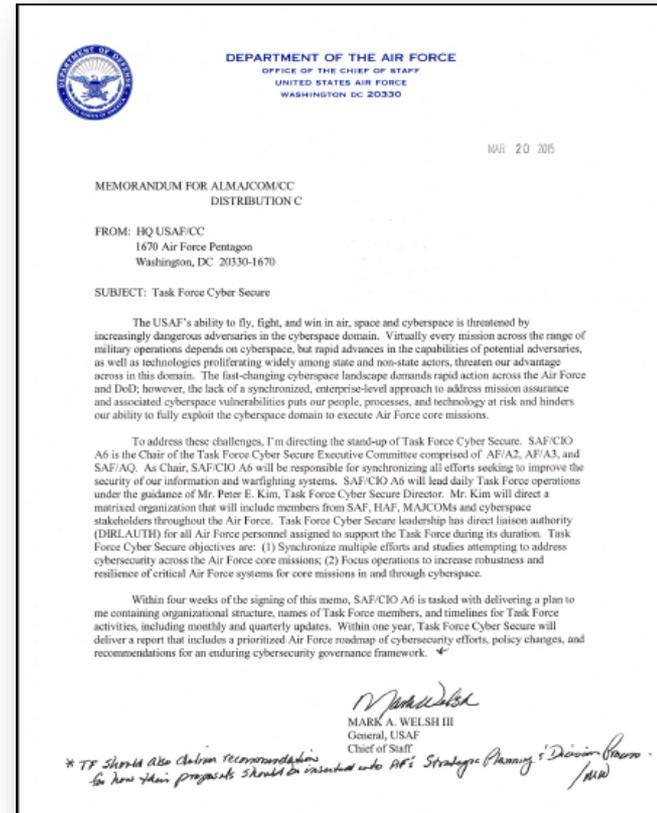


Task Force Objectives

U.S. AIR FORCE

CSAF Memo

- Synchronize multiple efforts and studies attempting to address cybersecurity across the Air Force core missions
- Focus operations to increase robustness and resilience of critical Air Force systems for core missions in and through cyberspace



"This task force is fundamental to understanding the inherent risks within the cyberspace domain and instituting a culture change, in which our Airmen realize the impact cybersecurity has on all the Air Force core missions." (CSAF, 31 Mar 2015)



■ “Hard” Deliverables”

- Risk management strategy aligned with the Risk Management Framework—will be part of the CISO strategy
- Enduring Framework—includes CISO, governance, and funding
- Insertion of proposals into SP3 process—handwritten in by CSAF

■ “Soft” Deliverables

- Cross functional dialogue
- Diagnosis of the problem
- Education and culture



U.S. AIR FORCE

TFCS Background

- Our missions are dependent on the cyberspace domain
- Our systems were designed for a different world
 - Implicit assumption of a permissive cyberspace environment
 - Network defenses sufficient if any
- The presence of a maneuvering enemy in cyberspace requires a different approach
- This isn't an IT problem, it is a mission problem



Mission Assurance Focus

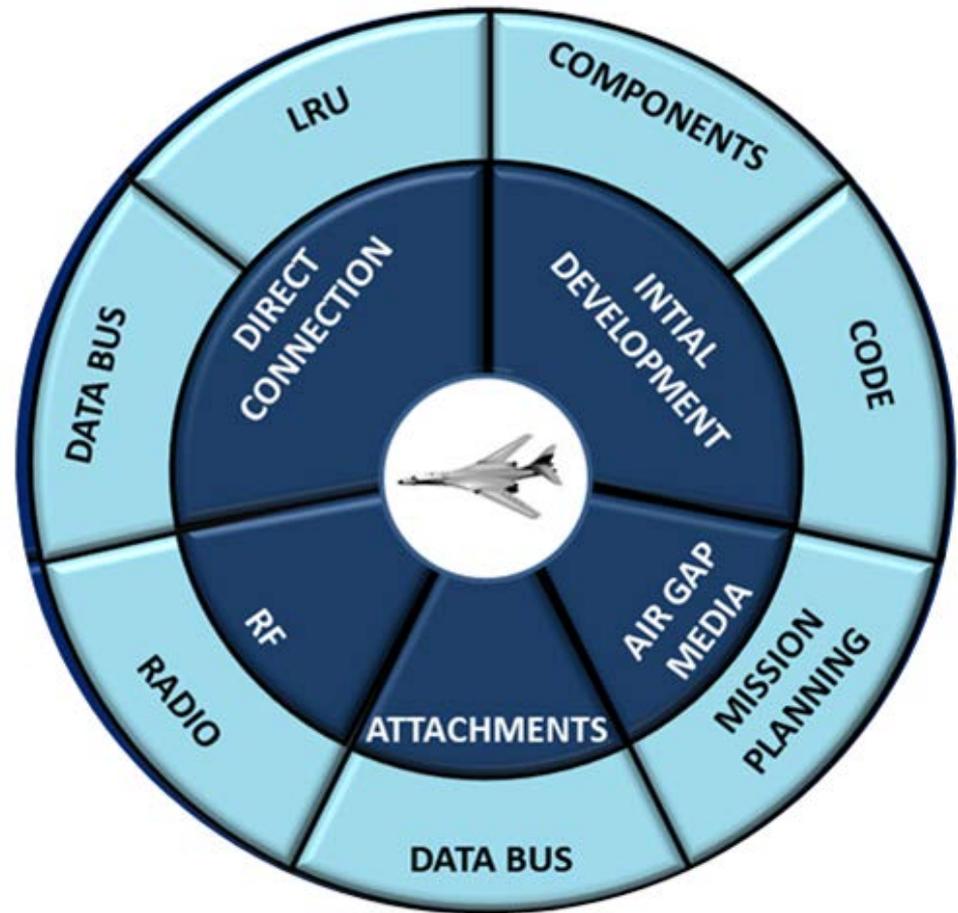
Integrity - Service - Excellence



AF Cyber Physical Systems

U.S. AIR FORCE

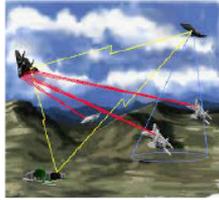
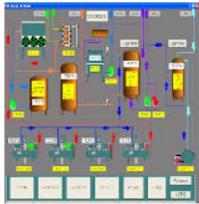
- Modern systems exist in both the physical and cyberspace domains
- Numerous pathways into vast number of systems
- Vulnerabilities change constantly—cannot fix and walk away
- Start by determining what is most important





Determine Key Cyberspace Terrain

U.S. AIR FORCE

	Traditional IT	Operational Technology	Platforms
Mission-Level			
System-level			
Component-level			

Our focus has been on the “lower left” of IT and components but needs to move to the “upper right” of weapons systems and missions

**OT = Operational Technology – Computer controlled physical processes such as ICS (i.e. power, water) logistics (i.e. fuel systems) or other control systems (i.e. building automation, security alarms)*

Integrity - Service - Excellence



U.S. AIR FORCE

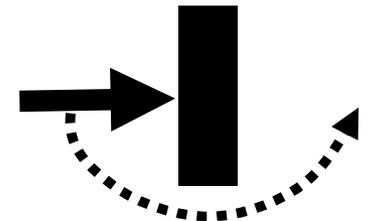
Problem

- Different communities see cyberspace through very different lenses based on their organizational culture and experience



- Traditional IT communities focus on defense in depth
 - Compliance and security emphasis

- Acquisition communities focus on how to build in resilience
 - Adaptable and resilient system emphasis



- Cyber operations communities focus on detection and response
 - Cyberspace maneuver emphasis



U.S. AIR FORCE

Solution

- All three approaches are needed and support each other



- Make it difficult for an enemy to stay
- Make it difficult for an enemy to achieve objectives
- Make it difficult for the enemy to get access

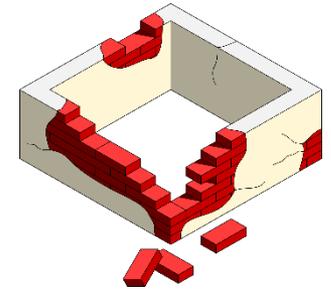
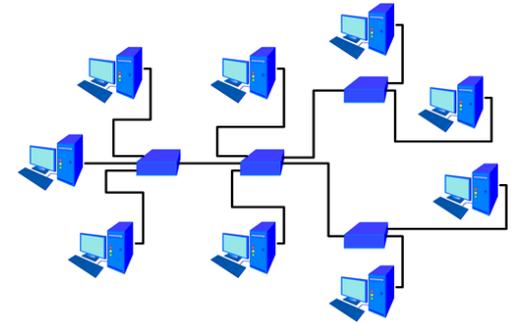
Integrity - Service - Excellence



U.S. AIR FORCE

Defense in Depth

- Most defenses are IT based and technical
 - Firewalls
 - Intrusion Detection and Prevention Systems
 - Blacklisting/Whitelisting
 - Etc.
- Static defense is necessary but not sufficient
 - Dynamic attackers will always find a way in
 - “Airgaps” are mostly mythical



- Cyber physical systems need their own defenses and should not rely on the network



U.S. AIR FORCE

Resiliency

- Network and system engineers should plan for enemy success and expect it, avoid single points of failure and easy targets



or



- Resilience in cyberspace may lay outside of cyberspace
 - Tactics, Techniques, and Procedures
 - Alternate systems
- Getting the mission done while under attack
 - Mission Assurance
- No chance of success unless the above options are routinely and realistically exercised



Active Defense

U.S. AIR FORCE

- **Monitoring and response inside the friendly network by defenders, not “hack-backs”**
- **Organizations serious about their cybersecurity in the IT world (i.e. banks) are already doing it**
 - **Must extend the concept into cyber physical systems**
 - **Mission analysis needed to identify where to defend**
- **Traditional IT systems are well understood, Operational Technology and platforms are not; issues include:**
 - **Specific obscure protocols**
 - **Performance impacts**
 - **Added attack surface**
- **Start by defending traditional IT networks around platform**



U.S. AIR FORCE

TFCS Framework

- **Cyberspace reliant systems are essential to mission success**
- **The best way to effectively defend both IT based, and cyber physical systems is through a combined approach**



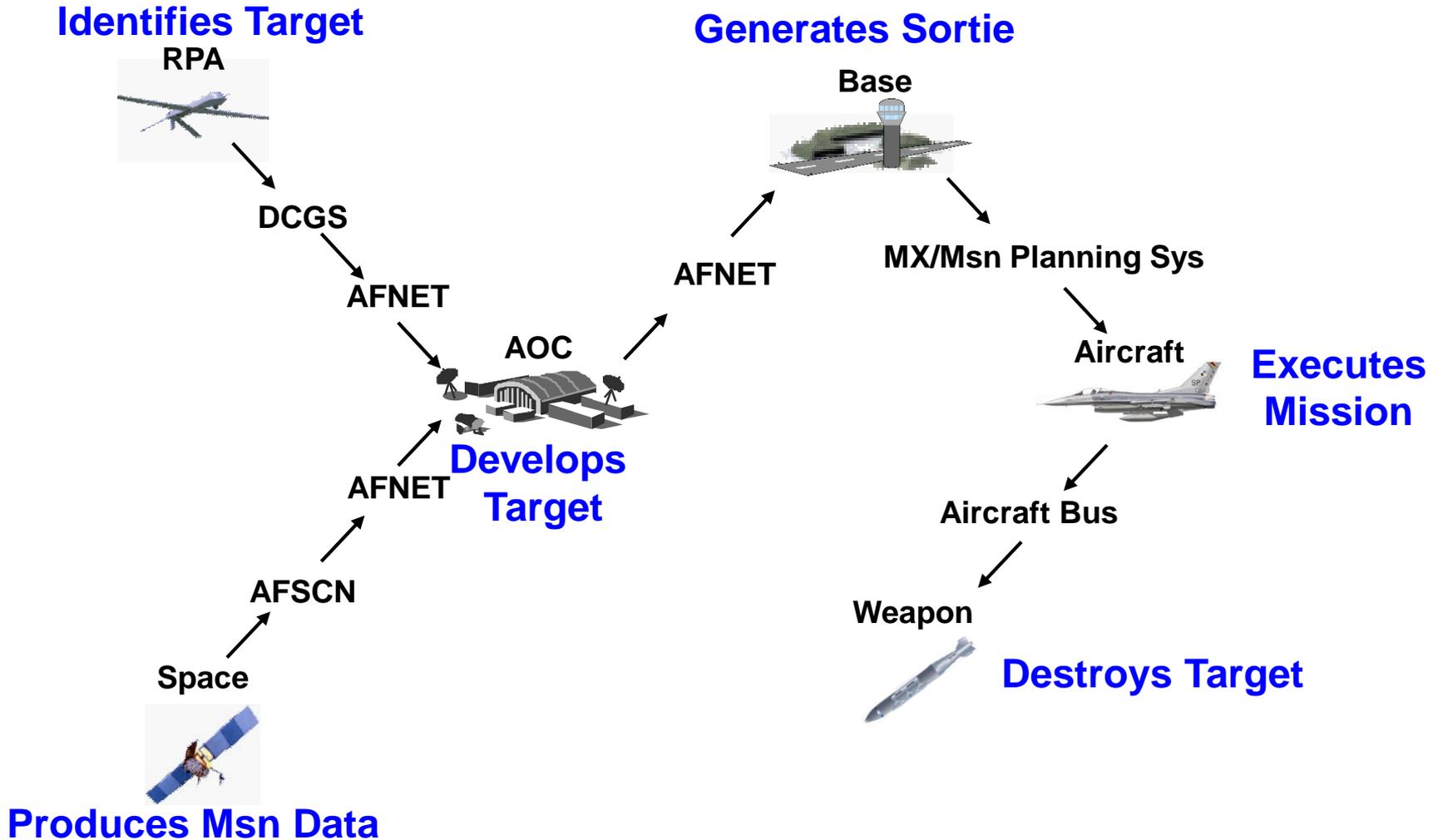
- **Find and respond to enemy forces**
- **Mission assurance so that enemy objectives are not accomplished**
- **Provides initial defense and blocks most attacks**

Integrity - Service - Excellence



Simple AF Mission Example

U.S. AIR FORCE

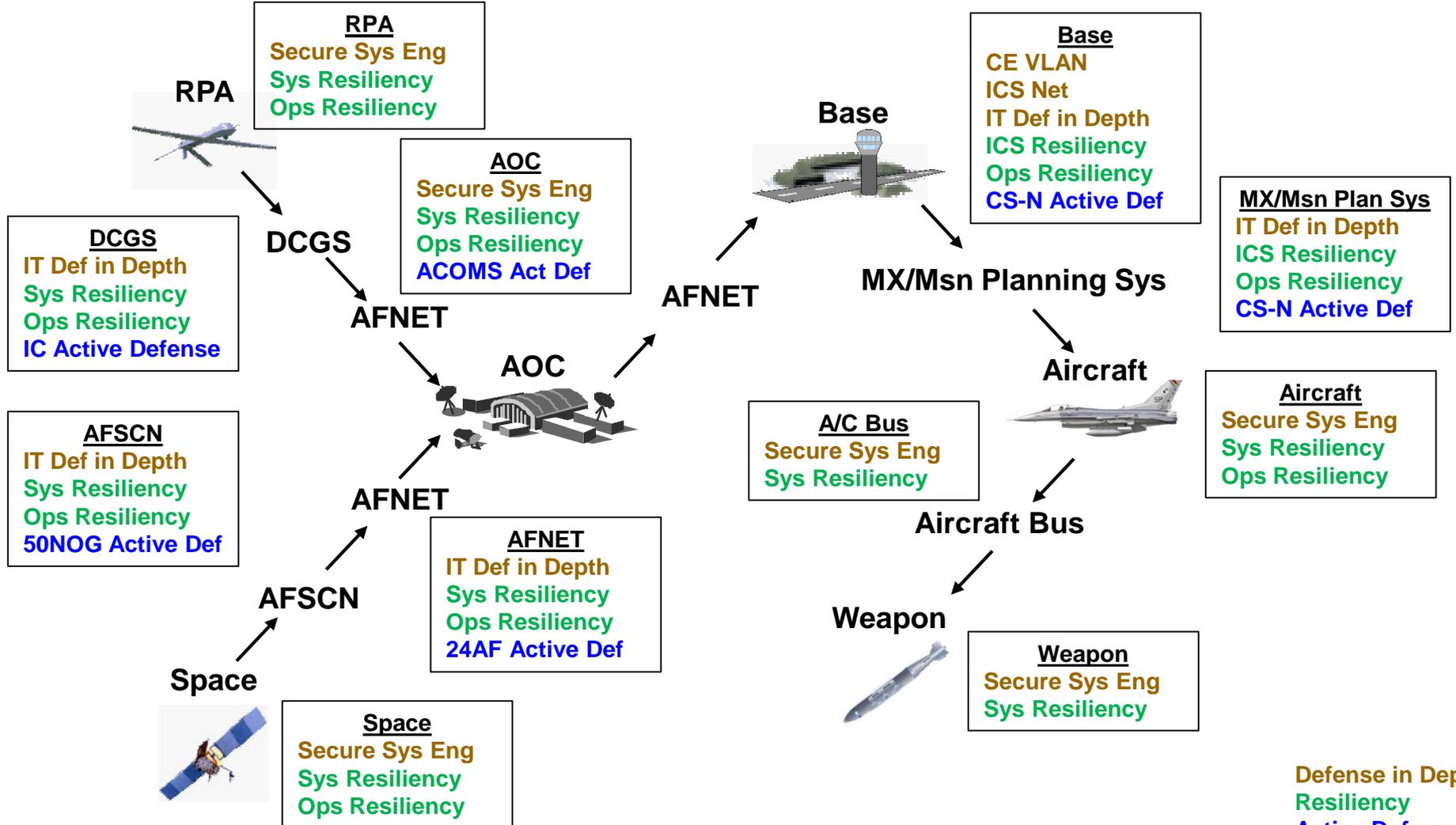


Integrity - Service - Excellence



Simple AF Mission Example

U.S. AIR FORCE



Defense in Depth
Resiliency
Active Defense



Early Draft Recommendations

U.S. AIR FORCE

- Issue 1 – The Air Force structure is not currently optimized to manage cyber risk at the enterprise level
- **Recommendation 1 – Stand up a Chief of Information Security Officer (CISO) and organization at the right level with sufficient staff to manage AF enterprise cyber risk (POC: CISO)**
- Issue 2 – Roles and lanes in defense and mission assurance of weapons and mission systems in cyberspace are unclear
- **Recommendation 2 – Produce a CSAF memorandum that lays out responsibilities and roles for defending and providing mission assurance of weapons and mission systems in cyberspace (POC: CISO)**
- Issue 3 – Legacy organizational structures in the communications/cyberspace world were built to support DODIN operations, not defense and mission assurance in and through cyberspace
- **Recommendation 3 – The Air Force should realign communications squadrons and shift their focus from exclusively IT provisioning to also accomplish defense and mission assurance in and through cyberspace (POC:CIO)**



Early Draft Recommendations

U.S. AIR FORCE

- Issue 4 – Control system cybersecurity is not centrally managed, but is fragmented into functional areas
- **Recommendation 4 – Assign enterprise level management of the cybersecurity of AF control systems to IMSC (POC: IMSC)**
- Issue 5 – The current cyberspace acquisition process is not agile enough to support operational missions in the cyberspace domain
- **Recommendation 5 – Create an Air Force Innovation Team empowered to fully leverage existing authorities to pursue rapid acquisition of innovative cyberspace capabilities (POC: CIO)**
- Issue 6 – The current system for funding cyberspace defense and mission assurance relies on unfunded requests and is slow to adjust for the rapid pace of change in cyberspace
- **Recommendation 6 – Establish and protect funding to create an agile environment to address emergent AF enterprise-wide cybersecurity requirements (POC: CIO)**



Early Draft Recommendations

U.S. AIR FORCE

- Issue 7 – Cyberspace effects are difficult to bring to bear in support of the AF core missions due to clearance issues and the separation of cyberspace operators from warfighter in other domains
- **Recommendation 7 – Stand up a cyberspace operations flight within Operations Support Squadrons to integrate cyber effects into the local wing’s mission (POC: A3)**
- Issue 8 – Key cyberspace terrain is not centrally analyzed or managed
- **Recommendation 8 – Mission thread work should continue and the results need to be centrally collected and placed into an overall enterprise level system to prioritize key cyber terrain (POC: CISO)**
- Issue 9 – There is currently no easy way to access cyberspace vulnerabilities of weapons and mission systems across the enterprise
- **Recommendation 9 – Create a secret level ACCM to contain vulnerability information collected from the programs that is controlled by AFMC (POC: AFMC)**



Early Draft Recommendations

U.S. AIR FORCE

- Issue 10 – Different communities within the AF have different concepts of what is inside, and outside, of the Air Force Information Network (AFIN) as well as who is responsible for defending the AFIN
- **Recommendation 10 – Revise AFI 10-1701 to clarify the precise boundaries of the AFIN as well as who has command and control of both AFIN and those areas of cyberspace determined to be outside the AFIN boundary (POC: A3)**
- Issue 11 – A lack of cyber-awareness in AF culture is hampering our cyberspace defense and mission assurance
- **Recommendation 11 – Create an enterprise level Cyber Assure program to push a wide range of actions that will improve AF culture in cyberspace (POC: CISO)**



U.S. AIR FORCE

Questions

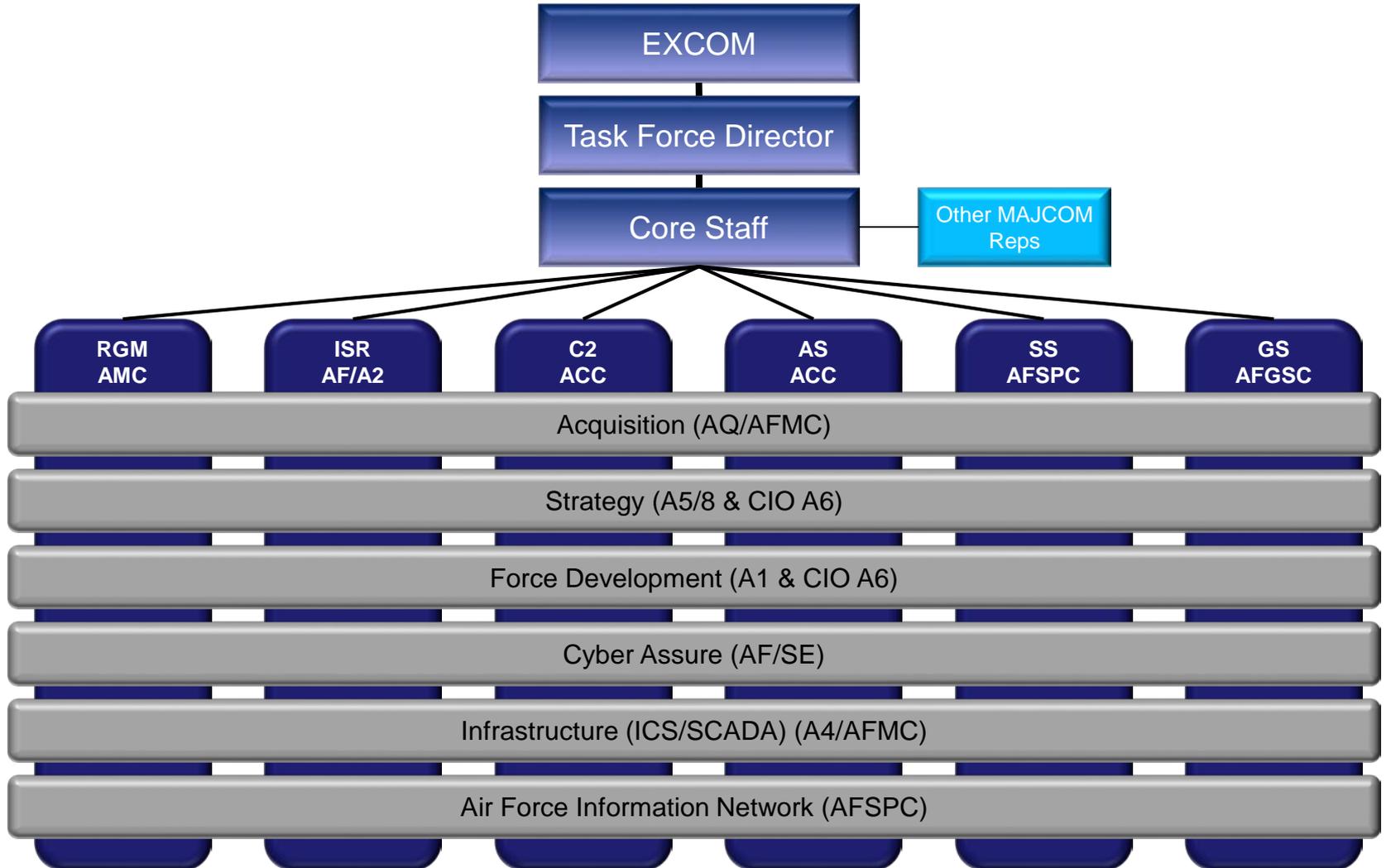


Integrity - Service - Excellence



U.S. AIR FORCE

TFCS Structure



Integrity - Service - Excellence

Headquarters U.S. Air Force

Integrity - Service - Excellence

CISO Implementation



U.S. AIR FORCE



CISO Statutory Requirements

U.S. AIR FORCE

Title 44 – CIO designates a senior agency information security officer who shall –

- **Head an office with the mission and resources to ensure agency compliance with this section**
- **Develop and maintain an agency wide information security program**
- **Develop and maintain information security policies, procedures, and control techniques to address all applicable requirements**
- **Ensure information security is addressed throughout lifecycle of systems**



U.S. AIR FORCE

CISO Functions – Carnegie Mellon

**Protect, Shield,
Defend, Prevent**



**Monitor, Hunt,
Detect**



**Respond,
Recover, Sustain**



24AF Mission

**Govern, Manage,
Comply, Educate,
Manage Risk**





Research Summary

U.S. AIR FORCE

Organization	CISO TITLE	Reports to CIO	Separate Budget	Cybersecurity Strategy/Plan
CACI	CSO	CEO	X	X
BAH	X	CEO	X	X
HPES	X	CEO	X	X
DELL	X	CSO		
MARINE CORPS	X	X		X
NAVY	X	X		
ARMY	X	X		
VA TECH	ITSO	X		
UM UNIVERSITY COLLEGE	CTO	X		
VETERANS AFFAIRS	X	X		
NSA	SISO	X		
CIA	SISO	X		

1. Industry CISOs reported directly to the CEO or equivalent, managed their own budget, and developed the cybersecurity strategy
2. MilDep CISOs reported to the CIO and the budget was a portion of the CIO budget



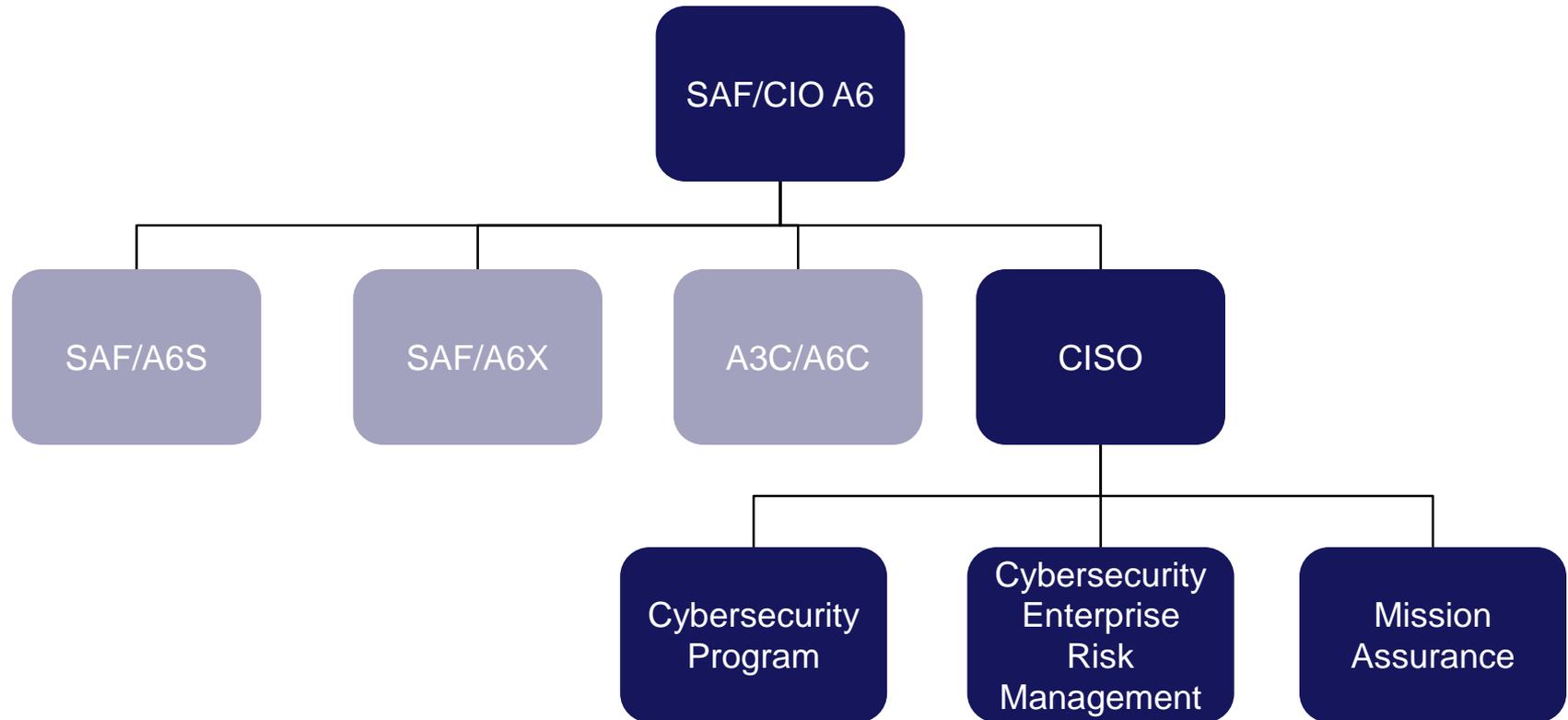
Research Findings

- **Research supports an organizational structure comparable to Services, agencies, private industry, and academia**
 - **SISO renamed to CISO (consistent with industry, DoD, and Federal)**
 - **CISO as primary role (must have a singular focus not an “additional duty”)**
 - **Direct report to CIO (consistent with MilDeps)**
 - **Cybersecurity funding (must have an operating budget and influence over mission owners execution)**
 - **Develop Enterprise Cybersecurity Plan (must establish a plan for other to follow and be measured against)**



U.S. AIR FORCE

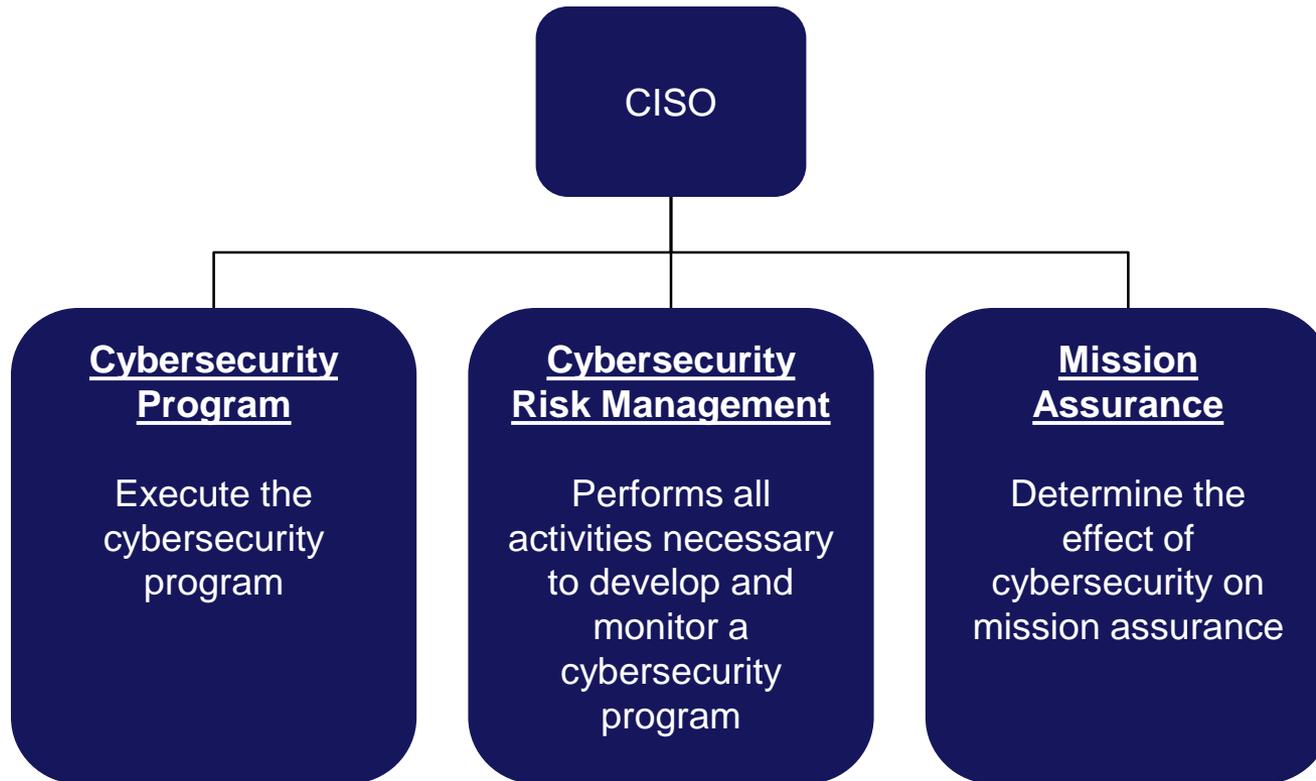
Proposed CISO Organization



CISO Direct Report to SAF/CIO A6



CISO Organization



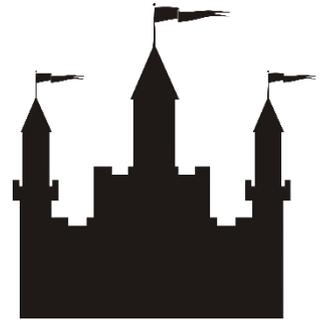
CISO must be equipped with an expert staff to execute mission regardless of placement within the Air Force structure



Defense in Depth Components

U.S. AIR FORCE

- **Border defenses make up the first layer of defense**
- **There must also be layers inside the borders**
 - **Barriers to lateral movement**
 - **Prevention of privilege escalation**
- **Reducing attack surface – easy to say, very hard to do**
- **Secure Systems Engineering (SSE)**
 - **“Baked-in” during design vs. “Bolted-on” after fielding**
 - **Has to look outside the system boundary**
 - **Design is too late, must start with requirements**

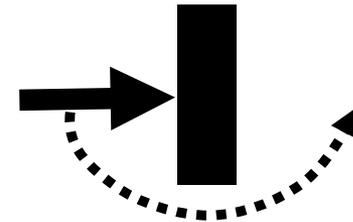




Resiliency Components

U.S. AIR FORCE

- **Build systems expecting the enemy to get in and cause damage**
 - **Create multiple mission pathways**
 - **Efficiency vs. effectiveness**
 - **Build segmentation**
 - **Embrace diversity**
- **Cost, schedule, and performance is no longer enough**
- **Must add assurance as a fourth major measure of performance**
 - **Otherwise mission assurance will fall below the cut line**
- **Leverage the human warfighter—people make this work**





Active Defense Components

U.S. AIR FORCE



- **Maneuver forces: getting the right people trained and equipped is the most important and difficult part**
 - **Operational mindset**
 - **Deep technical skills coupled with creativity and flexibility**
 - **Operational Technology/IT and platform/IT hybrids**

- **Sensors: you must first be able to find a hidden enemy**
 - **Standard IDS systems are a start, but not enough**
 - **Advanced persistent threats will generally not be seen by signature based systems**

- **Tools/weapons: once an enemy is found, what can you do about it?**



Headquarters U.S. Air Force

Integrity - Service - Excellence

Communications Squadron Next



U.S. AIR FORCE

*Lt Col Reid Novotny
Director of Staff
SAF-A6/CIO*



U.S. AIR FORCE

Mission Assurance of the Core AF Missions

- All our warfighting and support systems reside within the cyberspace domain
- Without freedom of action within cyberspace, our ability to accomplish the five core missions is threatened
- Most Air Force weapons and support systems were designed to operate in a permissive cyberspace environment
- Cyberspace is contested and the presence of a maneuvering enemy in cyberspace requires a different approach--active cyber defense

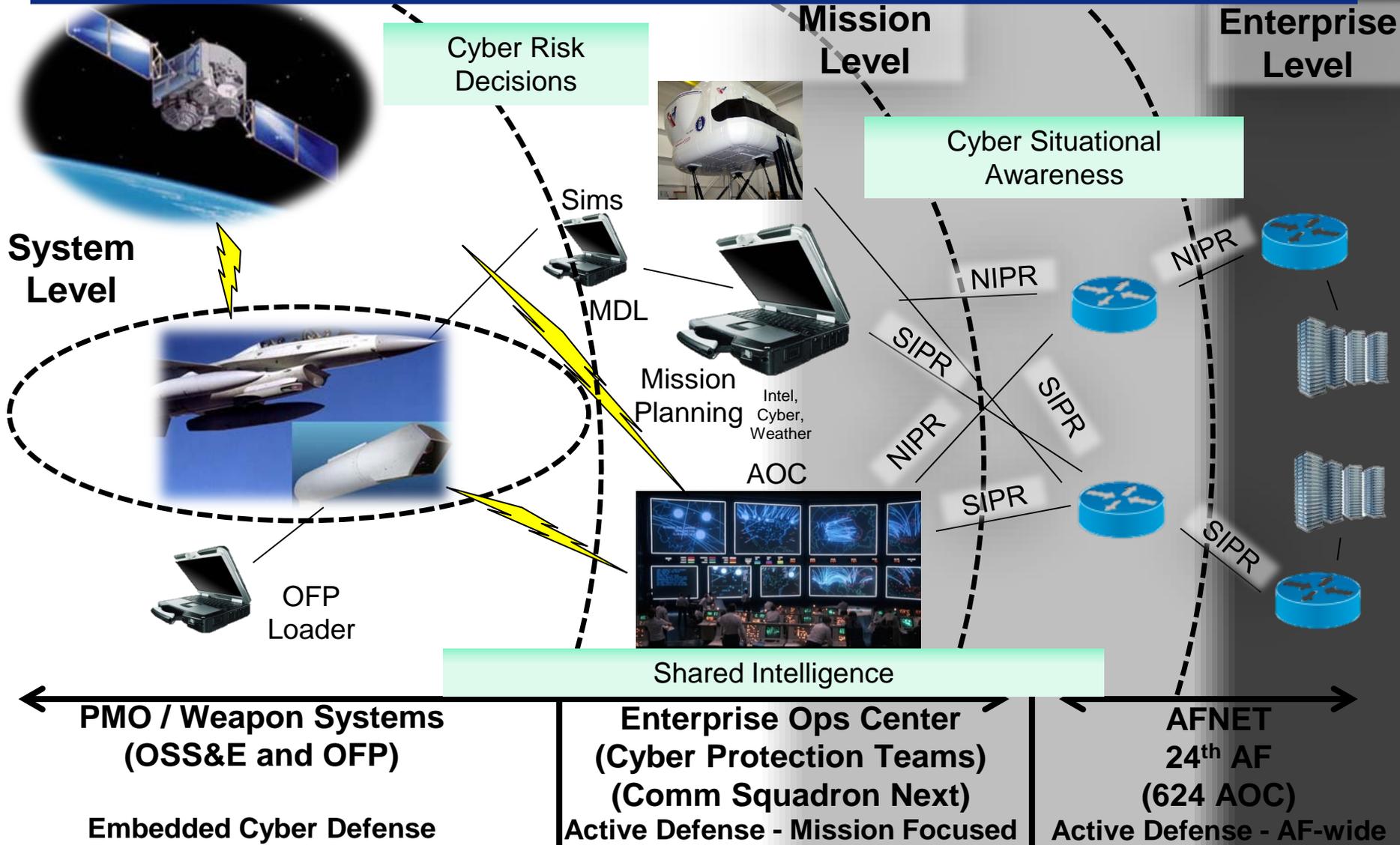


Compliance and boundary defenses are insufficient, we must shift to maneuver and “fighting through” a contested environment



Key Terrain Cyber Framework

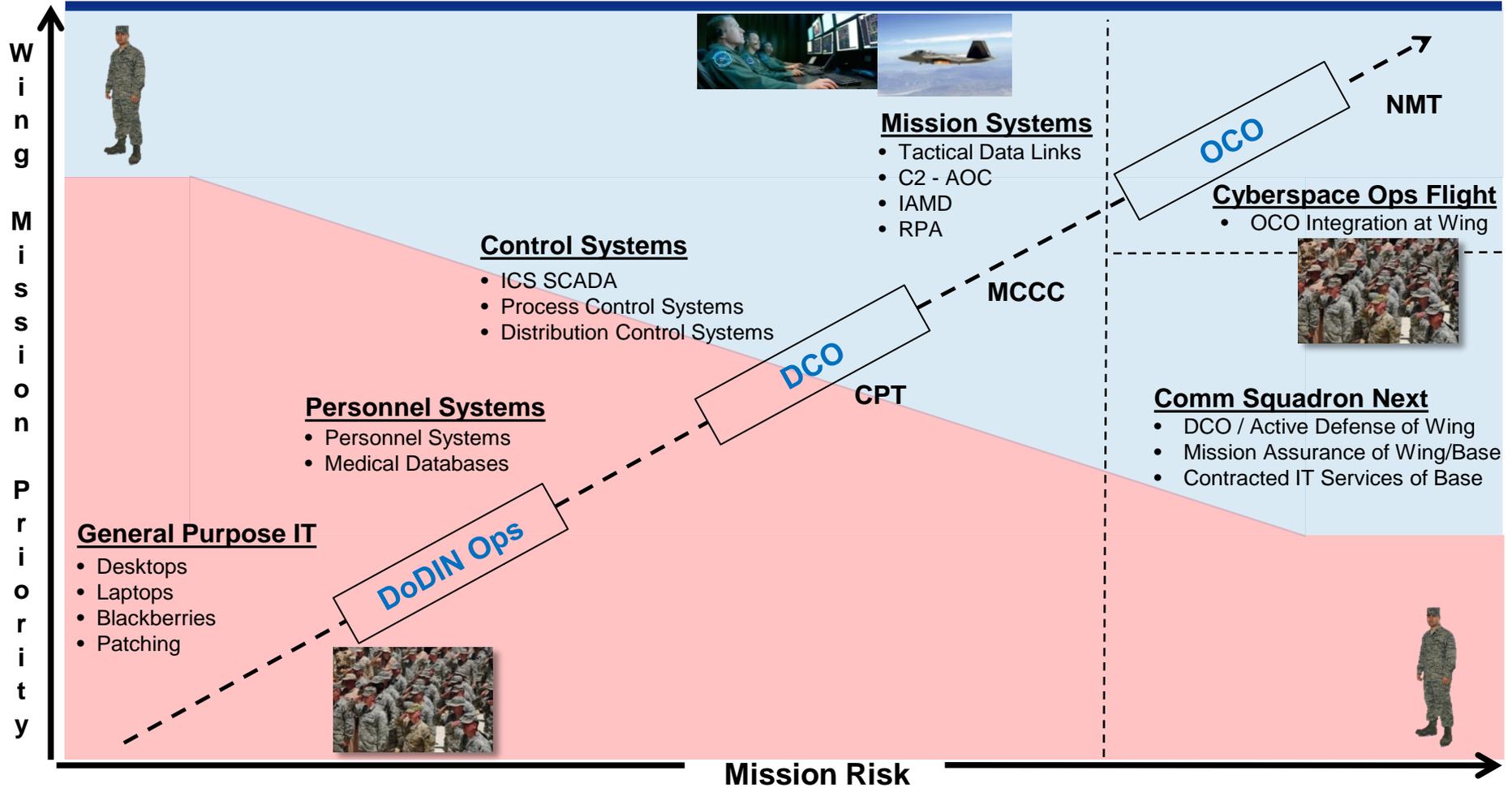
U.S. AIR FORCE





Site Picture of CS-Next Transition

U.S. AIR FORCE



Our main focus has been on IT, but freedom of maneuver in the information age demands a shift in focus to mission / weapon systems to operationalize and provide Mission Assurance.

Integrity - Service - Excellence



Transition Dependent on...

U.S. AIR FORCE

Present – Provide Service

- Customer Support
- AFNET focused
- Respond to NOSC
- Prepare for CCRI
- Organized around bases
- Missions vulnerable

Maximize Next Gen Enterprise Services

- Expand commercial services
- Outsource E-mail
- Outsource file services
- Non-assured UC
- Storage

Align w/ Enterprise Architecture

- Define core mission threads
- Determine IT services and who will provide them (NaaS)
- Focus on IT Weapon Systems
- Build EA strat and op model
- Establish cloud strategy

Reform CCRIs

Cloud
JRSS

NGeS

Complete mission analysis

- ID mission system threads
- Acquire funding for AF-wide
- Expand non-traditional IT Weapon Systems relationships
- Complete PAD
- Reorganize forces to meet mission

Initial Enterprise Solutions

- Conduct cloud pilots
- Integrate TFCS solutions
- Evaluate Tool solution
- Gain resources to establish EA framework

T
O
D
A
Y

FMA Pilot Tools

Transition IT Service Delivery

Pathfinder IOC

- Conduct tool training
- Tool funding acquired
- Update training/processes based on mission threads
- Establish critical relationships
- Incrementally increase functionality
- Finalize FMA/DCO processes

Draft PAD

Stand-up PROTAF

Pathfinder FMA

- Dec 15 – Jun 16
- Train and Conduct FMA
- Train on DCO processes
- Establish mentors
- Critical relationships ID'd
- Outbrief mission owner

Future – Assure Mission

- Mission Mapping
- Vulnerability Analysis and Hunting
- CPT maneuverability
- Malware analysis
- Signature development
- CounterIntel & OSI

Phase 1

Phase 2

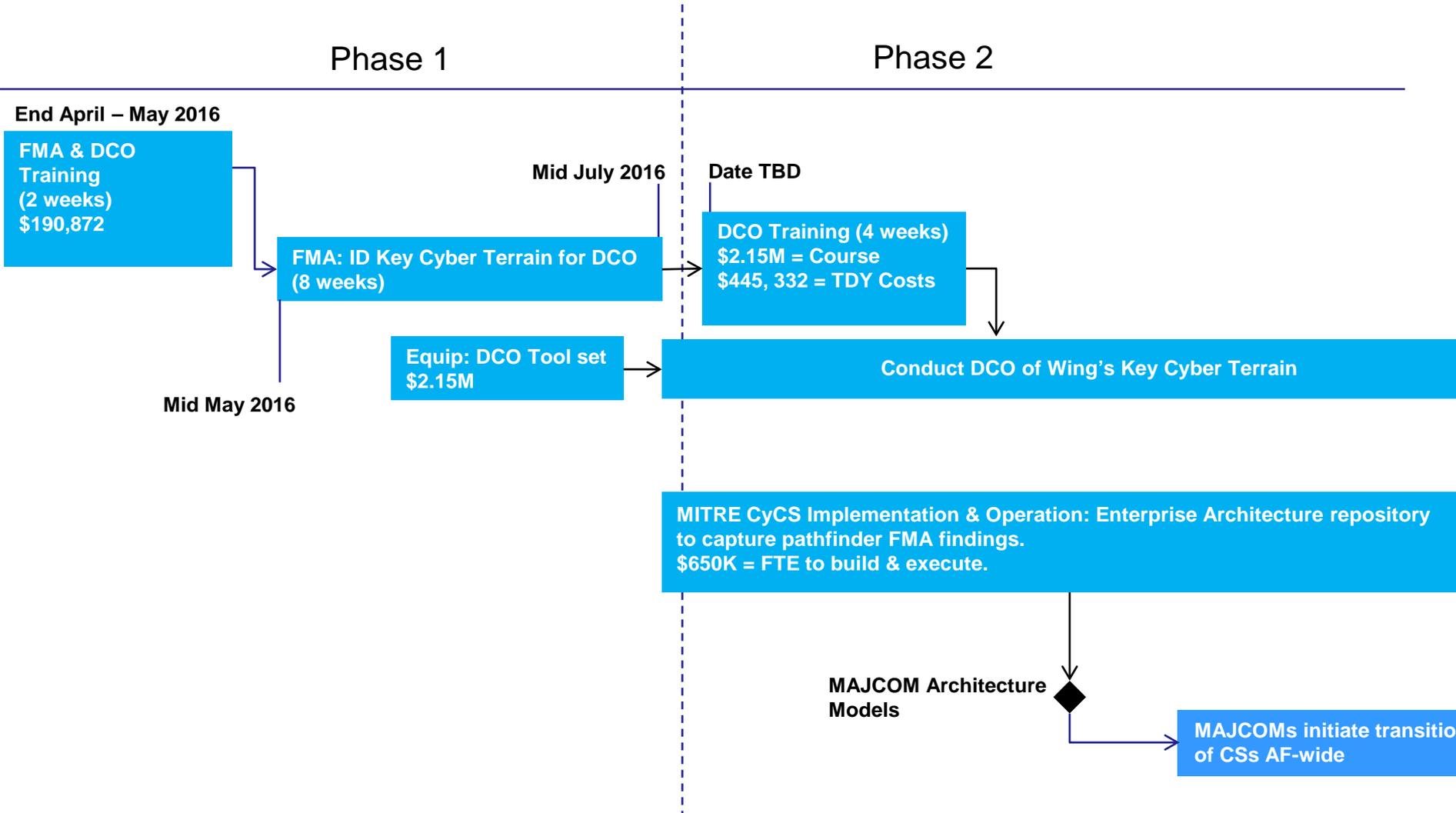
Phase 3

Integrity - Service - Excellence



Pipeline for Pathfinders

U.S. AIR FORCE



Integrity - Service - Excellence



CSN Pilot Organizations

U.S. AIR FORCE

	Unit	Location		Unit	Location
ACC	325 th CS	Tyndall AFB, FL	AFSOC	1 SOCS	Hurlburt Field, FL
AETC	42 nd CS	Maxwell AFB, AL	AMC	22 nd CS	McConnel AFB, KS
AFGSC	509 th CS	Whiteman AFB,	ANG	137 th CS / 116 th CS	Will Rogers ANGB / Robins AFB
AFMC	412 th CS	Edwards AFB	PACAF	673 rd CS/ 56 ACOMS	JB Elmendorf-Richards, AK JB Pearl Harbor-Hickam, HI
AFRC	452 nd /434 th / 482 nd /911 th /CS	March ARB, CA /Grissom ARB, ID/ Homestead ARB, FL /Pittsburgh ARS, PA	USAFE	52 nd CS	Spangdahlem AB, GE
AFSPC	50 th SCS	Schriever AFB, CO	AFDW	744 th CS	JB Andrews, MD

Funding based on 1 Sq per MAJCOM



U.S. AIR FORCE

Your Role Today

- **Transfer risk acceptance from mission systems to non-critical IT**
 - **FMA Process will inform future cyber focus**
 - **Ensure broken glass is minimized**
- **Drive CS Next Pilot organizations**
 - **Advocate comm squadrons participation in wing operations**
 - **Ensure mission analysis personnel include more than just Cyber Airmen (ops/mx/etc)**
 - **Lateral coordination for cyber intel required for success**
 - **Identify cyber capability shortfalls to include AQ community**
 - **There are DOTMLPF-P implications that require changes in the work force, organization, and institutional relationships**



U.S. AIR FORCE

50 SW Outsourcing Status (Personnel WG)

- **50 SW identified tasks for outsourcing to free up manpower for Mission Defense Teams (MDTs)**
- **50 SW using its own funds to execute**
- **Working issue through A1 channels**
 - **Clarifying actions to ensure legally feasible**
 - **Against federal law to outsource work that is currently being performed by a civilian**
 - **Moratorium against A-76 actions**
 - **Can't do a 1 for 1 military to civilian swap**
 - **Multiple civilian billet requests across the AF with limited growth forecasted**
- **ECD: 1 Jun 16**



U.S. AIR FORCE

Additional Tasks

- **Gain feedback from Pathfinders on proposed split of governmental/non-governmental tasks (Personnel WG)**
 - **AFSPC working with 50 SW and 52 FW to establish proposal**
 - **Presented to MAJCOM/A6s and pathfinder units for feedback**
 - **Will become basis of outsourcing strategy such as NaaS**
 - **ECD: 30 Jun 16**

- **Establish initial C2 construct (Ops/C2 WG)**
 - **Establish focus group to establish construct**
 - **Pathfinders, MCCCs, 24 AF**
 - **ECD: 30 Jun 16**



U.S. AIR FORCE

Backup

Integrity - Service - Excellence



Cyberspace Definitions

U.S. AIR FORCE

Active Cyber Defense - Active cyber defense is DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks. (Department of Defense [DOD] Strategy for Operations in Cyberspace July 2011)

Air Force Network (AFNET) - The Air Force's underlying Nonsecure Internet Protocol Router Network (NIPRnet) that enables Air Force operational capabilities and lines of business, consisting of physical medium and data transport services. Includes transmission mediums, gateways, routers, switches, hubs and firewalls, and the functions required to support and enable the environment such as command and control, management, maintenance, network authentication, and defense. (AFI10-1701)

Air Force Information Network (AFIN)—The globally interconnected, end-to-end set of AF unique information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. (AFI10-1701)

Computer Network Defense - Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. Computer network attack is defined as actions taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (GAO-11-695R)

Cyberspace - A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)



Cyberspace Definitions

U.S. AIR FORCE

Cyberspace Operations - The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

Cyberspace Superiority - The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference (AFDD 3-12).

Defensive Cyberspace Operations - Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called **DCO**. (JP 3-12)

DoD Information Networks Operations - Department of Defense information network operations. Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 3-12)

DoD Enterprise Architecture - A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the “current” and “target” environments; and the roadmap for transition to the target environment. (DoDD 8000.01)

Enterprise Architecture - a strategic information asset base, which defines the mission, the information necessary to perform the mission and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs. An enterprise architecture includes a baseline architecture, target architecture, and a sequencing plan. (Federal Enterprise Architecture Chief Information Officer Council)

Information Dominance – The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects. (IDFP, 2015)



Cyberspace Definitions

U.S. AIR FORCE

Information Superiority – The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02)

Information Technology - The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. [(40 USC 11101 (6))]

Mission Assurance - Actions taken to achieve mission resiliency and ensure the continuation of MEFs and assets, including personnel, equipment, facilities, networks, information, infrastructure, and supply chains, so that the DIE can conduct its critical missions under all conditions and across the spectrum of threats and hazards. Mission assurance will evolve to meet organizational and mission needs but typically will encompass those programs related to the national preparedness elements of prevention, protection, mitigation, response, and recovery. (DODI 3020.39)

Mission Assurance (Cyberspace) - Measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities. (AFDD 3-12)

Offensive Cyberspace Operations - Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called **OCO**. (JP 3-12)



U.S. AIR FORCE

(Working) Cyberspace Terms

Communications Squadron - Next (CS-Next) - The shift in focus within the current communications squadrons to Mission Assurance (DODI 3020.39 March 2, 2015) through DoD Information Networks Operations (JP 3-12) and Defensive Cyberspace Operations (JP 3-12). (SAF/CIO A6 lead for planning)

Cyberspace Operations Flight - Initiative to build cyber expertise at the wing level to leverage and integrate cyber capabilities and effects created in, through, and from cyberspace at the tactical and operational level. In addition to maximizing current operations through interaction with the Operations Support Squadron, this initiative will aid in highlighting future requirements, and operational gaps, related to operations in, through, and from cyberspace to increase the effectiveness of Air Force core missions. (HAF/A3 lead for planning)

Functional Mission Analysis – The study of assigned missions, mission threads, organizational structures, TTPs, systems, tasks and personnel to identify or develop the operational approach to accomplish the mission. The primary inputs include higher headquarters' planning directives, other strategic guidance, and the commander's initial planning guidance, which may include a description of the operational environment, a definition of the problem, the operational approach, initial intent, and intelligence. (Hybrid of Mission Thread definition [SAF/AQ LOA 1 Action Plan] & Mission Analysis [JP 5-0])

Headquarters U.S. Air Force

Integrity - Service - Excellence

Health of Career Fields



SAF/CIO A6SF
April 2016

U.S. AIR FORCE



Air Force Information Dominance Flight Plan

INFORMATION DOMINANCE VISION

The Air Force fully exploits the manmade domain of cyberspace to execute, enhance and support Air Force core missions

PRIORITIZED TENETS (ALWAYS TRUE)

I. Increase Effectiveness of Air Force Core Missions

II. Increase Cybersecurity of Air Force Systems and Information

III. Realize Efficiencies through Innovative IT Solutions

CURRENT LINES OF EFFORT

- 1. Support transition to JIE
- 2. Transform IT/Cyberspace career force development
- 3. Lead Air Force Task Force to strengthen protection of core missions from Cyber threats
- 4. Operationalize the authorities/responsibilities of the CIO

STRATEGIC GOALS (10 YEAR EFFORTS)

- 1. Provide Airmen trusted information where they need it so they can be most effective
- 2. Organize, train and educate Cyber-Airmen to become experts in cyberspace and in the Air Force core missions to which they contribute
- 3. Deliver freedom of action in cyberspace to advance Air Force core missions
- 4. Optimize the planning, programming, budgeting and execution of cyberspace investments



U.S. AIR FORCE

Overview

- **Cyberspace Workforce**
- **Health Data by AFSC**
- **Challenges**



Cyberspace Workforce

U.S. AIR FORCE

57K

Cyberspace Workforce
44.5K Total Force

Officer

Active: 2499
Guard: 670
Reserve: 390

Enlisted

Active: 19.5K
Guard: 9.9K
Reserve: 2.5K

Civilian
9.7K

Cyberspace Operations
Cyber Warfare Operations
Cyber Systems Operations
Cyber Surety
Computer Sys Programmer
Client Systems
Cyber Transport Systems
RF Transmission Systems
Spectrum Operations
Knowledge Ops Management (*)
Computer Ops, Mgmt, etc. (*)
Comp/Engineering (*)
Mathematical Sciences (*)
Information Technology (*)

Realigned as non-Cyber functions

Admin and Postal

(~14K people)

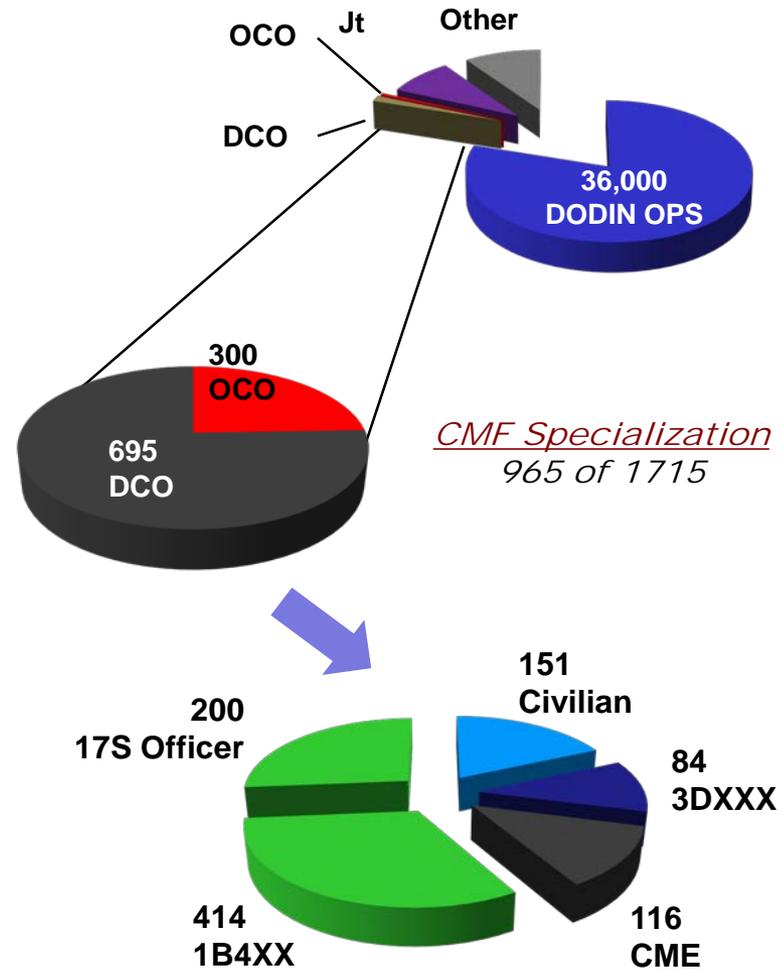
Airfield Systems and Radar

(~2.5K people)

KEY

OFFICER
ENLISTED
CIVILIAN

(*) only some within these specialties are considered 'Cyber'



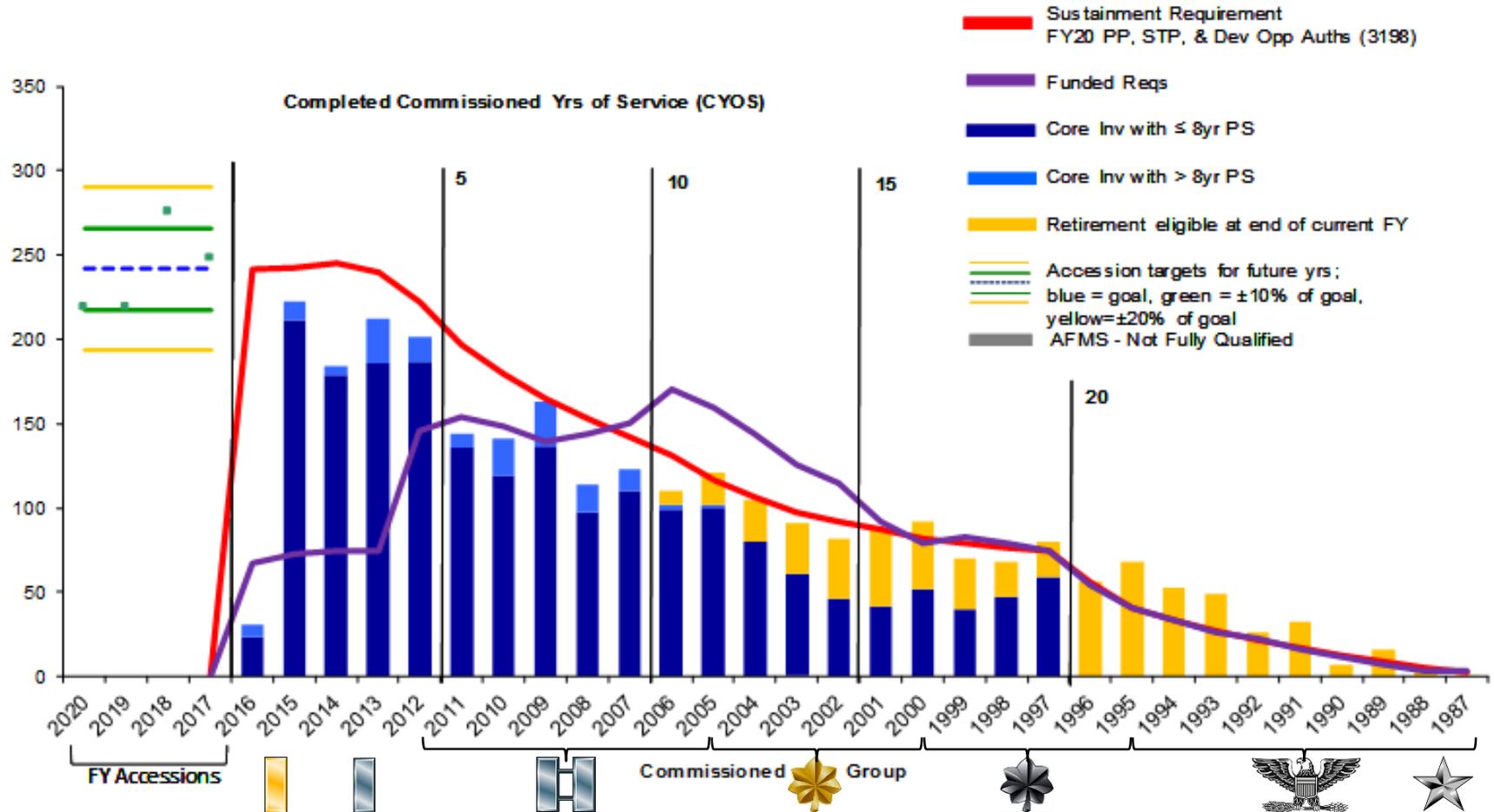


17D - Cyberspace Operations

U.S. AIR FORCE

Career Field Health as of 31 Mar 2016

17X - Cyberspace Operations

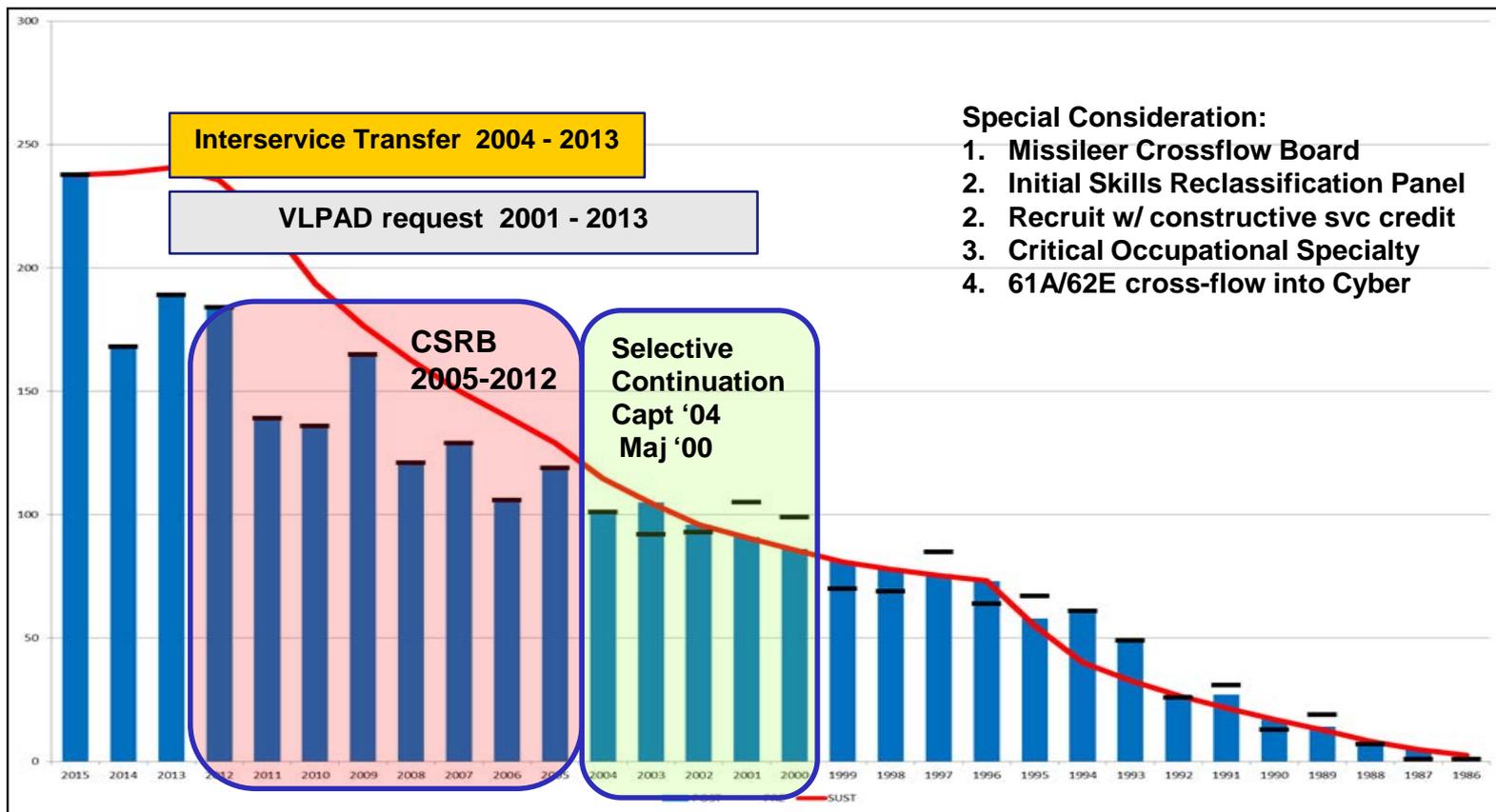


Integrity - Service - Excellence



Recruiting and Retention Initiatives

U.S. AIR FORCE



Integrity - Service - Excellence



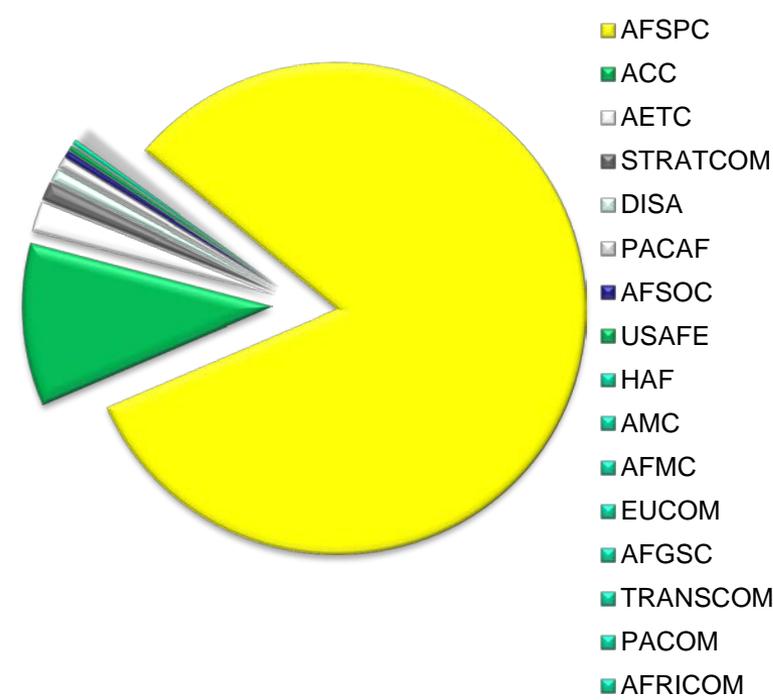
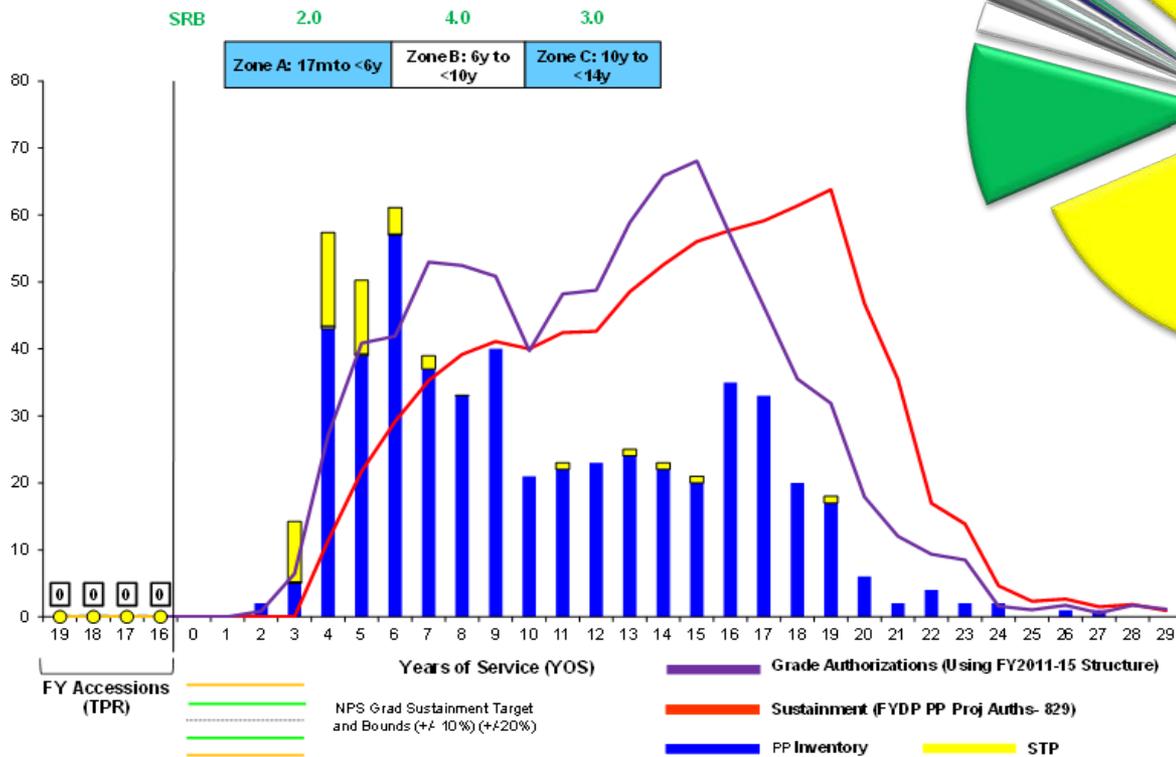
1B4X1 - Cyber Warfare Operations

U.S. AIR FORCE

	Auth	Asgnd	Manning %
AD	829	511	61.64%
ANG	449	187	41.65%
AFRC	195	60	30.77%
TOTAL	1473	758	51.46%

PP Inventory

1B4X1 - Cyber Warfare Operations



Integrity - Service - Excellence



Career Field Snapshot

1B4X1 – Cyber Warfare Ops

as of: Apr 2016

U.S. AIR FORCE

Primary Role:

- **Conducts OCO** to **project power** by application of force in and through cyberspace
- **Conducts DCO** to **defend DoD** and other friendly cyberspace
- Conducts specific cyberspace actions including **cyberspace defense, cyberspace ops in support of intel, cyberspace OPE and cyber attack** to support OCO/DCO

AF Cyber Weapon System/Service Roles ~450:

- Network Attack System
- Air Force Cyberspace Defense
- Cyber Command and Control Mission System
- Air Force Intranet Control
- Cyber Security and Control System
- Cyberspace Vulnerability Assessment/Hunter (also CMF)
- Air Force/Joint Red Team
- Air Operations Centers
- Joint/Coalition Forces

Challenges:

- 61% AFSC Manning
- Sluggish AETC training development model
- Competing with industry to retain trained cyber workforce
- Constant churn across cyber communities make stabilizing a career field difficult
 - Tendencies to change without fully understanding problem

CMF Work Roles ~420 Auth:

- Presence on almost all types of CMF teams
 - Includes but not limited to
 - Interactive Operator
 - Cyber Planner
 - Access Network Operator

On the Horizon:

- Cyber Operations Flight
 - Wing OCO integration with DIRCYBERFOR
- CS Next – 1B4 role TBD

Successes:

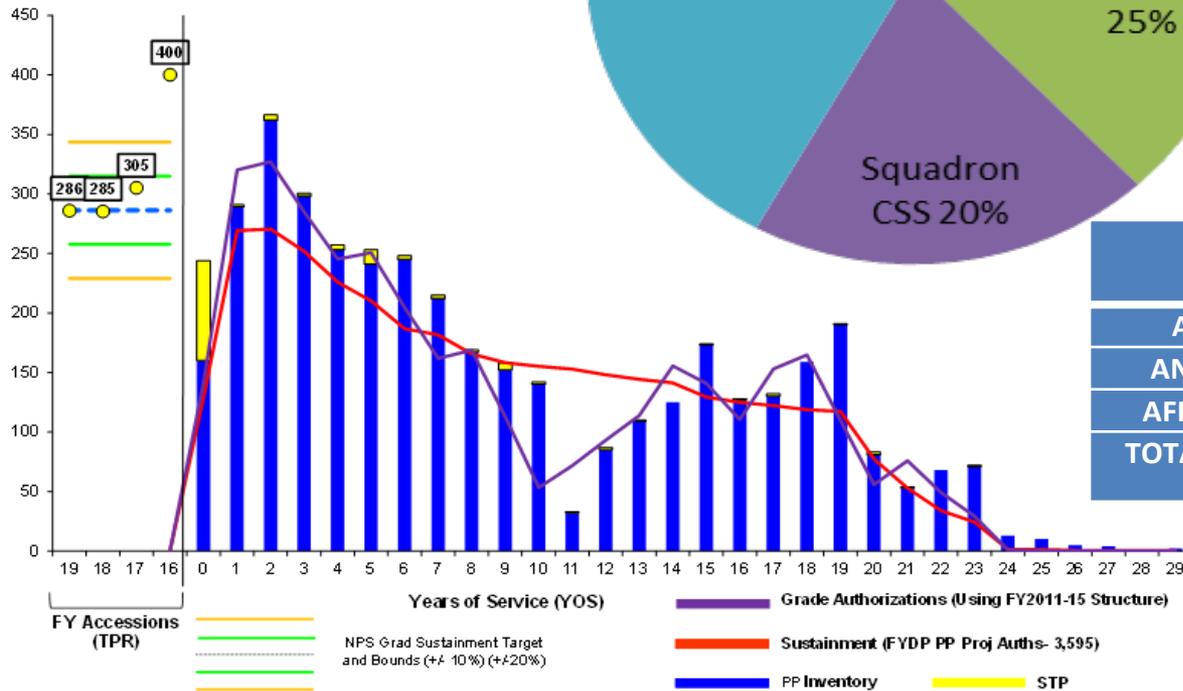
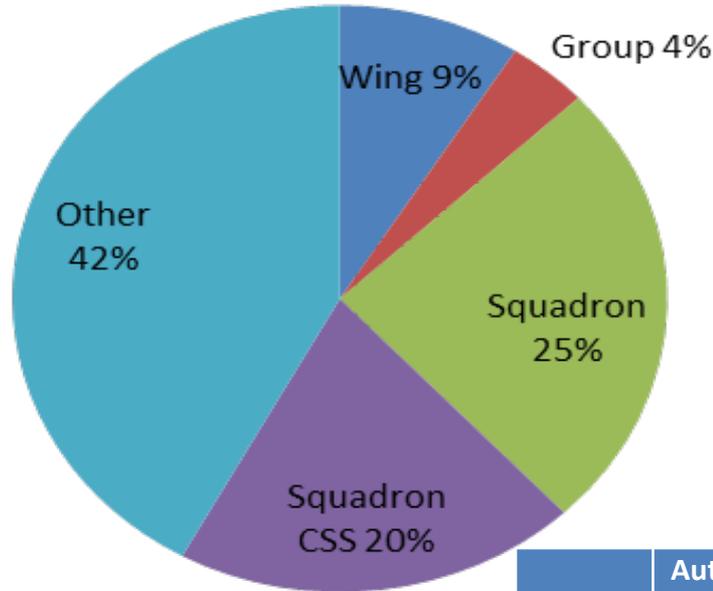
- Contract awarded for Cyber Aptitude Assessment
- SDAP for Cyber Warfare Operators
- ***Training development funding***



3A1X1 - Administration

U.S. AIR FORCE

PP Inventory
3A1X1 - Administration



	Authorized	Assigned	Manning %
AD	3615	3916	108%
ANG	1105	1154	104%
AFRC	998	1285	129%
TOTAL	5718	6355	111%



Primary Role:

- Provides administrative support to AF, DoD, and joint organizations and their CCs, Directors, and Senior Leaders
- Specializes in:
 - Office Management
 - Human Resources
 - Executive Support
 - Postal and Official Mail

On the Horizon:

- FY16 Enlisted Development Teams for CMSgt
- SMSgt Prioritization Plan
- Update AFECD and CFETP based on STRT recommendations
- A1 Publish Human Resources PSDM
- Monitor CCAF degree conversion for FY17 Catalog
- SEL Meeting - Keesler
- Dedicated 3A1 AFPC Assignment NCO

Successes:

- Postal SEI 984 Updated 29 Jan 15
- 3A151 CDCs published Oct 15
- AFI 33-301 Published 15 Jul 15
- Base Level Training Published 29 May 15
- AFECD updated/published 30 Apr 15

Challenges:

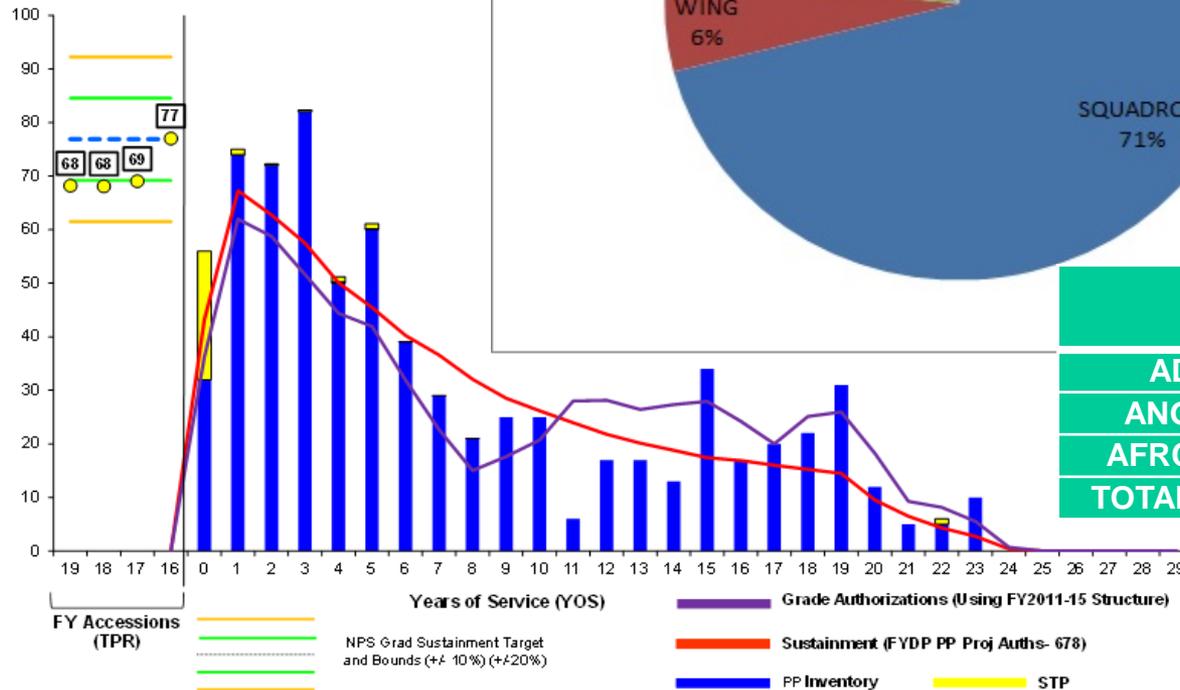
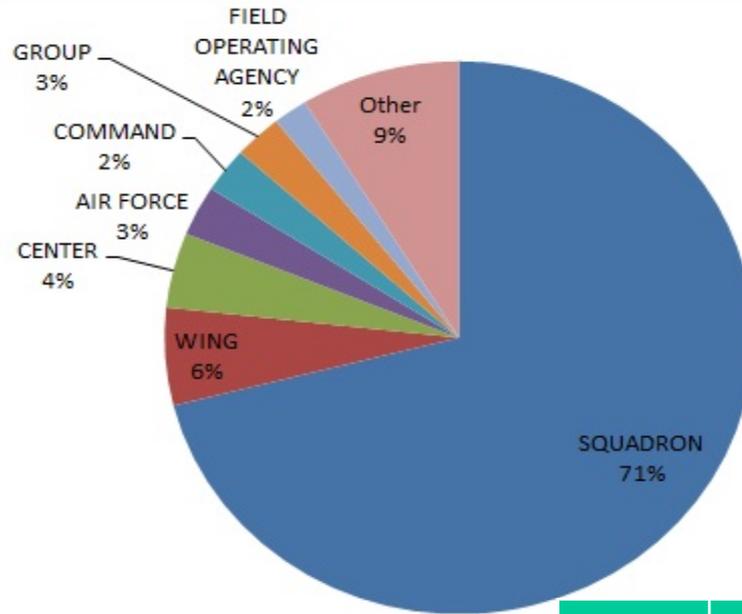
- CMSgt authorized/assigned disproportionate to total Career Field population: Should have at least 30 positions (30% deficit in authorizations, 30/21)
 - Not enough CMSgt positions for MFMs
- Conversion of encumbered 3A billets to 3S without the 3S manpower to fill vacancies
- CS/CC responsible for OMM but required grade not available
- Manning imbalances across MAJCOMs
- Post office experience / manning
- SEI-984 – Personnel/Unit not updating MilPDS (2096s)



3D0X1 - Knowledge Operations Mgt

U.S. AIR FORCE

PP Inventory
3D0X1 - Knowledge Operations Mgt



	Authorized	Assigned	Manning %
AD	678	718	105.90%
ANG	418	455	108.85%
AFRC	229	214	93.45%
TOTAL	1325	1387	104.68%



Primary Role:

- Business Process Optimization through judicious application of AFSO21 and Lean Six Sigma principles
- Specializes in information access programs, such as FOIA, Privacy Act, PII, etc. (looking to move IAP to 3A1, timeline still TBD)
- Drives Best Practice implementation of content mgt tools (i.e. SharePoint, AF Portal, EIM technologies)
- Manages base/wing Pubs/Forms program IAW 33-360

On the Horizon:

- Continue to drive change from legacy learning modes to AF E-Learning blended learning environment
- Replace initial membership of AFKMWG with new members
- SKT exempt in 2017 promotion cycle

Successes:

- Realigning 3D0X1s to the KMC (AFMC)

Challenges:

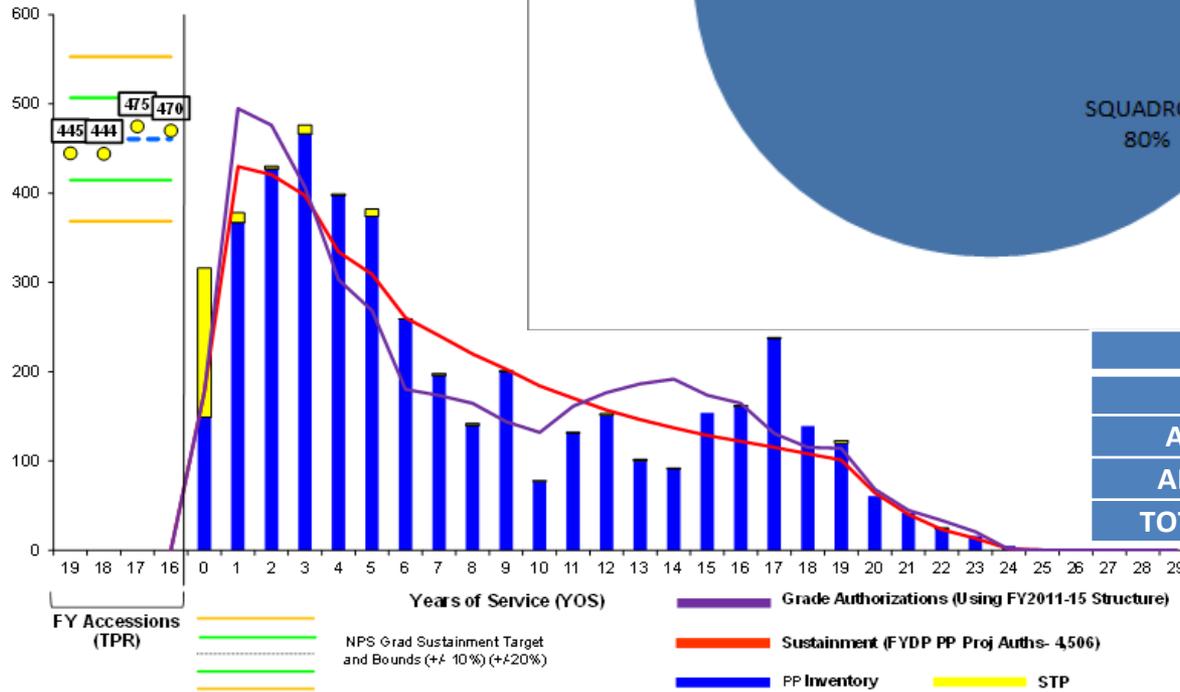
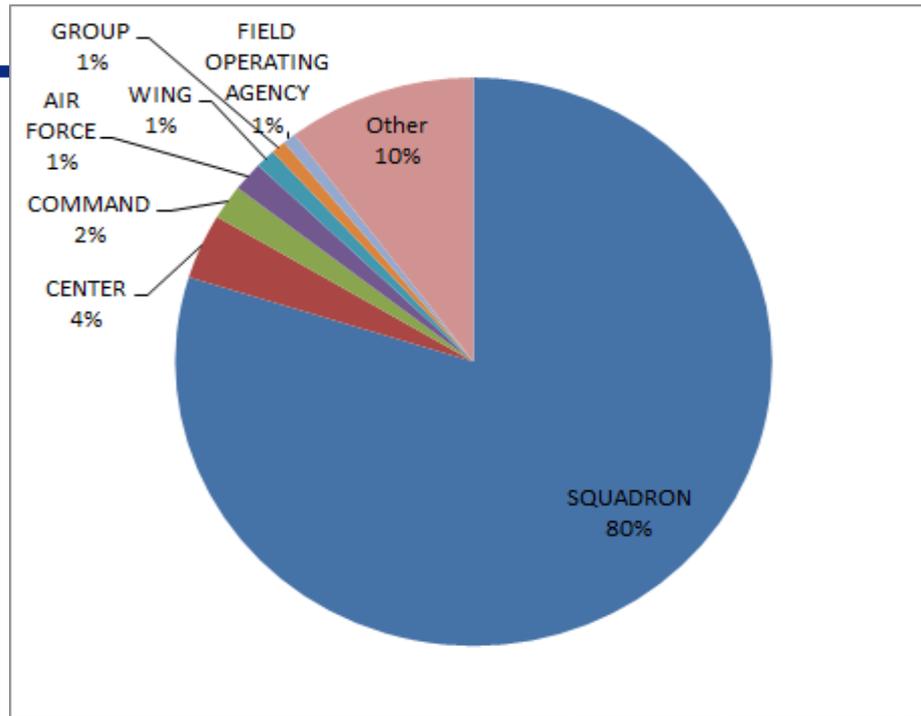
- Workforce is still treated as Administrators in the absence of any 3A1X1s in the unit.
- Commanders don't see the difference in the two AFSCs
- Individuals in this career field often make a difference, but the career field still suffers an identity crisis
- Shortage of NCO/SNCO 3D0X1s (AETC)
 - Artificially low due to new 37 TRW
 - Populating new Battlefield Airman Training Wing: 37 TRW, 37 TRW Det 1 Insufficient manning to stand up a mobile KM cell (AFMC)
- Lack of funding and time for extraneous hands-on/application-based training now needed (AFMC)
 - SharePoint (Advanced/Designer)
 - Knowledge Management Certification
 - Continuous Process Improvement
- Limited direction in how to establish a KMC given installation specific challenges (AFMC)
- Lack of required certification prohibiting ability to gain elevated permissions to fulfill EIS and IAO capabilities outlined in AFI 33-396 (AFMC)
- Ambiguous MICT checklist language limiting units' ability to determine if they are meeting requirements (AFMC)
- i.e. AFI 33-396, para 4.2.2. Mobile Capabilities (AFMC)



3D0X2 - Cyber Systems Operations

U.S. AIR FORCE

PP Inventory
3D0X2 - Cyber Systems Operations



	Authorized	Assigned	Manning %
AD	4506	4484	99.51%
ANG	1586	1703	107.38%
AFRC	511	548	107.24%
TOTAL	6603	6735	102.00%



Career Field Snapshot

3D0X2 – Cyber System Ops

as of: Mar 2016

U.S. AIR FORCE

Primary Role:

- Installs, supports and maintains servers or other systems; responds to outages/interruption
- Designs, configures, installs and manages data services
- Performs system management, backups and recovery
- Implements security updates and patches
- Reviews and implements C4 systems

Challenges:

- Base level 3D0X2s still haven't realized any 'new' rights since the advent of the Federated Rights program inception
- Outdated CDCs (last edit is from 2010)
 - Effecting WAPS testing for SSgts this year
- Overcoming manning imbalance due to re-assignment of boundary protection from 3D0X3 to 3D0X2 (AFSPC)

On the Horizon:

- Continue to drive change from legacy learning modes to AF E-Learning blended learning environment
- SKT exempt in 2017 promotion cycle

Successes:

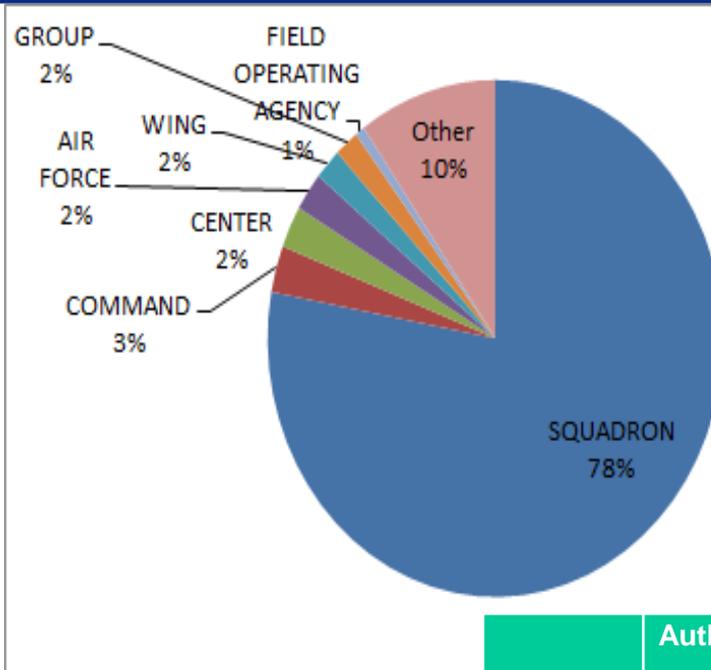
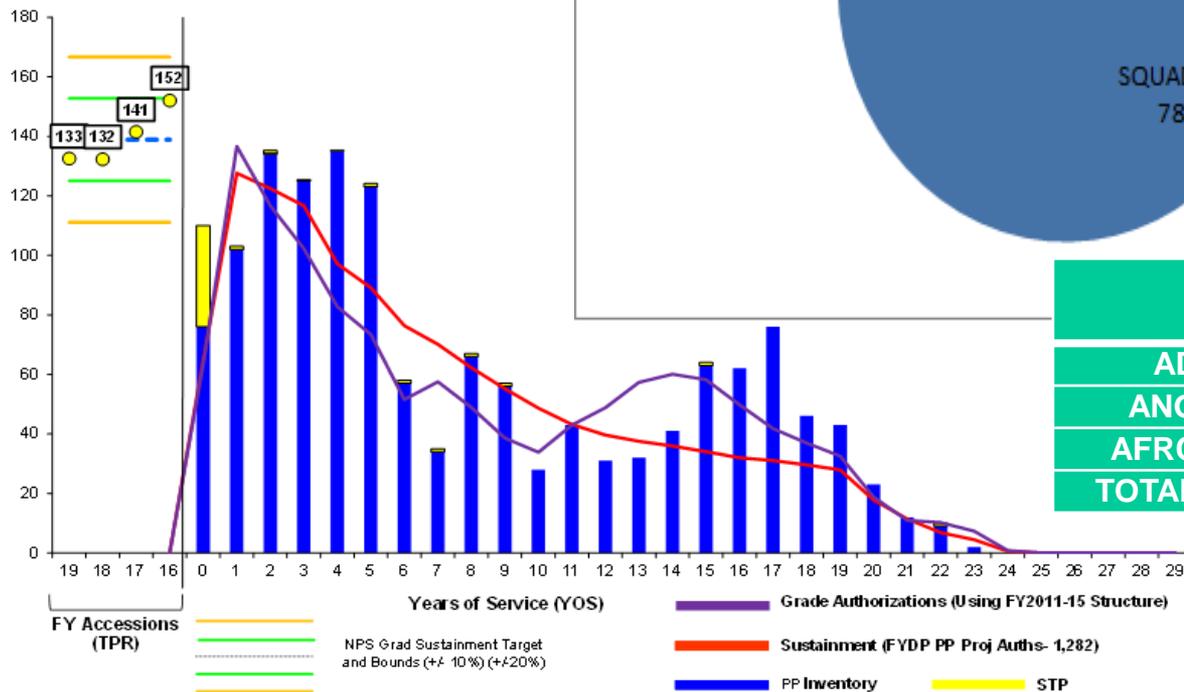
- 56 ACOMS creation of Cyberspace Defense Cell for 613 AOC as part of Communications Squadron Next pilot comprised of 1B4X1, 3D0X2s, and 3D1X2s
- May become Cyberspace Defense Cell model for all AOCs
- CFETP task 15.1 no longer core task for 5 level upgrade, still available for supervisors to assign coursework within as needed for work center task coverage



3D0X3 - Cyber Surety

U.S. AIR FORCE

PP Inventory
3D0X3 - Cyber Surety



	Authorized	Assigned	Manning %
AD	1282	1419	110.69%
ANG	751	875	116.51%
AFRC	194	129	66.49%
TOTAL	2227	2423	108.80%



U.S. AIR FORCE

Career Field Snapshot 3D0X3 – Cyber Surety

as of: Mar 2016

Primary Role:

- COMSEC / EKMS (to be replaced by KMI by FY17)
- EMSEC / COMPUSEC
- Information Assurance (IA)
- Certification & Accreditation (C&A)
- Combat Crew Comm (<10% of AD force)

On the Horizon:

- Continue to drive change from legacy learning modes to AF E-Learning blended learning environment
- Combat Crew Comm (CCC) waiting for completion of AFMS, potential future for CCC is as 1C3X1 (Command Post)
- Champion conversion of PKI/LRA course from in-resident to DL; #1 USAFE/A6 training concern (revisited yesterday)
- SKT exempt in 2017 promotion cycle

Successes:

Challenges:

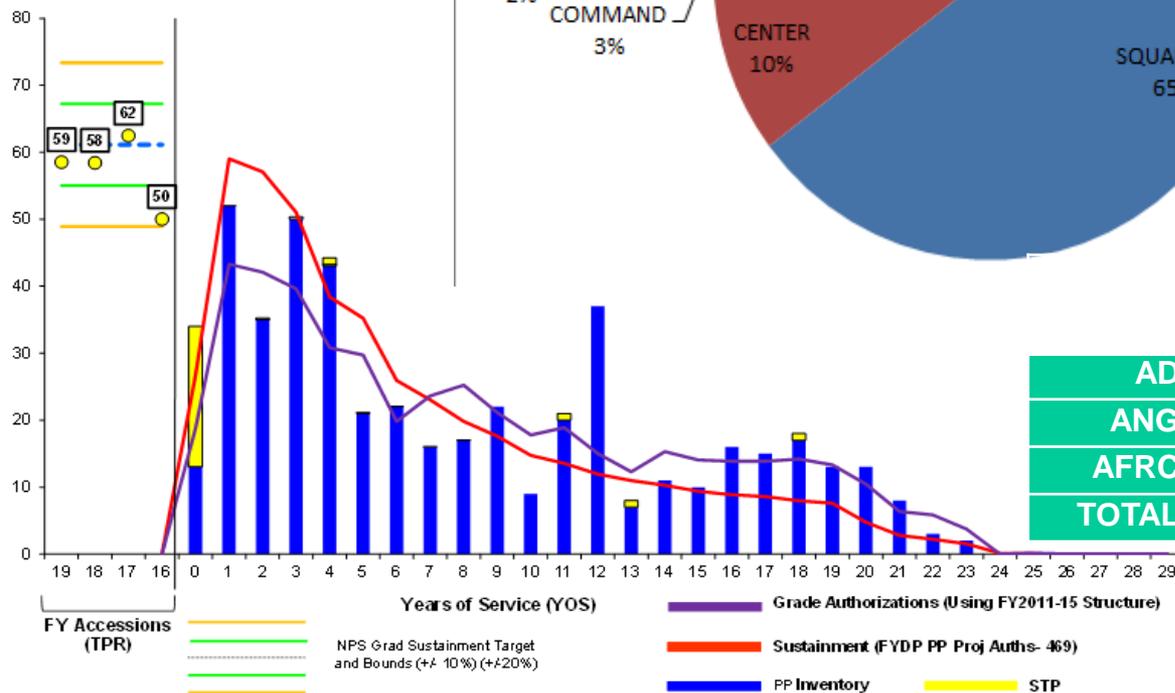
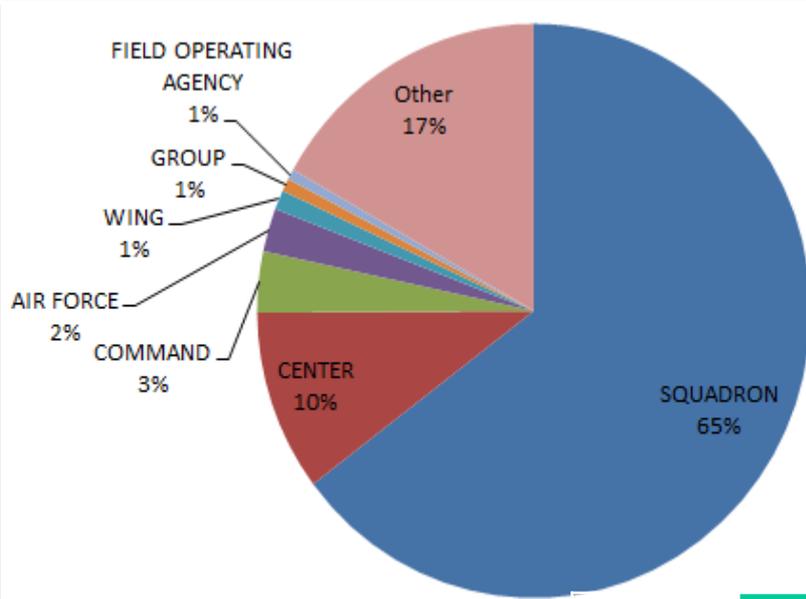
- Info Assurance (IA) Manpower Standard stalled
 - CFM in conversation with AF/A1MR about killing study due to the aged information being used for analysis
- Combat Crew Comm “uniqueness”
 - AFMS out for MAJCOM coord
- KMI training, 7 of 9 PACAF/COMSEC accounts will be migrated to KMI by the end of FY16 and the remaining two accounts will be migrated during FY17
- PACAF received 10 AETC funded slots, this is not enough to fulfill our requirements; ideally we would like 4 trained personnel at each location
- New SEI would be helpful, 269 does not indicate if a member has attended EKMS or KMI training (PACAF)
- 3D0X3 manpower study- AMC non-concurred with cuts. Requirements are growing and losing personnel will be detrimental
- 8570 cert & tech schools don’t prepare Amn for their job



3D0X4 - Computer Systems Programming

U.S. AIR FORCE

PP Inventory
3D0X4 - Computer Systems Programming



	Authorized	Assigned	Manning %
AD	469	472	100.64%
ANG	7	6	85.71%
AFRC	6	6	100.00%
TOTAL	482	484	100.41%



Career Field Snapshot

3D0X4 – Computer Programming

as of: Mar 2016

Primary Role:

- Application security
- Software development & lifecycle sustainment
- Mobile app & collaborative tool development
- Database management
- Systems analysis and design
- Mission Systems Software Sustainment
- Analytical & theoretical problem solving

On the Horizon:

- Continue to drive change from legacy learning modes to AF E-Learning blended learning environment
- SKT exempt in 2017 promotion cycle

Successes:

Challenges:

- Highly-specialized training for specific languages
- Shift toward database programming/analysis
- Low flow throughput at initial skills training (~52/yr)
- Perception of ambiguous or diminishing work roles
 - In locations shared with Civilian programmers, not allowed to program, low job satisfaction

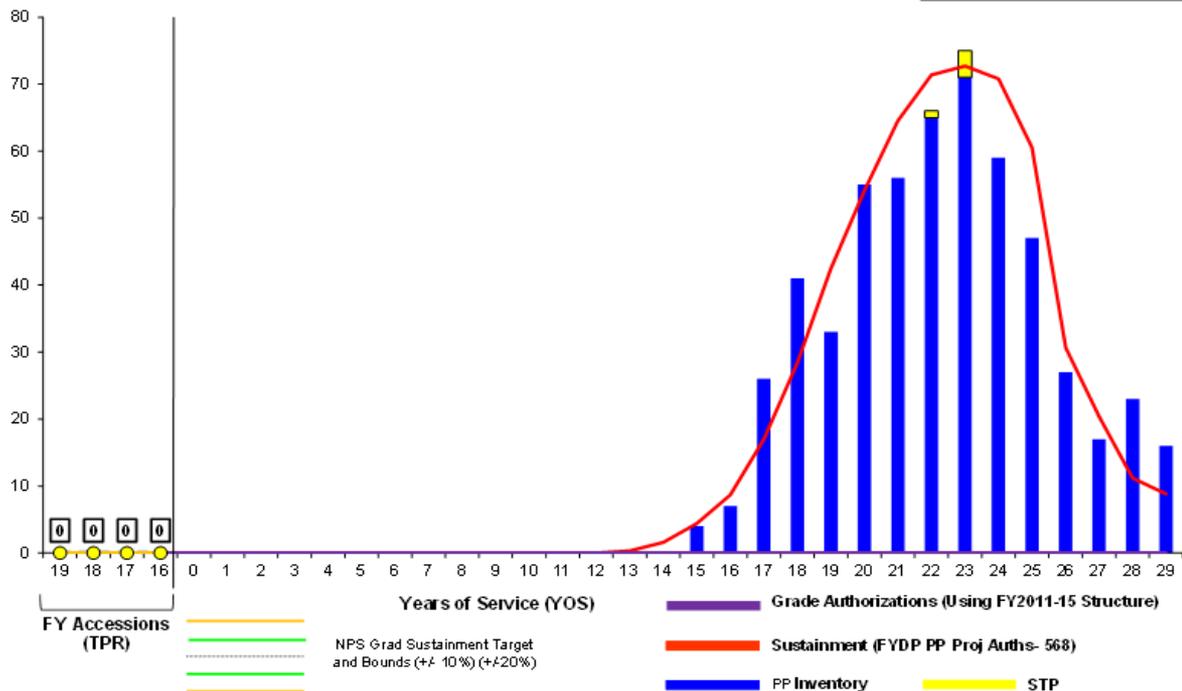


3D1X0 - Cyber Systems Manager

U.S. AIR FORCE

PP Inventory
3D1X0 - Cyber Systems Manager

End of Feb 16
Gray bars show DSDs serving outside AFSC





Career Field Snapshot

3D1X0 – Cyber Systems Manager

as of: Mar 2016

Primary Role:

- Manages cyberspace system analysis and design, programming, systems operation and maintenance, resource management and security management.
- Directs activities for installing, maintaining, repairing, overhauling, deploying, and modifying cyberspace systems and equipment platforms.
- Manages and directs network operations in garrison and at deployed locations by performing duties to develop, sustain, and enhance network and electromagnetic capabilities to defend national interests from attack.
- Ensures personnel are trained, equipped, and available to perform the assigned mission. Conducts career field development and mentoring for subordinate cyberspace support personnel.
- Introduces Airmen to career field path and steers growth to feed into the cyberspace deliberate development program

On the Horizon:

- EDT starting Fall 2016
- Identifying Superintendents to attend 17D Squadron Commander's Course
- All SNCOs in TBA to include Top 3%

Successes:

- Superintendents added to 17D Squadron Commander's Course

Challenges:

- Communications from tactical to strategic level
- Losing grades/billets to AFIMSC
- Losing operational/strategic level billets
- Developing technically competent, and institutionally mindful leaders
- Currently no "Succession Planning" for 3D SNCOs
- "Entitled" sr ldrs and CC's Involvement Program billets
- Current CMSgt assignment process is mostly voluntary
- EDT will be "All-in" similar to Command CMSgt
- "Entitled" CMSgts staying to HYT and not taking on higher responsibility—Chiefs need to lead at progressively higher levels—NOT "up or out" program

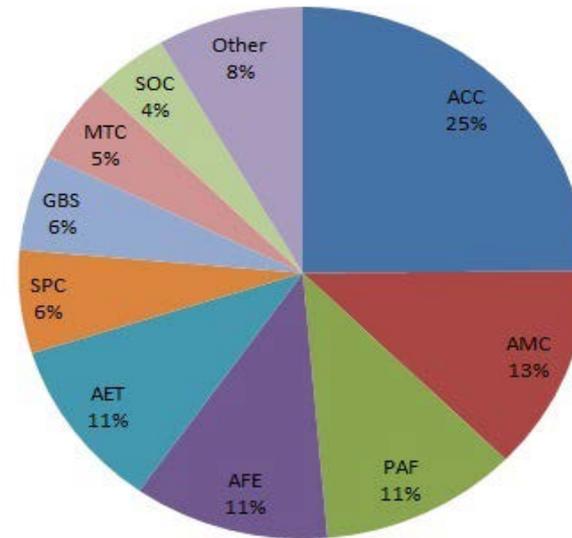
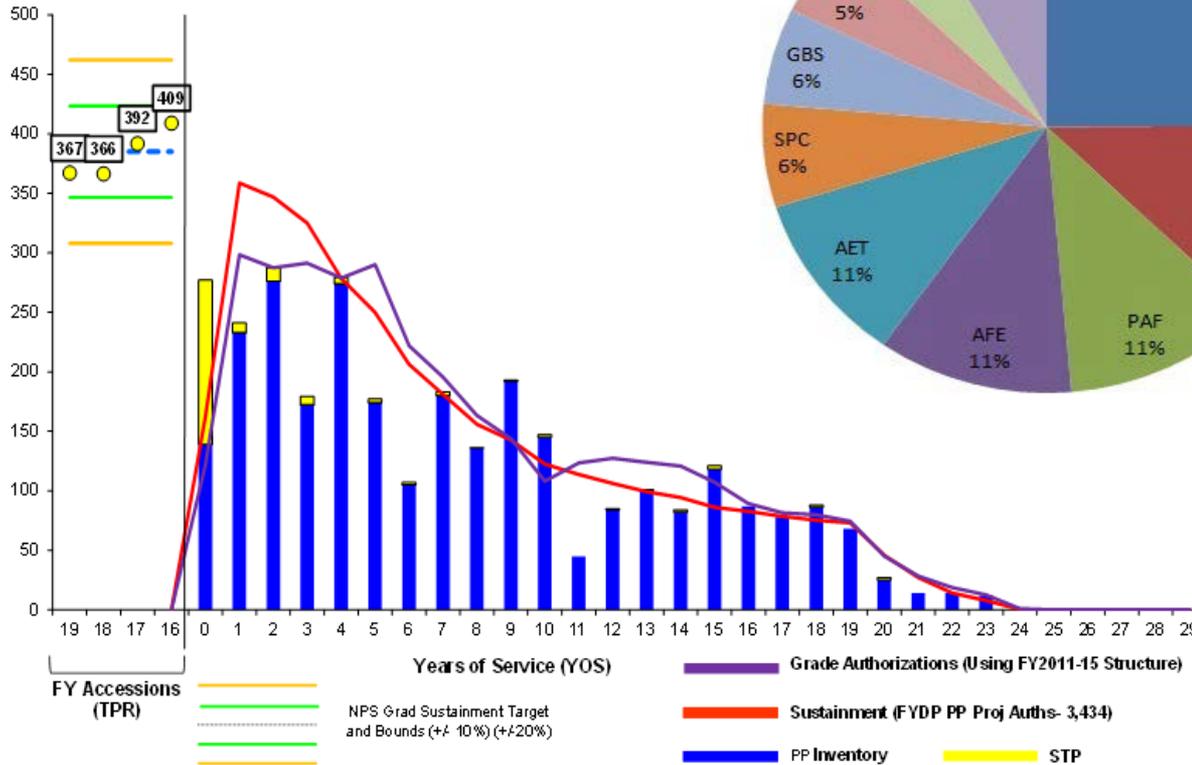


3D1X1 - Client Systems

U.S. AIR FORCE

3D1X1 Consumers

PP Inventory
3D1X1 - Client Systems



	EOFY Auth	Assigned	Manning %
AD	3434	2840	83%
ANG	1093	1143	104.57%
AFRC	391	503	128.64%
TOTAL	4918	4486	91.22%



Primary Role:

- Deploys, sustains, troubleshoots & repairs standard voice, data, video network & crypto devices
- Manages client user & organizational client accts
- Performs client-lvl info tech, voice net spt and Personal Wireless Comm Systems functions

On the Horizon:

- Sec+ requirement mandatory by Oct 2016
- Accession increase--FY 16 PGL 350 vs FY 15 of 265

Successes:

- Sec+ now part of Apprentice course (Oct '15)
- Apprentice capstone block requested...\$0 cost
 - 36 Adobe Reader licenses (enterprise)
 - 36 Windows 7 licenses (enterprise)
 - 6 Server 2008 licenses (AFMC provided)

Challenges:

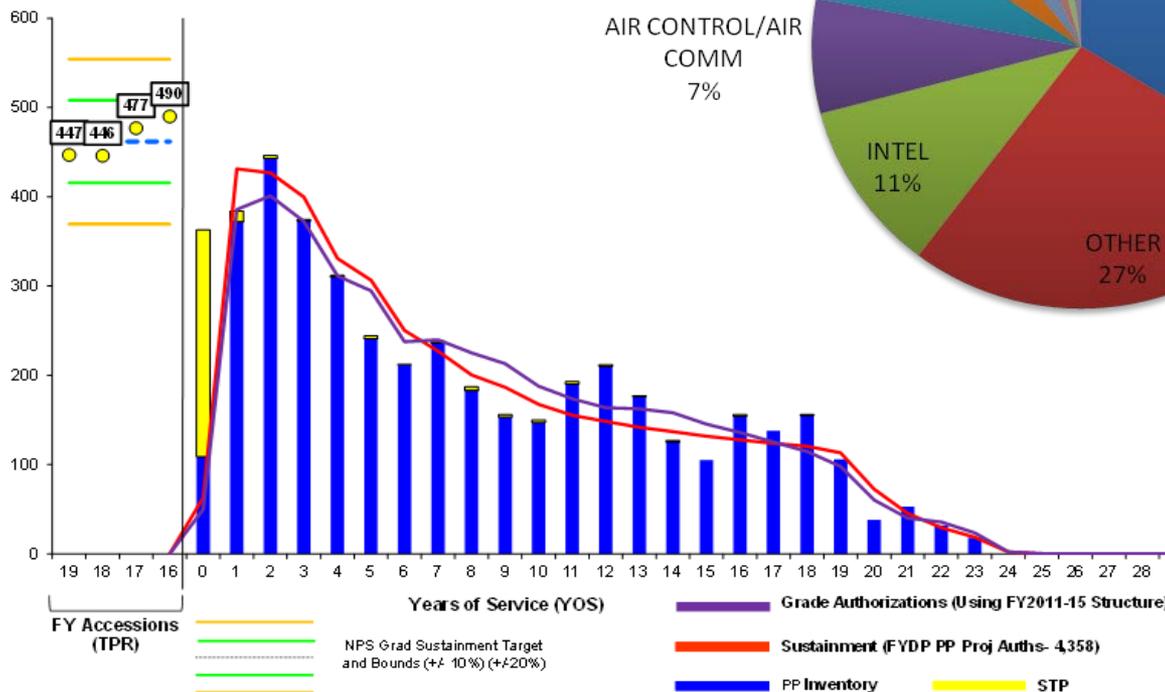
- Lines of responsibility
 - Still some confusion in the field on where 3D1X1 responsibility begins
 - Telephone and LMR client device training
 - Civ/contractor at most stateside locations
 - 3D1X1s expected to know in AOR
- AFSPC—Federated Rights
- Manning: SrA-70%, SSgt-82%, TSgt-100%, MSgt-115%
 - Deployment demand exacerbates situation
- Radio tasks still 3D1X1 CFETP and required to train on tasks. However units utilizing are 3D1X3s for radios
- 8570 cert & tech schools don't prepare Amn for their job



3D1X2 - Cyber Transport Systems

U.S. AIR FORCE

PP Inventory
3D1X2 - Cyber Transport Systems



	EOFY Auth	Assigned	Manning %
AD	4358	4279	98.19%
ANG	2216	2295	103.56%
AFRC	384	313	81.51%
TOTAL	6958	6887	98.98%



Career Field Snapshot

3D1X2 – Cyber Transport Systems

as of: Mar 2016

Primary Role:

- Deploys, sustains, troubleshoots & repairs standard voice, data, video network & crypto devices
- Provide mission critical voice, data & video services

On the Horizon:

- STRT/U& TW scheduled for Sep '16
- Accession increase FY16 450 vs 409 FY15

Successes:

- 1B4 serves as SME and lead trainer for AOC Cyberspace Defense Cell comprised of 3D0X2 and 3D1X2 AFSCs

Challenges:

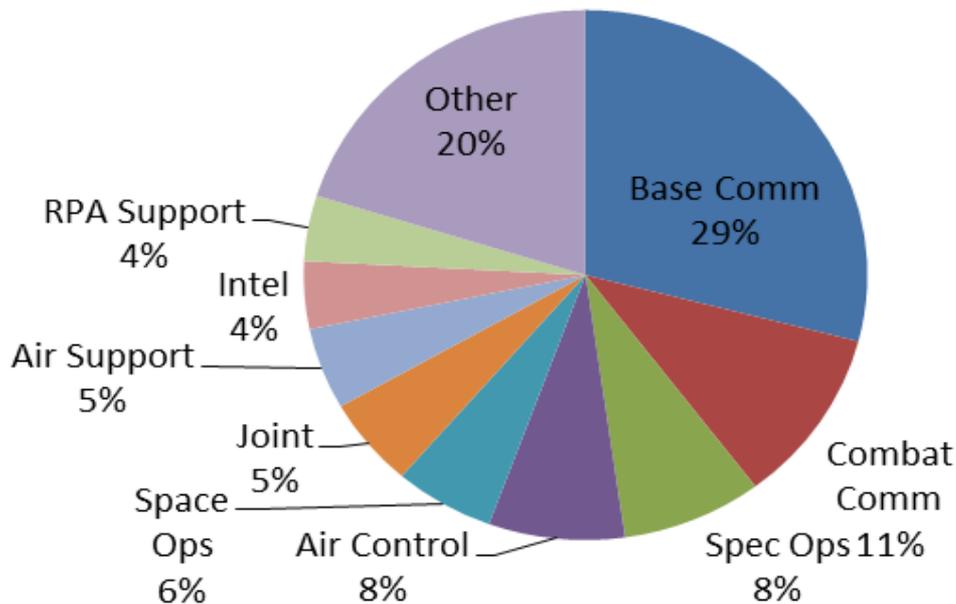
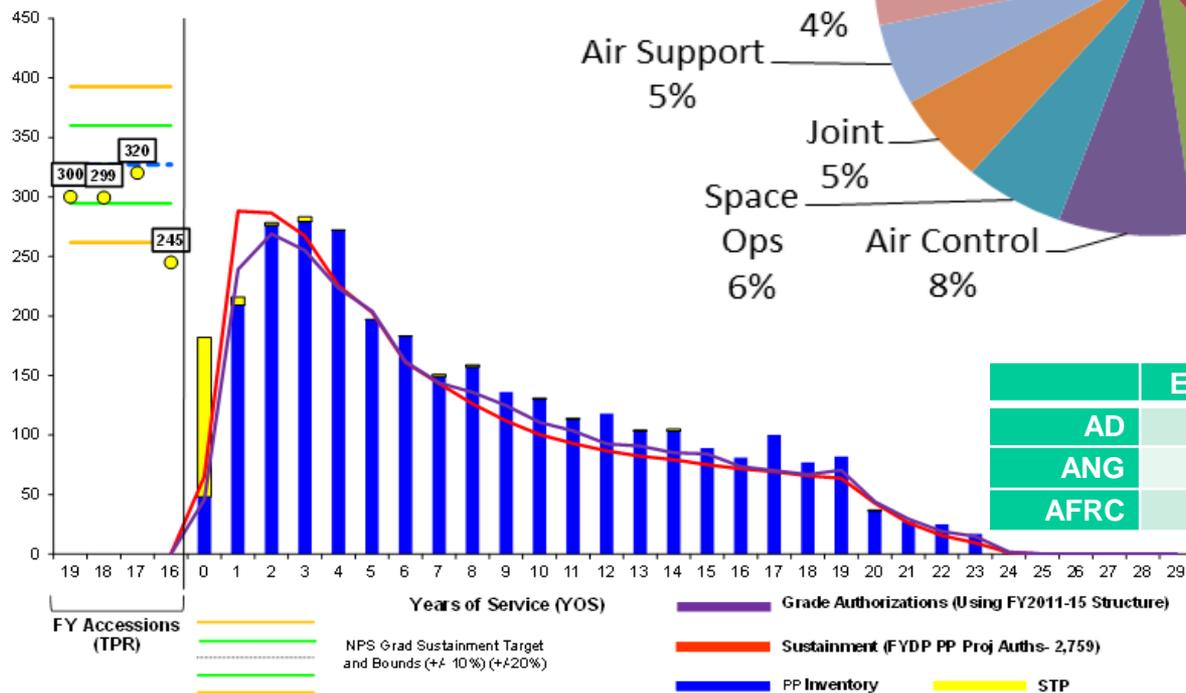
- Very diverse AFSC/Difficult to provide focused training
 - RPA, Intrusion Detection Systems, Telephone, Network Management, etc
 - Could PCS and have no experience at new base
 - Routers/switches from multiple vendors, i.e Cisco, Juniper, HP, etc
- SSgt manning at 83%/TSgt manning 92%
 - Deployment demands for 5 levels



3D1X3 - RF Transmission Systems

U.S. AIR FORCE

PP Inventory
3D1X3 - RF Transmission Systems



	EOFY Auth	Assigned	Manning %
AD	2759	3008	109.03%
ANG	1860	1868	100.43%
AFRC	467	445	95.29%



Career Field Snapshot

3D1X3 – RF Transmission Systems

as of: Mar 16

Primary Role:

- Deploys, sustains, troubleshoots & repairs standard radio frequency, line-of-site, beyond line-of sight, wideband and ground-based satellites
- Employs orbiting comm satellite, line-of-sight, and tropospheric scatter techniques

On the Horizon:

- Closely monitoring direction of radio systems with regards to 8570 requirements
 - Requirement is not currently sufficient to include 8570 training in initial skills course
- Introduce more IP based training in Technical Training
 - New Course ~Jul 2016
- Potential adding 8570 requirements for 3D1X3
- Garnered funding for PRC-117G Radios

Successes:

Challenges:

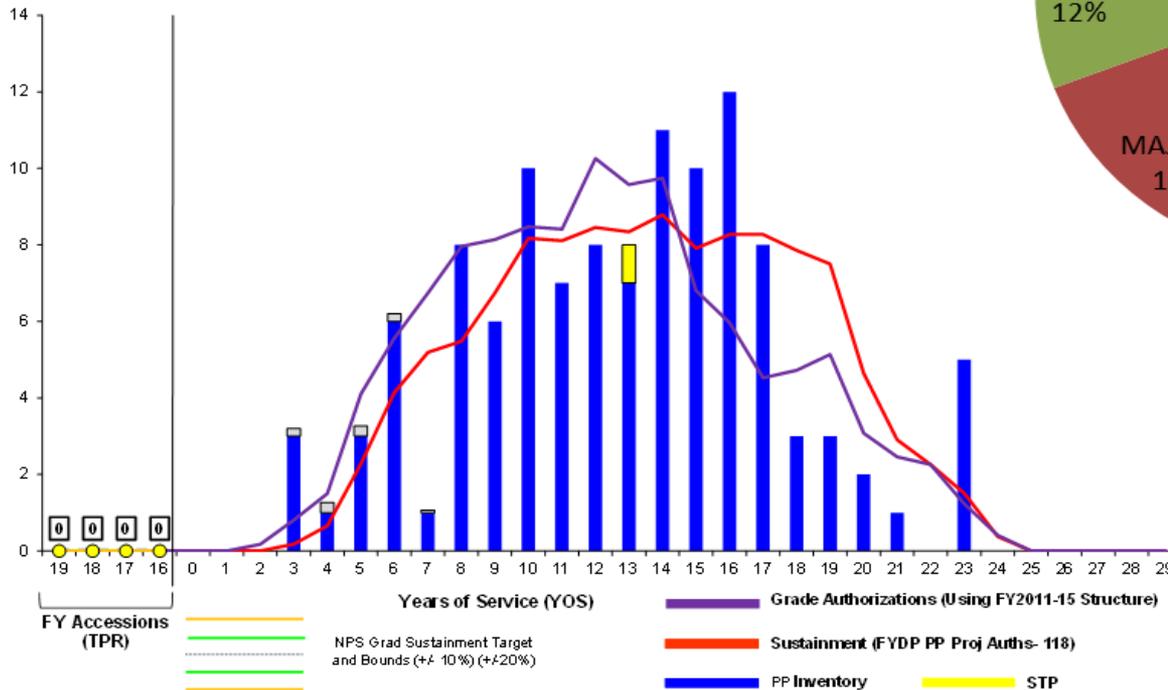
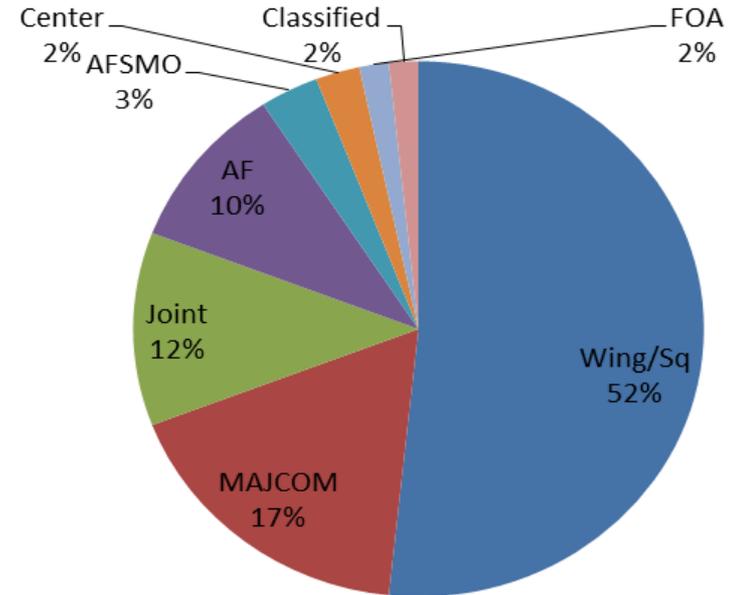
- Complexity between assignments (base Radio vs STEP site)
 - Larger satellite system sites systems are much more complex (skill atrophy)
- Radio systems becoming IP based and leading to 8570 requirements
- XTS-5000 radios for course
- Tech School not teaching troubleshooting skills
- MILSTAR training
 - FAB-T (~FY19 new install)
 - Current course has failing HPA (\$500K fix)



3D1X4 - Spectrum Operations

U.S. AIR FORCE

PP Inventory
3D1X4 - Spectrum Operations



	EOFY Auth	Assigned	Manning %
AD	118	115	97.46%
ANG	85	59	69.41%
AFRC	2	1	50.00%
TOTAL	205	175	85.37%



Primary Role:

- Analyze rfmnts/requests frequencies in spt of:
 - Terrestrial, aircraft and space systems
- Provides guidance on spectrum certification
- Joint Task Force Spectrum Manager

On the Horizon:

- Work with AFSMO to prioritize assignments for our Spectrum Managers.
- Flow Airmen into Joint Spectrum course when being assigned to Joint Billet
- Validate need for improved math skills and radio principles

Successes:

Challenges:

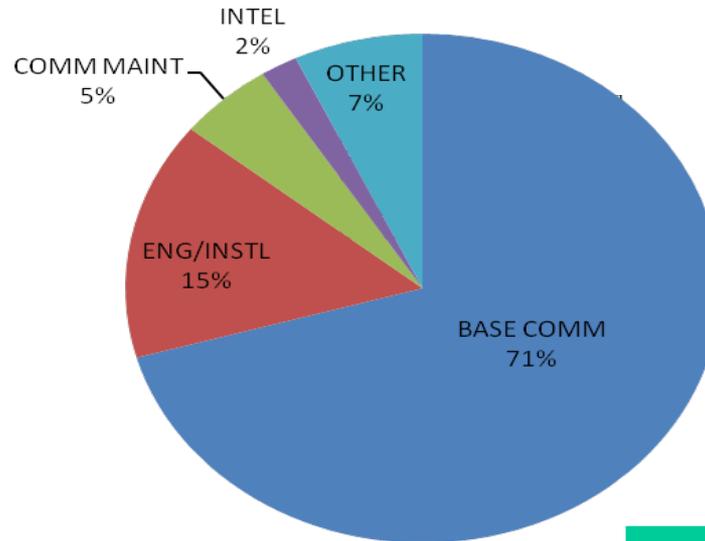
- Installation Spectrum Manager (ISM) trng deficiencies
 - ISM positions are one deep at base level
 - MAJCOM Spectrum Managers must train 3 level
 - If 3D1X4 is unavailable, a 3D1X3 performs ISM
- Initials skills is an Interservice Training Review Organization (ITRO) course
 - AF is executive agent. Navy/Marines utilize crse
 - Army pulled out 3 yrs ago, some friction exists



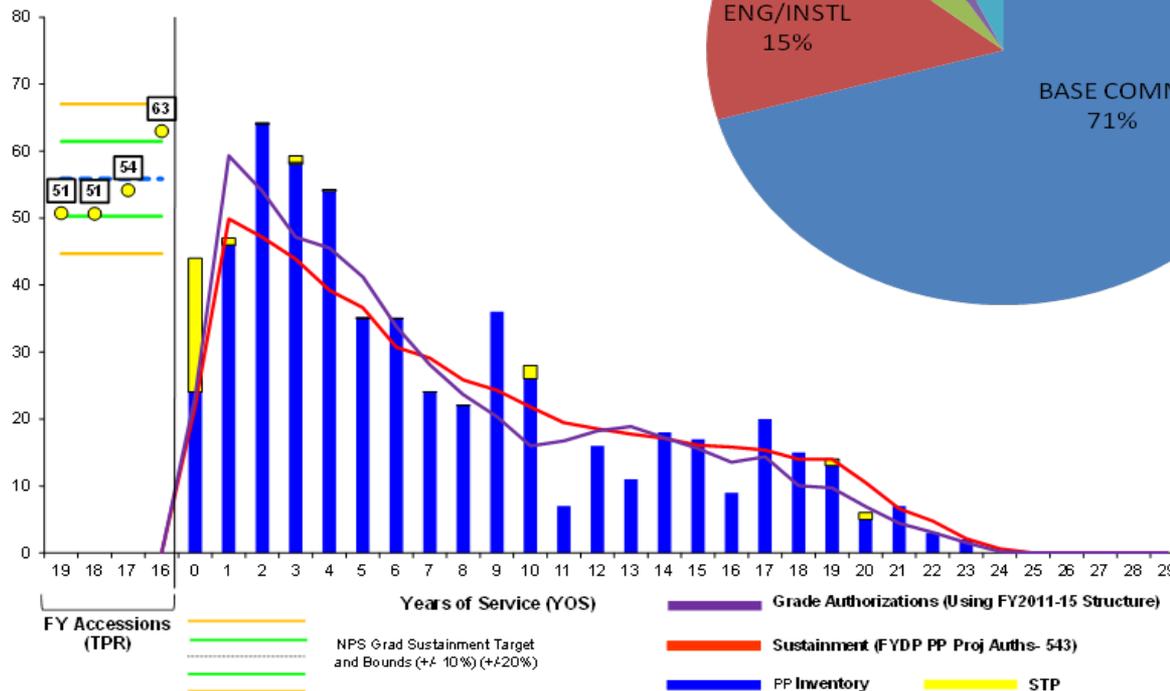
3D1X7 - Cable and Antenna Sys

U.S. AIR FORCE

3D1X7 Consumers



PP Inventory
3D1X7 - Cable and Antenna Sys



	EOFY Auth	Assigned	Manning %
AD	543	567	104.42%
ANG	621	557	89.69%
AFRC	1	3	300.00%
TOTAL	1165	1127	96.74%



U.S. AIR FORCE

Career Field Snapshot

3D1X7 – Cable & Antenna Systems

as of: Mar 2016

Primary Role:

- Provides C2 capabilities through installation, mx of fixed cable, wireless distro systems and LANs
- Monitors performance of underground, buried, aerial cable and antenna networks
- Locates, repairs faulty closures in copper core, waveguide, coaxial, and fiber optic cable systems

On the Horizon:

- Working with CYSS antenna experts to identify antenna inventory, and develop a program get- well plan
- Specialty Training and Requirements Team tentatively scheduled for early FY17

Successes:

Challenges:

- Antenna PMI program issues
 - Most bases have civilian or contracted cable maintenance that do not cover antenna maintenance; bases have historically relied on ANG units to perform PMIs
 - Available MPA days has made this more difficult, forcing units to rely on 3D1X3s and 1C8X2s to become climb certified
 - Two 5 day courses available from Sheppard J7AST3D157 0C0B (mobile) and J3AZR3D1570C0B



Force Development Big Rocks

U.S. AIR FORCE

- **Communications Squadron Next affect to AFSCs**
- **JIE affect to AFSCs**
- **Modernizing Agility of Tech Training**
- **Manpower Standards... they are all old**
- **IMSC affect on MAJCOM Functional Management**
- **Drafting Cyberspace Professional Development Program AFI**

- **Officer Specific**
 - **B Prefix for Squadron DO positions (ongoing)**
- **Enlisted Specific**
 - **Updating JQS Training Products**



U.S. AIR FORCE

QUESTIONS?

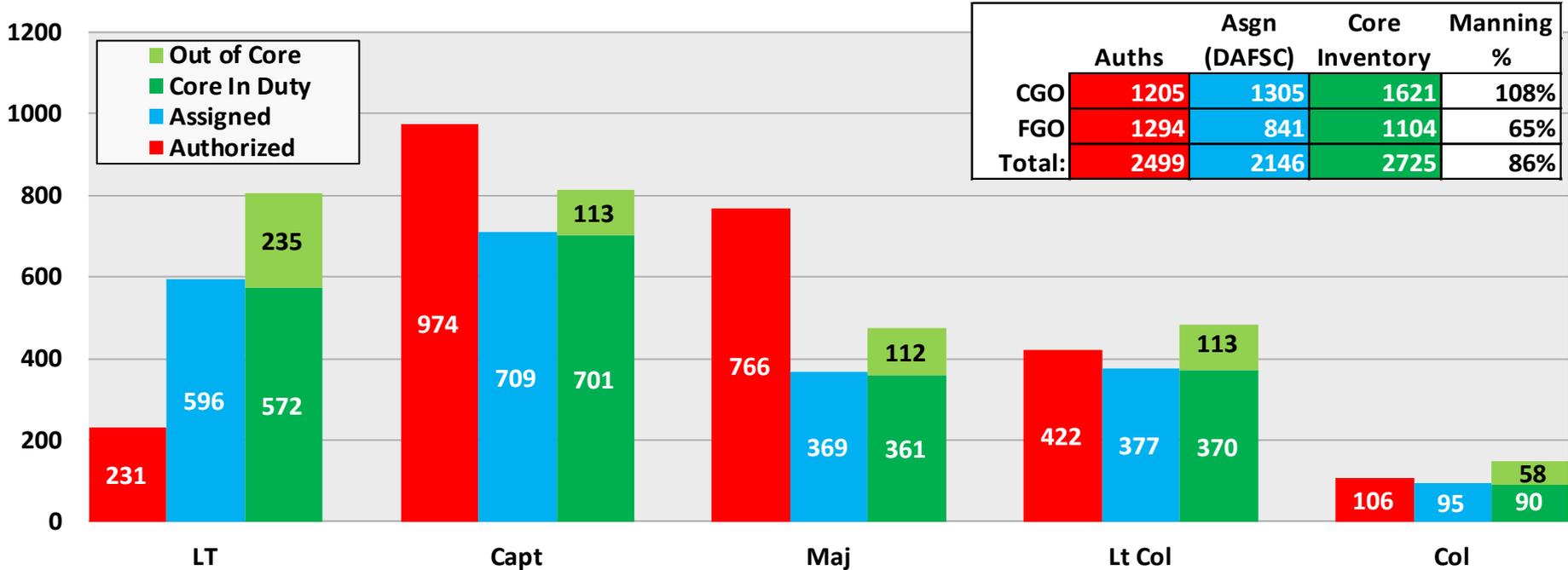


Integrity - Service - Excellence



17D Manning

U.S. AIR FORCE



■ Overall manning is 86%

■ CGO: 108%

■ FGO: 65%

A1 lists 17D as a stressed career field
Approximately 450 officers short

Data as of: 29 Feb 2016



Total - Enlisted Air Force

U.S. AIR FORCE

PP Auths, Inv, Manning	
End of Feb PP Auths	235,060
End of Feb No Fill PP Inv	224,815
Manning	95%

Sustainment Deviation	
Current (Goal = 0)	0.18

PERSTEMPO (A1PFR)	
% Time TDY	7%
Avg # of TDY days	2%
	9

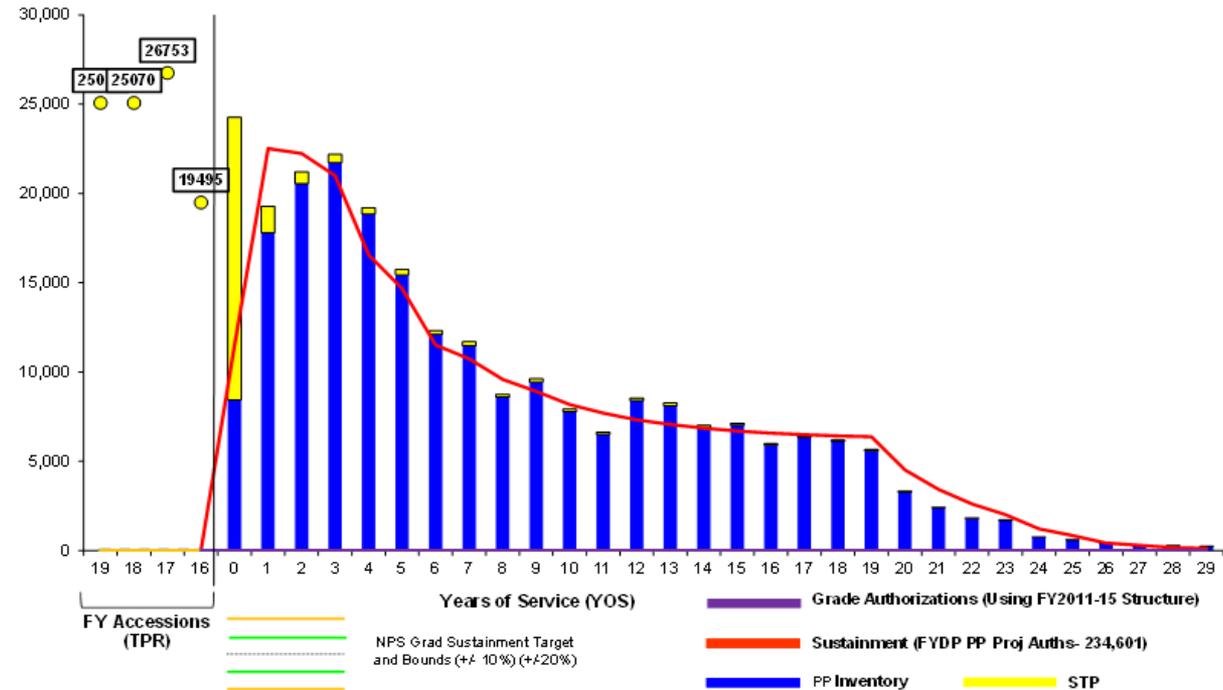
Ops Demand (AF/A1PFR)	
Current (Aug 2015)	5%

Stressed List Metrics	
Ops Demand	"N/A"
Career Field Health	"N/A"

Retraining		
Fiscal Year	Retrain-In	Retrain-Out
FY16	2,841	0
FY17	4,197	0
FY18	4,146	0

Grade Structure		
Grade	5-Yr Actual	Curr Auths
E1-E3	18.7%	20.7%
E4	22.9%	20.1%
E5	27.6%	28.4%
E6	16.8%	17.0%
E7	10.6%	10.5%
E8	2.1%	2.2%
E9	1.1%	1.1%

PP Inventory
Total - Enlisted Air Force



RETENTION - 1 year & 4 month trend									
RETENTION GOALS		Historical	Feb-15	Nov-15	Dec-15	Jan-16	Feb-16	% Plan Met	Zone Manning
ACL	8.84	10.17	8.22	10.54	10.50	10.50	10.73	121%	
Zone A	0.51	0.53	0.47	0.56	0.56	0.56	0.57	110%	97%
Zone B	0.60	0.68	0.53	0.67	0.67	0.66	0.67	110%	102%
Zone C	0.62	0.81	0.67	0.80	0.80	0.80	0.82	132%	101%
Zone E	0.70	0.67	0.52	0.62	0.63	0.63	0.62	88%	91%

NPS TPR		FY15
Upper Bound (+20%)		0
Upper Bound (+10%)		0
Sustainment Target		0
Lower Bound (-10%)		0
Lower Bound (-20%)		0
PGL		19,495
% Sustainment Met		N/A

17D/S (Cyber Operations)

Training Pipeline

(as of: 1 Jan 16)

- = USAF School
- = Joint School
- = ITRO School
- = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr Jim Rector AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 115

Average cost per graduate: \$65K

Today's Available Supplemental/Advanced Courses

Cyber 400 <u>5 Days</u> MTT	Cyberspace Officer Warfighting Integration Education <u>4 Days</u> Distance Learning	DCAPES MAJCOM FAM <u>3 Days</u> MTT	Cyberspace 200 <u>15 Days</u> AFIT, Wright Patterson AFB	Intermediate Network Warfare Training <u>41 Days</u> AFSPC, Hurlburt Field
Cyberspace Officer Engineer <u>15 Days</u> Distance Learning	Spectrum Operations Apprentice <u>58 Days</u> Keesler AFB	DCAPES MAJCOM Planner <u>4 Days</u> MTT	Cyberspace 300 <u>10 Days</u> AFIT, Wright Patterson AFB	Joint Network Attack Course <u>20 Days</u> Cory Station
				Joint C4 Planners Course <u>20 Days</u> Ft Gordon

Integrity - Service - Excellence

1B4X1 (Cyber Warfare Operations)

Training Pipeline

(as of: 11 Mar 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC



Total Days in Pipeline (including days between courses): 105

Average cost per 3-level graduate : \$67K

Today's Available Supplemental/Advanced Courses

Cyber Defense and Control
Operations IQT
26 Days
AFSPC, Hurlburt Field

Advanced
Cyber Warfare Operations
36 Days
AFSPC, Hurlburt Field

RIOT
Varies
NSA, Ft Meade

Cyberspace 200
15 Days
AFIT, Wright
Patterson AFB

Cyber Vulnerability
Assessment/Hunter
IQT
51 Days
AFSPC, Hurlburt Field

Air Force Cyber Defense
IQT
32 Days
AFSPC, Hurlburt Field

Cyberspace
Superintendent
60 Days
Distance Learning

Cyberspace 300
10 Days
AFIT, Wright
Patterson AFB

Integrity - Service - Excellence

3A1X1 (Administration)

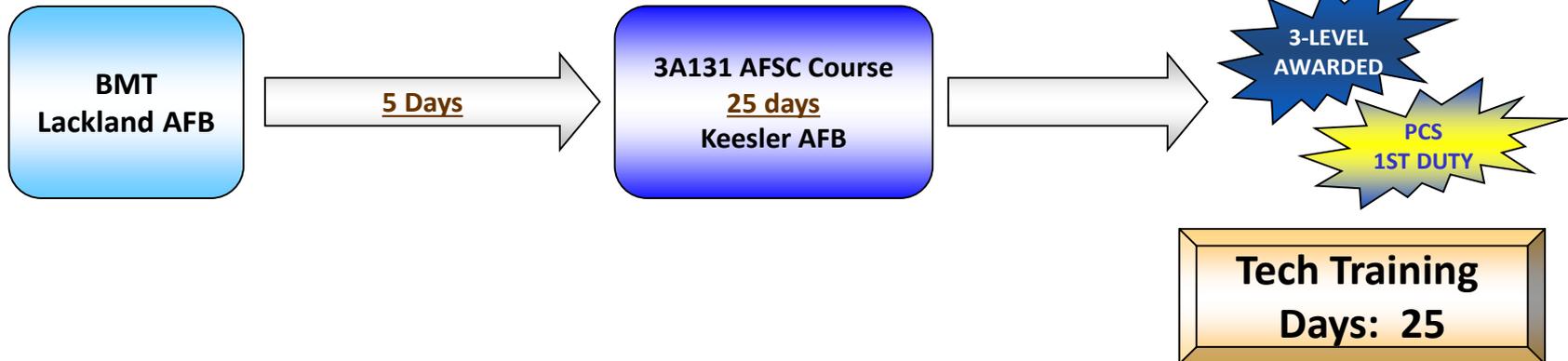
Training Pipeline

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 30

Average cost per graduate (Recruitment through ISC): \$36K

Today's Available Supplemental/Advanced Courses

Postal Operations Course
23 days
Ft Jackson SC



U.S. AIR FORCE

PP Auths, Inv, Manning	
End of Feb PP Auths	6,934
End of Feb No Fill PP Inv	7,093
Manning	102%

Sustainment Deviation	
Current (Goal = 0)	0.00

PERSTEMPO (A1PFR)	
% Time TDY	5%
Avg # of TDY days	5

Ops Demand (AF/A1PFR)	
Current (Aug 2015)	0%

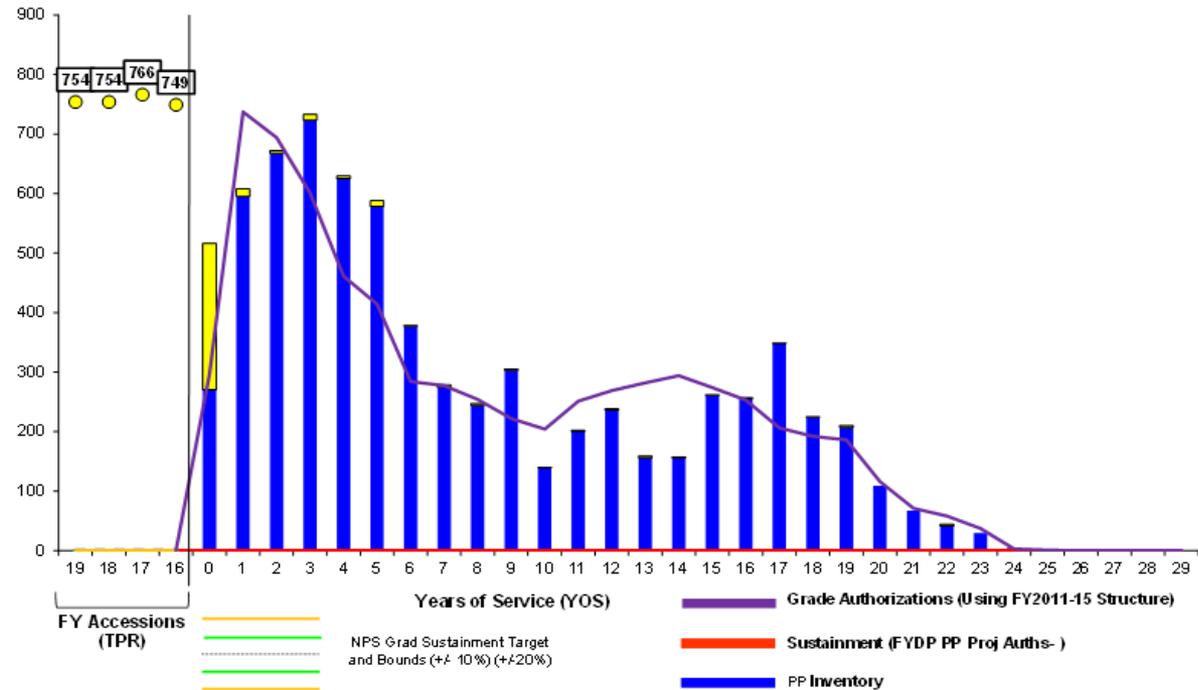
Stressed List Metrics	
Ops Demand	"N/A"
Career Field Health	"N/A"

Retraining		
Fiscal Year	Retrain-In	Retrain-Out
FY16	81	0
FY17	74	0
FY18	74	0

Grade Structure		
Grade	5-Yr Actual	Curr Auths
E1-E3	19.9%	8.8%
E4	20.9%	22.1%
E5	25.9%	33.1%
E6	19.6%	21.4%
E7	13.6%	14.6%
E8	0.2%	0.0%
E9	0.0%	0.0%

PP Inventory
3D0 -

End of Feb 16
Gray bars show DSDs serving outside AFSC



RETENTION - 1 year & 4 month trend									
RETENTION GOALS		Historical	Feb-15	Nov-15	Dec-15	Jan-16	Feb-16	% Plan Met	Zone Manning
ACL	12.06	11.38	7.38	11.31	17.67	11.32	566.18	4692%	
Zone A	0.62	0.60	0.39	0.59	0.75	0.60	0.63	100%	-
Zone B	0.80	0.71	0.50	0.69	0.82	0.67	0.63	78%	-
Zone C	0.84	0.83	0.55	0.85	0.91	0.85	0.82	98%	-
Zone E	0.60	0.66	0.42	0.72	0.84	0.70	0.69	114%	-

NPS TPR		FY15
Upper Bound (+20%)		0
Upper Bound (+10%)		0
Sustainment Target		0
Lower Bound (-10%)		0
Lower Bound (-20%)		0
PGL		749
% Sustainment Met		N/A

3D0X1 (Knowledge Operations)

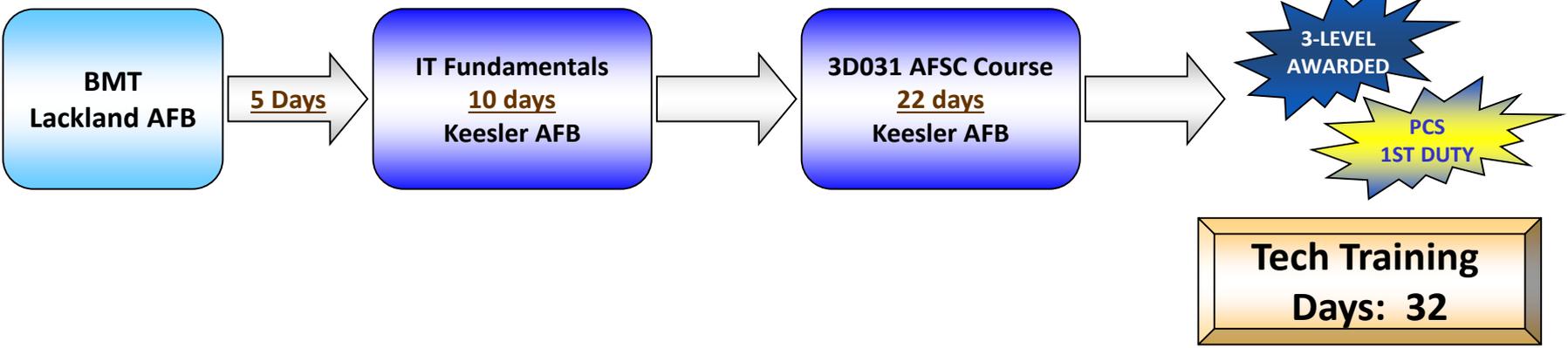
Training Pipeline

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 37

Average cost per graduate (Recruitment through ISC): \$36K

Today's Available Supplemental/Advanced Courses

- Project Management**
10 Days
Keesler AFB
- Cyberspace Supp Quality Assurance Procedures**
10 Days
Keesler AFB/MTT
- Cyberspace Career Advancement**
60 Days
Distance Learning
- Cyberspace Superintendent**
60 Days
Distance Learning

3D0X2 (Cyber Systems Operations)

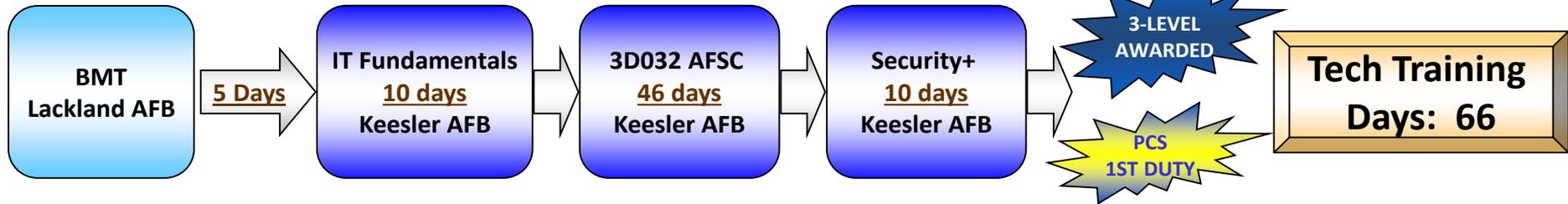
Training Pipeline (slide 1 of 2)

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 71

Average cost per graduate (Recruitment through ISC): \$42K

Today's Available Supplemental/Advanced Courses

Cyberspace Superintendent
60 Days
Distance Learning

Cyberspace Career Advancement
60 Days
Distance Learning

GCCS-J Advanced System Administration
5 Days
Keesler AFB/MTT

GCCS-J Installation Familiarization
10 Days
Keesler AFB/MTT

Project Management
10 Days
Keesler AFB

Cyberspace Supp Quality Assurance Procedures
10 Days
Keesler AFB/MTT

GCCS-J I3 Familiarization
5 Days
Keesler AFB/MTT

GCCS-J Situational Awareness Familiarization
5 Days
Keesler AFB/MTT

3D0X2 (Cyber Systems Operations)

Training Pipeline (slide 2 of 2)

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469

Today's Available Supplemental/Advanced Courses

Theater Deployable
Communications
Network
Control Center –
Deployed
15 Days
Robins AFB

Theater Deployable
Communications
Network
Control Center –
Deployed - Extended
20 Days
Savannah ARB

3D0X3 (Cyber Surety)

Training Pipeline

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 45

Average cost per graduate (Recruitment through ISC): \$36K

Today's Available Supplemental/Advanced Courses

COMSEC Account Manager/EKMS
15 Days
Keesler AFB

Information Systems Security Manager
10 Days
Keesler AFB

Project Management
10 Days
Keesler AFB

PKI/LRA
4 Days
Keesler AFB

Cyberspace Supp Quality Assurance Procedures
10 Days
Keesler AFB/MTT

Cyberspace Superintendent
60 Days
Distance Learning

Emission Security Manager
5 Days
Keesler AFB

Key Management Infrastructure (KMI)
15 Days
Keesler AFB

Cyberspace Career Advancement
60 Days
Distance Learning

Integrity - Service - Excellence

Return

3D0X4 (Computer Systems Programming)

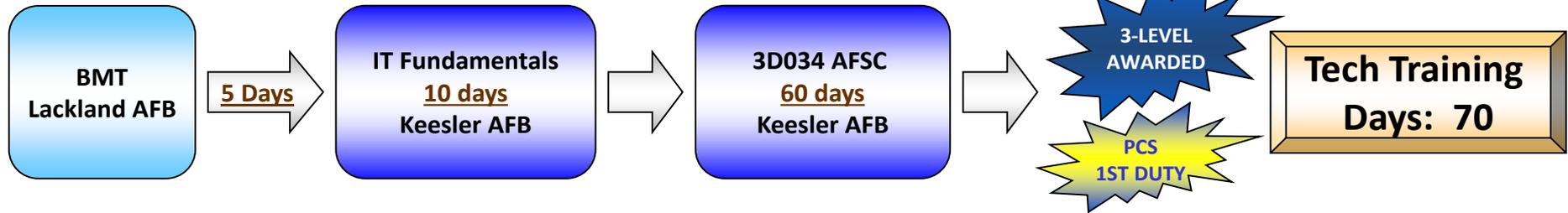
Training Pipeline

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 75

Average cost per graduate (Recruitment through ISC): \$45K

Today's Available Supplemental/Advanced Courses

Project Management
10 Days
Keesler AFB

Cyberspace Supp Quality Assurance Procedures
10 Days
Keesler AFB/MTT

GCCS-J Database Fundamentals
5 Days
Keesler AFB/MTT

GCCS-J Oracle Administration
5 Days
Keesler AFB/MTT

Cyberspace Career Advancement
60 Days
Distance Learning

Cyberspace Superintendent
60 Days
Distance Learning

GCCS-J Sybase Administration
5 Days
Keesler AFB/MTT



3D1 -

U.S. AIR FORCE

PP Auths, Inv, Manning	
End of Feb PP Auths	11,754
End of Feb No Fill PP Inv	11,356
Manning	96%

Sustainment Deviation	
Current (Goal = 0)	0.00

PERSTEMPO (A1PFR)	
% Time TDY	12%
Avg # of TDY days	7

Ops Demand (AF/A1PFR)	
Current (Aug 2015)	0%

Stressed List Metrics	
Ops Demand	"N/A"
Career Field Health	"N/A"

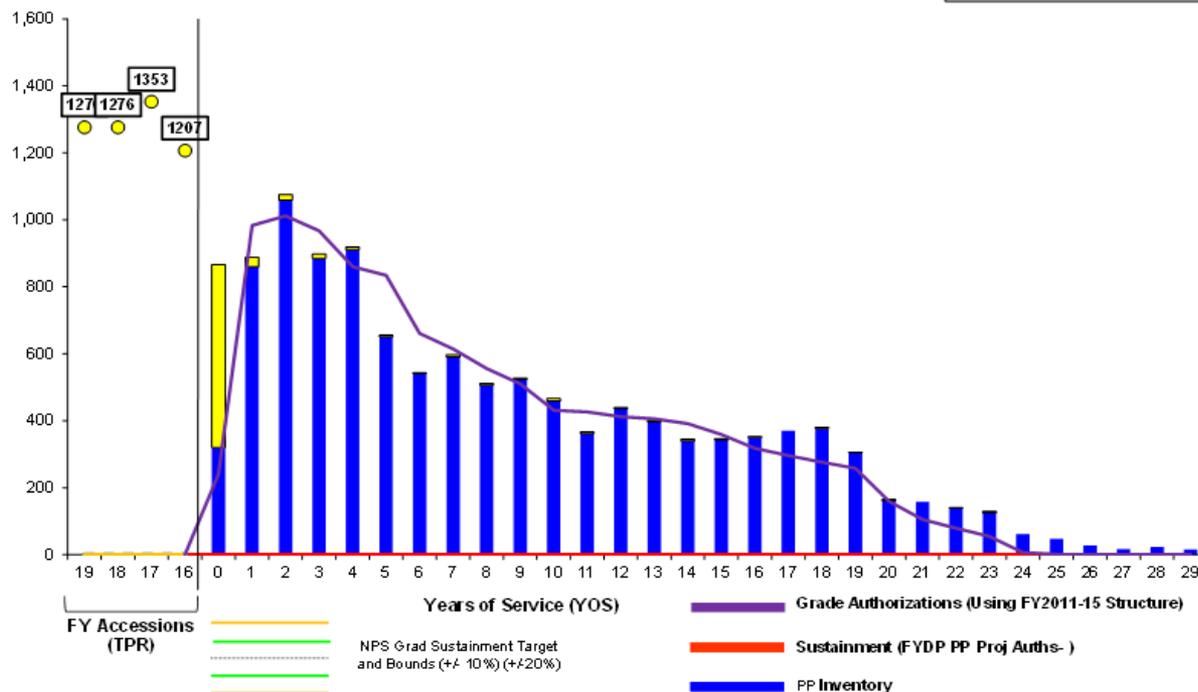
Retraining		
Fiscal Year	Retrain-In	Retrain-Out
FY16	80	0
FY17	78	0
FY18	78	0

Grade Structure		
Grade	5-Yr Actual	Curr Auths
E1-E3	14.9%	14.1%
E4	21.9%	19.9%
E5	30.1%	32.2%
E6	17.4%	18.6%
E7	10.7%	10.5%
E8	0.4%	3.6%
E9	4.5%	1.2%

PP Inventory
3D1 -

End of Feb 16

Gray bars show DSDs serving outside AFSC



RETENTION - 1 year & 4 month trend									
RETENTION GOALS		Historical	Feb-15	Nov-15	Dec-15	Jan-16	Feb-16	% Plan Met	Zone Manning
ACL	12.26	12.00	8.49	10.69	15.73	10.99	582.19	4746%	-
Zone A	0.64	0.61	0.53	0.57	0.69	0.57	0.58	91%	-
Zone B	0.68	0.70	0.47	0.59	0.70	0.60	0.68	98%	-
Zone C	0.77	0.84	0.60	0.74	0.78	0.73	0.88	113%	-
Zone E	0.69	0.66	0.43	0.50	0.64	0.49	0.58	84%	-

NPS TPR		FY15
Upper Bound (+20%)		0
Upper Bound (+10%)		0
Sustainment Target		0
Lower Bound (-10%)		0
Lower Bound (-20%)		0
PGL		1,207
% Sustainment Met		N/A

3D1X1 (Client Systems)

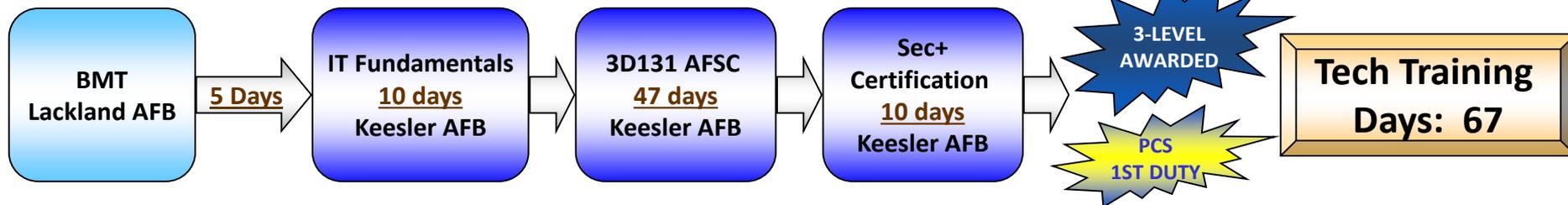
Training Pipeline

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 72

Average cost per graduate (Recruitment through ISC): \$43K

Today's Available Supplemental/Advanced Courses

Cyberspace Supp Quality Assurance Procedures
10 Days
Keesler AFB/MTT

Cyberspace Career Advancement
60 Days
Distance Learning

Project Management
10 Days
Keesler AFB

Cyberspace Superintendent
60 Days
Distance Learning

Integrity - Service - Excellence

Return

3D1X2 (Cyber Transport Systems)

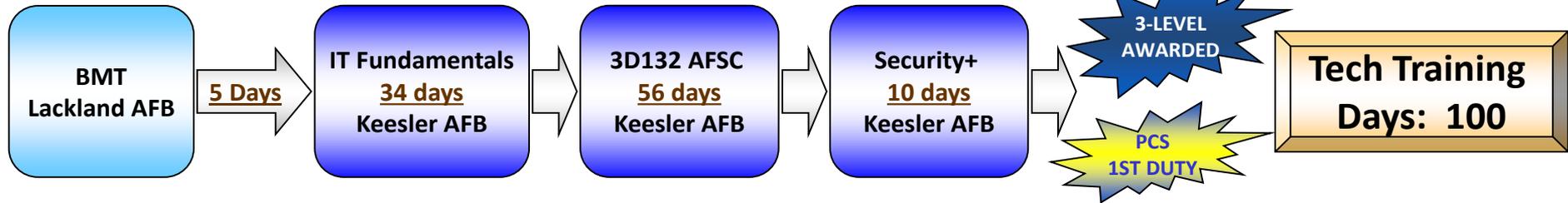
Training Pipeline (slide 1 of 3)

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 105

Average cost per graduate (Recruitment through ISC): \$61K

Today's Available Supplemental/Advanced Courses

Modular Control
Equipment Org Maint
33 Days
Keesler AFB

Cyberspace Supp Quality
Assurance Procedures
10 Days
Keesler AFB/MTT

Cyberspace
Superintendent
60 Days
Distance Learning

Network Management
Infrastructure Associate
15 Days
Keesler AFB

Global Broadcast
Service Systems
5 Days
Distance Learning

Project Management
10 Days
Keesler AFB

Cyberspace Career
Advancement
60 Days
Distance Learning

Network Management
Infrastructure Professional
15 Days
Keesler AFB

3D1X2 (Cyber Transport Systems)

Training Pipeline (slide 2 of 3)

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469

Today's Available Supplemental/Advanced Courses

Meridian 1 Opt 61C
5 Days
Sheppard AFB

AS5300 Config, Maint,
and Admin
10 Days
Sheppard AFB

High Reliability
Soldering & Connections
10 Days
Keesler AFB

TSEC/KG-30 Series
Depot Maint (STP)
18 Days
On Site

Digital
Voice Switching
25 Days
Sheppard AFB

Avaya Voice
Network Switching
10 Days
Sheppard AFB

TSEC/KG-30 Series
Limited Maint (STP)
5 Days
On Site

TSEC/KY-99
Limited Maint (STP)
5 Days
On Site

Telecommunications
Mgmt System
5 Days
Sheppard AFB

Cisco Call Manager
5 Days
Sheppard AFB

TSEC/KG-81
Limited Maint (STP)
5 Days
On Site

TSEC/KG-40A
Limited Maint (STP)
5 Days
On Site

Voice Translations
10 Days
Sheppard AFB

Telephony Install
And Maint Tech
5 Days
Sheppard AFB

TSEC/KG-84 Series
Limited Maint (STP)
5 Days
On Site

TSEC/KG-95 Series
Depot Maint (STP)
5 Days
On Site

3D1X2 (Cyber Transport Systems)

Training Pipeline (slide 3 of 3)

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469

Today's Available Supplemental/Advanced Courses

TSEC/KI-1 Series
Limited Maint (STP)
5 Days
On Site

TSEC/CI-10
Limited Maint (STP)
5 Days
On Site

TRI-TAC COMSEC
Equipment Limited
Maint (STP)
5 Days
On Site

TSEC/KY-57/58
Limited Maint (STP)
5 Days
On Site

TSEC/KY-68/78
Limited Maint (STP)
5 Days
On Site

TSEC/KY-90
Limited Maint (STP)
5 Days
On Site

(STP) COMSEC
Awareness
1 Days
On Site

TSEC/KGV-8/11 Series
ST-61 Depot Maint (STP)
5 Days
On Site

TSEC/KG-83 Operational
Certification Training (STP)
5 Days
On Site

3D1X3 (RF Transmission Systems)

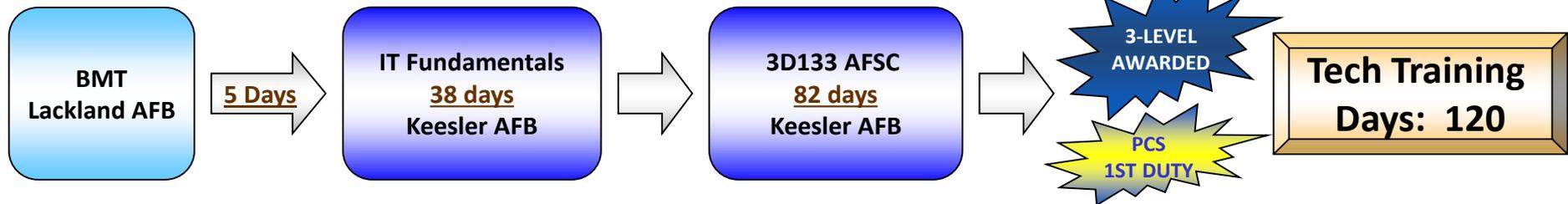
Training Pipeline (slide 1 of 2)

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 125

Average cost per graduate (Recruitment through ISC): \$62K

Today's Available Supplemental/Advanced Courses

**MILSTAR
Ops & Maintenance**
27 Days
Ft Gordon

**Ground Multi-band
Terminal O/I Maintenance**
10 Days
Ft Gordon/MTT

**Expeditionary Combat
Supp Radio Comm**
12 Days
Keesler AFB

Project Management
10 Days
Keesler AFB

**Cyberspace Supp Quality
Assurance Procedures**
10 Days
Keesler AFB/MTT

**High Reliability
Soldering & Connections**
10 Days
Keesler AFB

**Cyberspace
Superintendent**
60 Days
Distance Learning

**Cyberspace Career
Advancement**
60 Days
Distance Learning

3D1X3 (RF Transmission Systems)

Training Pipeline (slide 2 of 2)

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469

Today's Available Supplemental/Advanced Courses

MILSTAR Smart-T
17 Days
Ft Gordon

Digital Comm
Satellite Subsystems
61 Days
Ft Gordon

Theater Deployable
Communications
RF Transmission
Systems
15 Days
Robins AFB

AEH Mission Planning
Element (MPE) Comm
Planning - Tactical
10 Days
Ft Gordon

Expeditionary
Cyberspace Mission
Integration Training
TDC Cyber
15 Days
Robins AFB

Theater Deployable
Communications
RF Transmission
Systems - Extended
20 Days
Savannah ARB

SATCOM Strategic
Terminals
49 Days
Ft Gordon

Theater Deployable
Communications
Cyber Transport
Systems/Infrastructure
- Extended
20 Days
Savannah ARB

3D1X4 (Spectrum Operations)

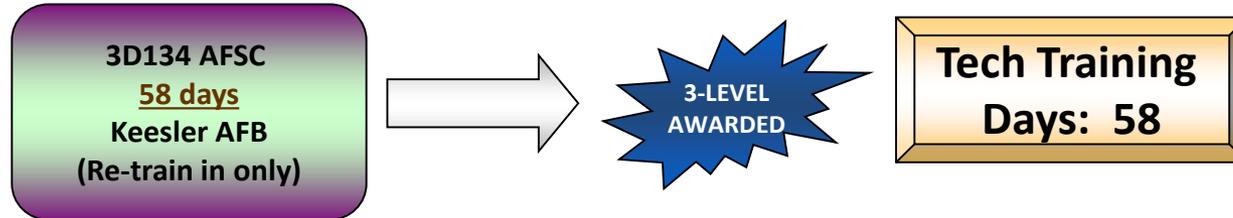
Training Pipeline

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 58

Average cost per graduate (Recruitment through ISC): \$50K

Today's Available Supplemental/Advanced Courses

Joint Task Force
Spectrum Mgt
13 Days
Keesler AFB

Cyberspace Supp Quality
Assurance Procedures
10 Days
Keesler AFB/MTT

Cyberspace
Superintendent
60 Days
Distance Learning

Project Management
10 Days
Keesler AFB

Cyberspace Career
Advancement
60 Days
Distance Learning

3D1X7 (Cable & Antenna Systems)

Training Pipeline

(as of: 1 Jan 16)

-  = USAF School
-  = Joint School
-  = ITRO School
-  = Other School

Today's Training Pipeline for Award of AFSC

OPR: Mr. Jim Rector, AETC/A3TC, DSN 487-9469



Total Days in Pipeline (including days between courses): 82

Average cost per graduate (Recruitment through ISC): \$53K

Today's Available Supplemental/Advanced Courses

Tower Climbing & Certifier Training
5 Days
Sheppard AFB/MTT

Cyberspace Career Advancement
60 Days
Distance Learning

Project Management
10 Days
Keesler AFB

Cyberspace Superintendent
60 Days
Distance Learning

Cyberspace Supp Quality Assurance Procedures
10 Days
Keesler AFB/MTT

High Reliability Soldering & Connections
10 Days
Keesler AFB

Fiber Optic Cable Inst, Splicing and Mnt
8 Days
Sheppard/MTT (5 days)

Integrity - Service - Excellence

Return 136



3DXXX Common Core

U.S. AIR FORCE

as of: Oct 2015

- **Specialty Training Requirements Team (SRT)**
 - Held @ Keesler AFB June 2016 or Aug 2016
- **All MAJCOMs and Agencies reviewed draft 3DXXX training plan; focused on *continuum of training* for Cyberspace Support**
- **IT Fundamentals adjusted to include more applicable subjects and appropriate depth**
- **Electronics Principles (EP) reviewed for modernization**
- **5-Level Common Core CDCs better reflect entry-level knowledge**
- **7-Level Course to be converted to CDCs; integrated with promotion testing**
- **9-Level Course will focus more on Superintendent skills**
- **3DXXX CFETP to be published Summer 2014**

DEPARTMENT OF THE AIR FORCE
Headquarters US Air Force
Washington, DC 20330-1030

CFETP 3DXXX
Parts I and II
TBD

AFSC 3DXXX

CYBERSPACE SUPPORT

1. TASKS, KNOWLEDGE AND TECHNICAL REFERENCES	2. CORE & WARTIME TASKS	3. Certification for OJT				4. PROFICIENCY CODES USED TO INDICATE TRAINING INFORMATION PROVIDED				
		A	B	C	D	3 SKILL LEVEL	3 SKILL LEVEL	5 SKILL LEVEL	7 SKILL LEVEL	9 SKILL LEVEL
		START DATE	STOP DATE	TRAINEE INITIALS	TRAINER INITIALS	ITF Course	ITF-EP Course	CDC	CDC	OJT
1. INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)										
1.1. Overview	-					A	-	A	A	-
1.2. Service Strategy	-					A	-	A	A	-
1.3. Service Design	-					A	-	A	A	-
1.4. Service Transition	-					A	-	A	A	-
1.5. Service Operation	-					A	-	A	A	-
1.6. Continual Service Improvement	-					A	-	A	A	-
2. SAFETY & OPERATIONAL RISK MANAGEMENT (ORM) TR: AFIs 90-901, 91-203, 91-302										
2.1. Safety	5					B	-	A	-	-
2.2. ORM	5					A	-	A	A	-
2.3. Practice safety precautions:										
2.3.1. Maintenance actions	-					-	B	-	-	-
2.3.2. Energized equipment	-					-	B	-	-	-

Combat Communications Update



Col Keith Mueller
5 CCG/CC



Overview

- Historical Operations
- Force Structure
- TDC Program
- Challenges
- CCSG Initiatives
- Successes





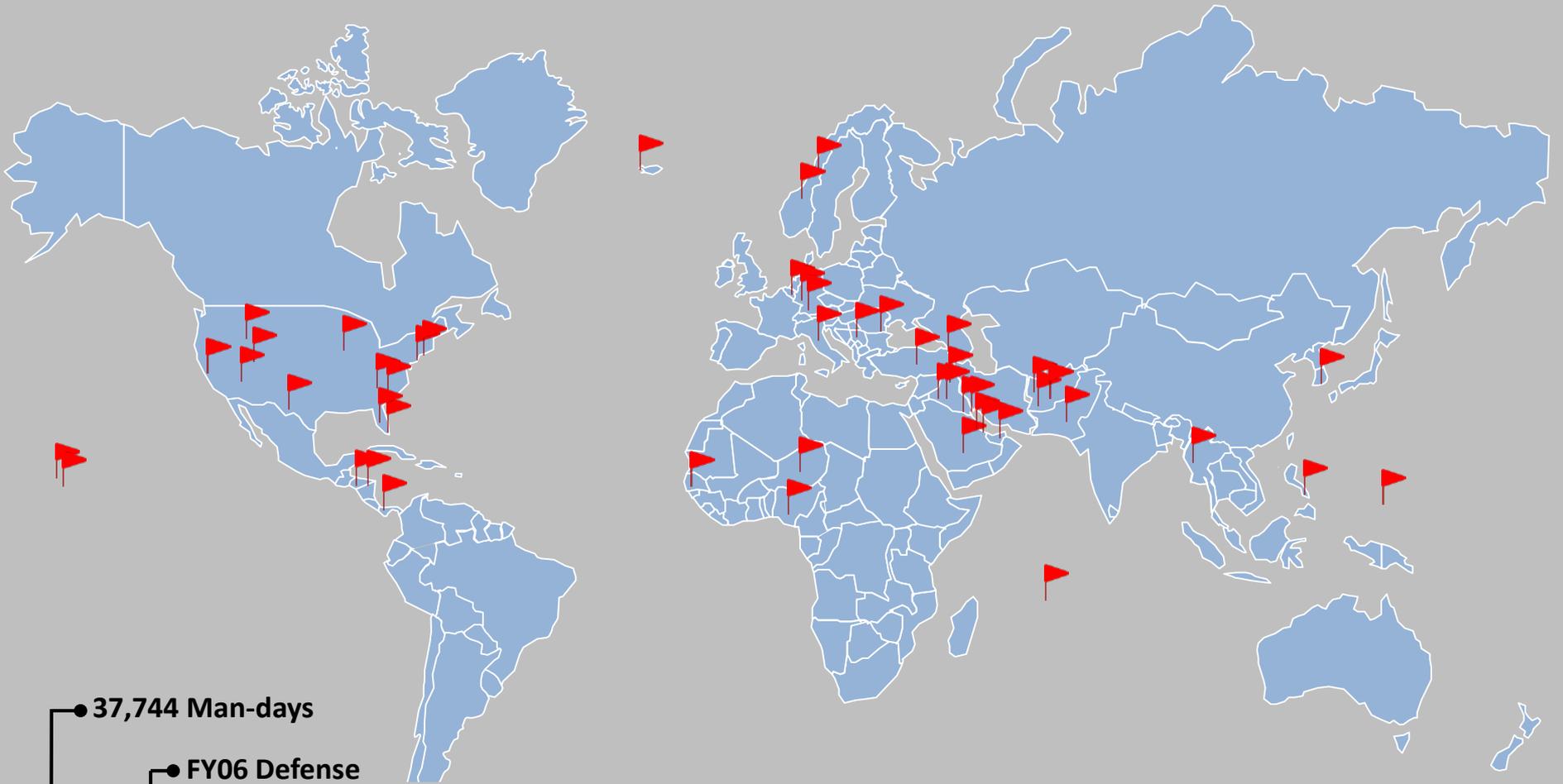
**Combat Communications
Operations, 2006-Present**

Combat Comm Deployments



2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016

Combat Comm Deployments

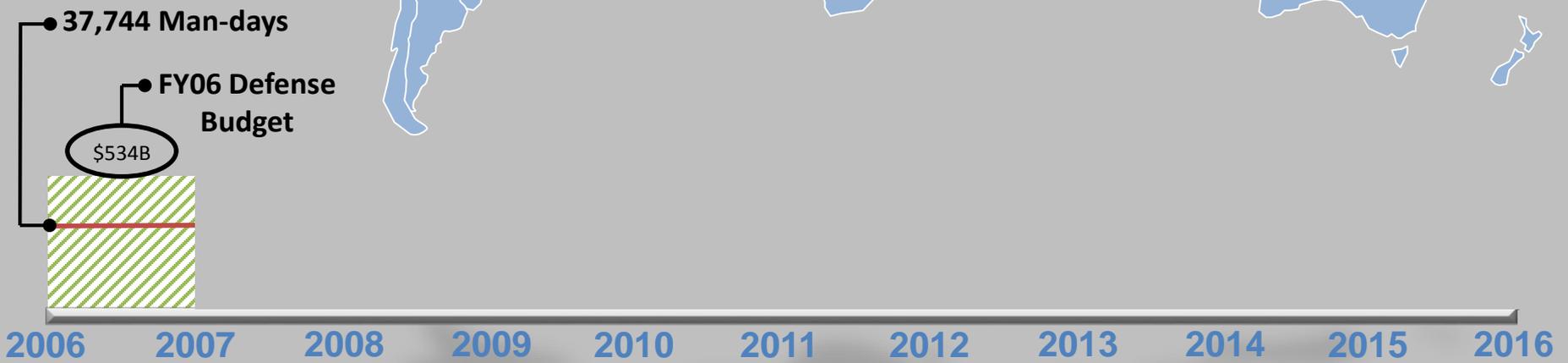
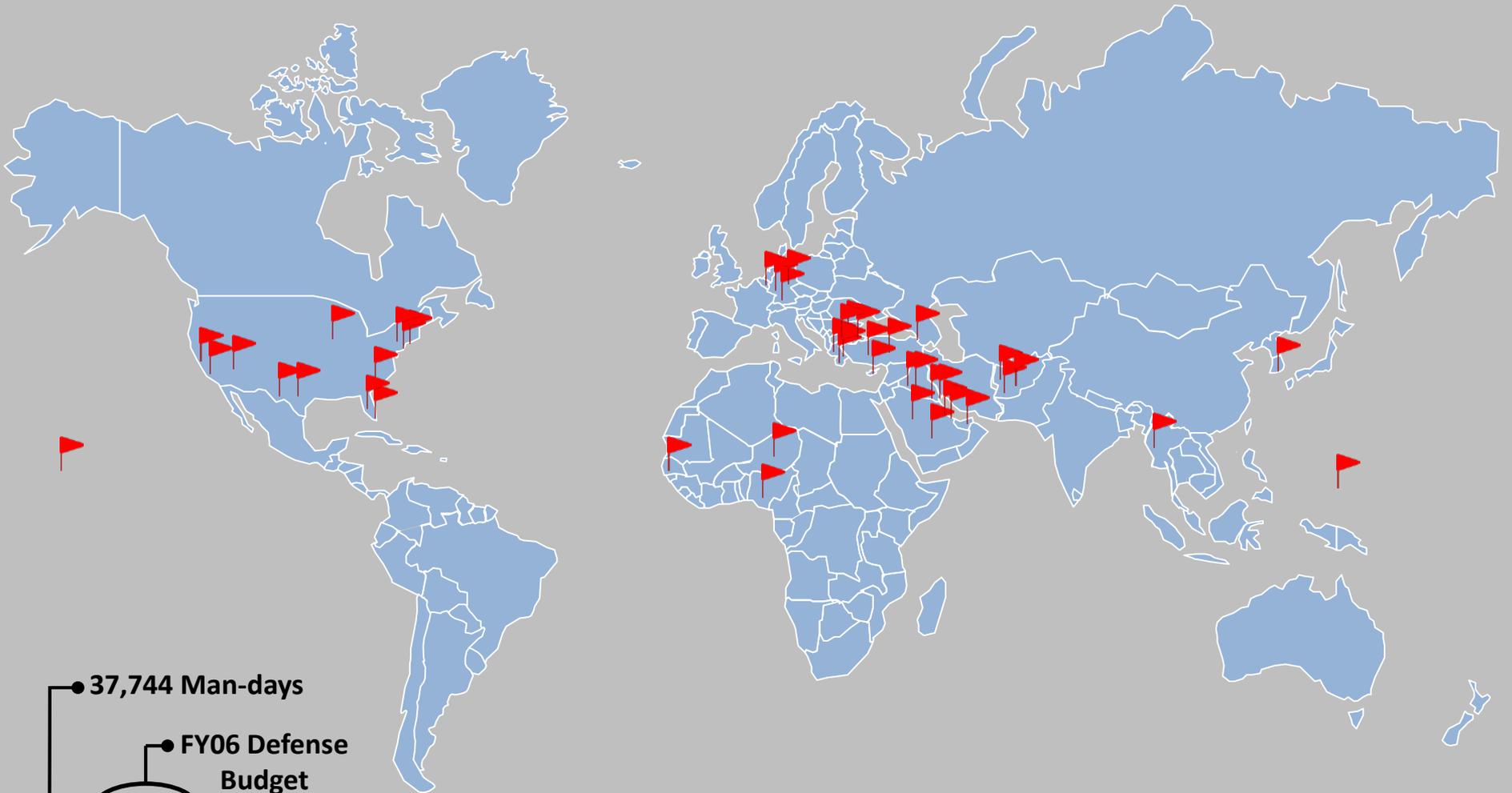


● 37,744 Man-days
● FY06 Defense Budget

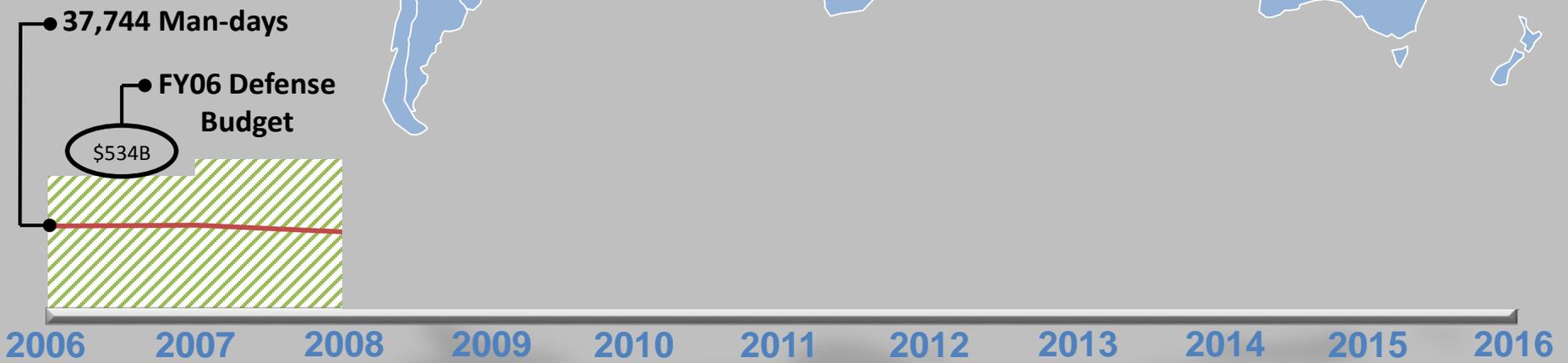
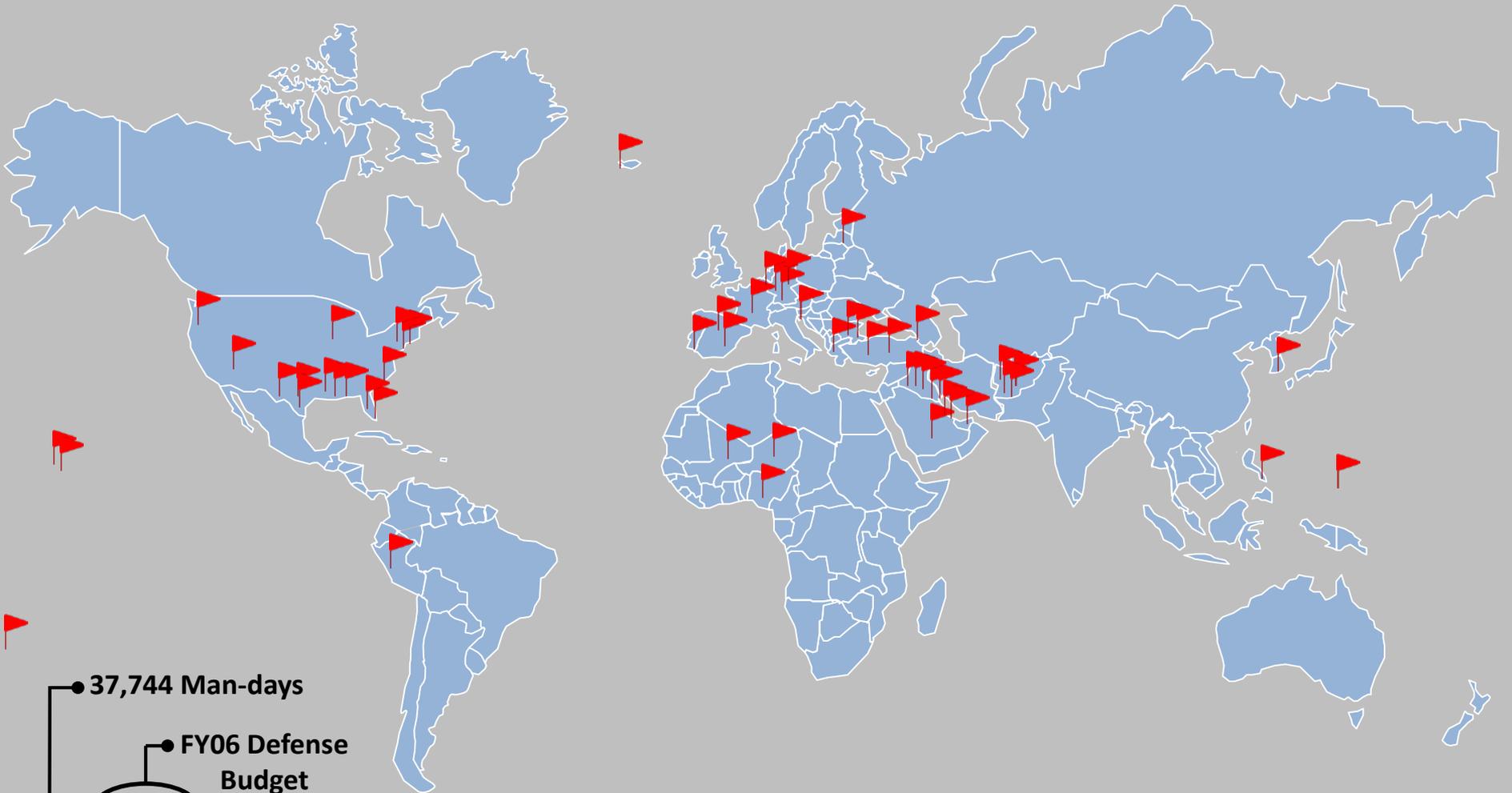
A diagram consisting of a black line that starts from the text, goes down, then right, then up, and finally curves into a circle on the map. The circle is positioned over the United States, representing the FY06 Defense Budget.



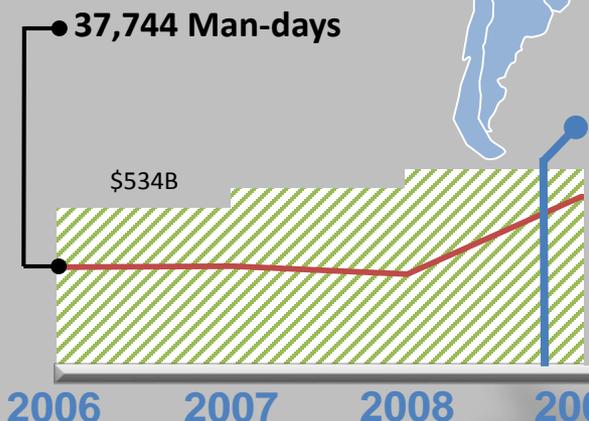
Combat Comm Deployments



Combat Comm Deployments



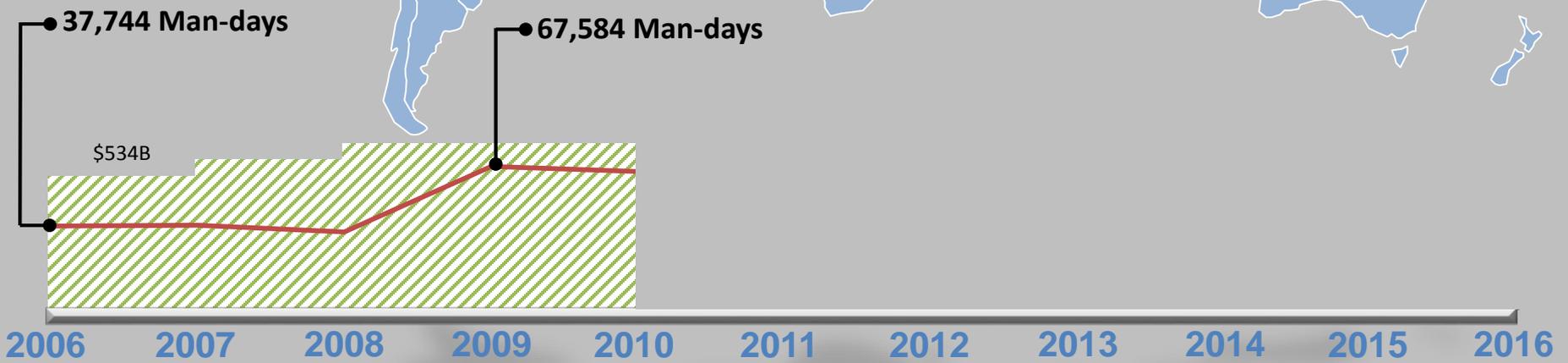
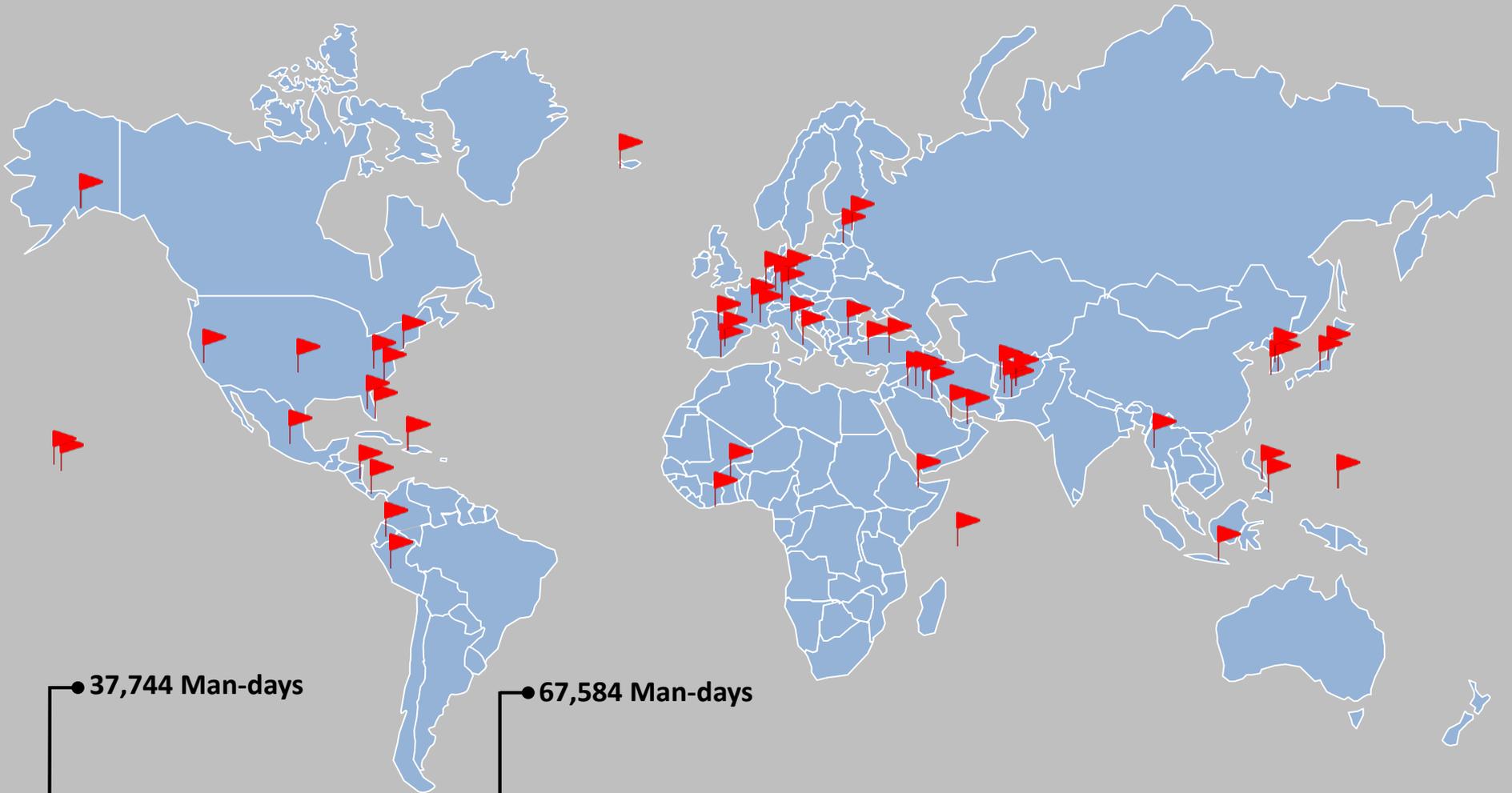
Combat Comm Deployments



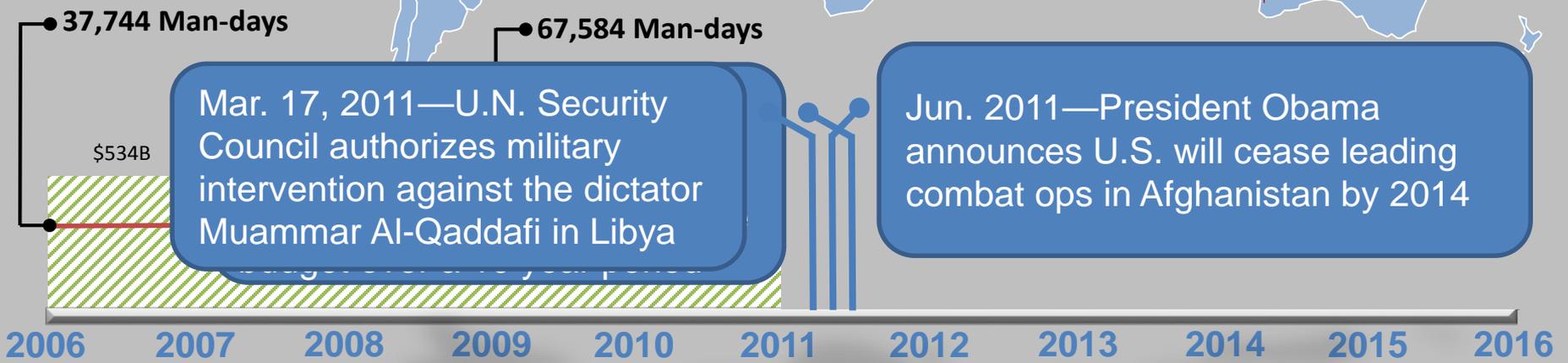
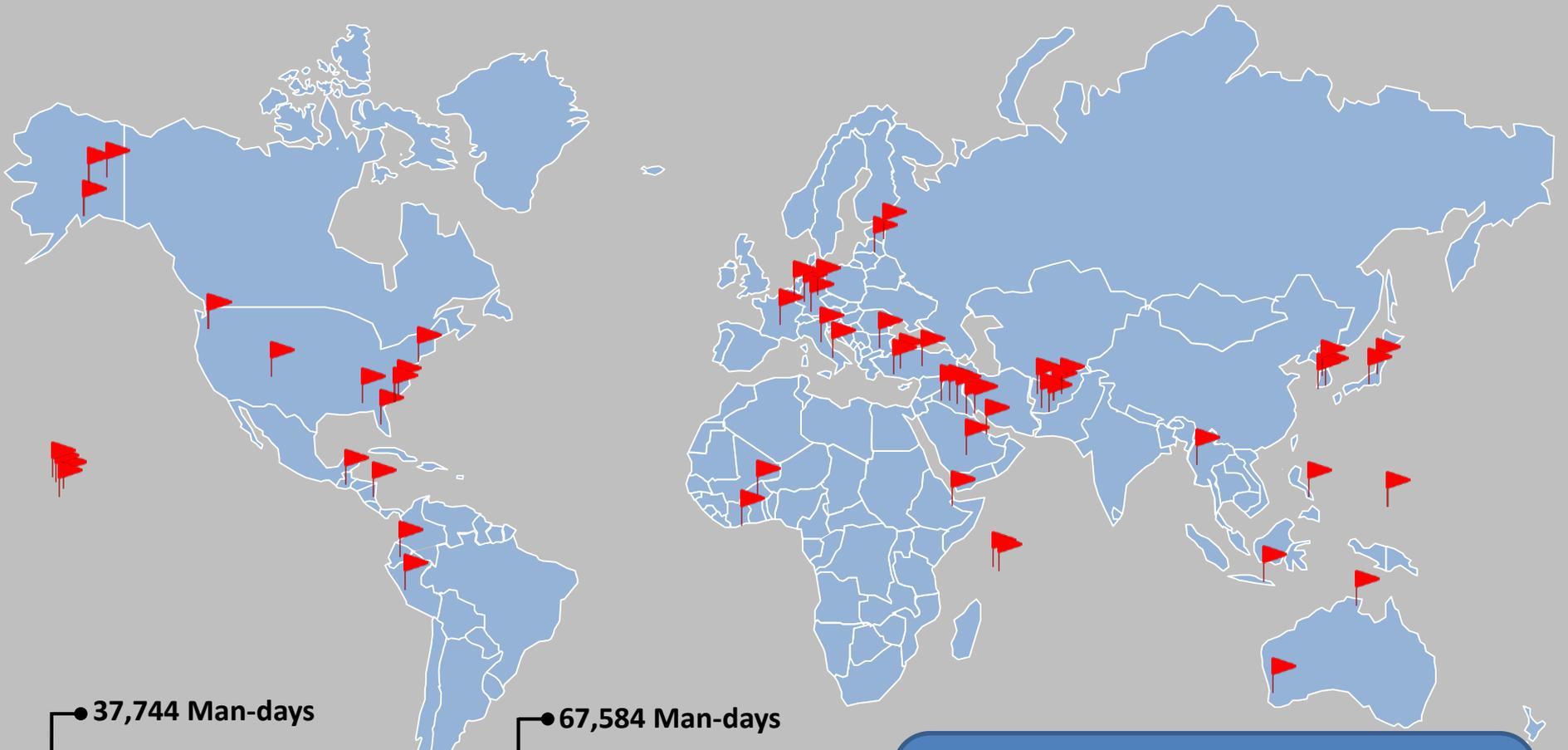
Dec. 1, 2009—President Obama announces the deployment of 30,000 additional troops, bringing U.S. strength to nearly 100,000 boots on the ground in addition to NATO's 40,000 troops

2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016

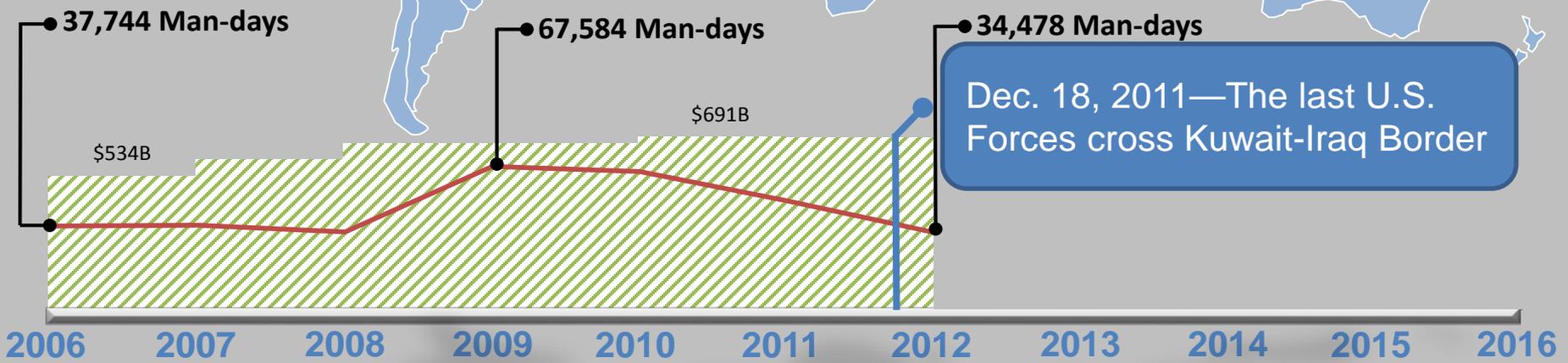
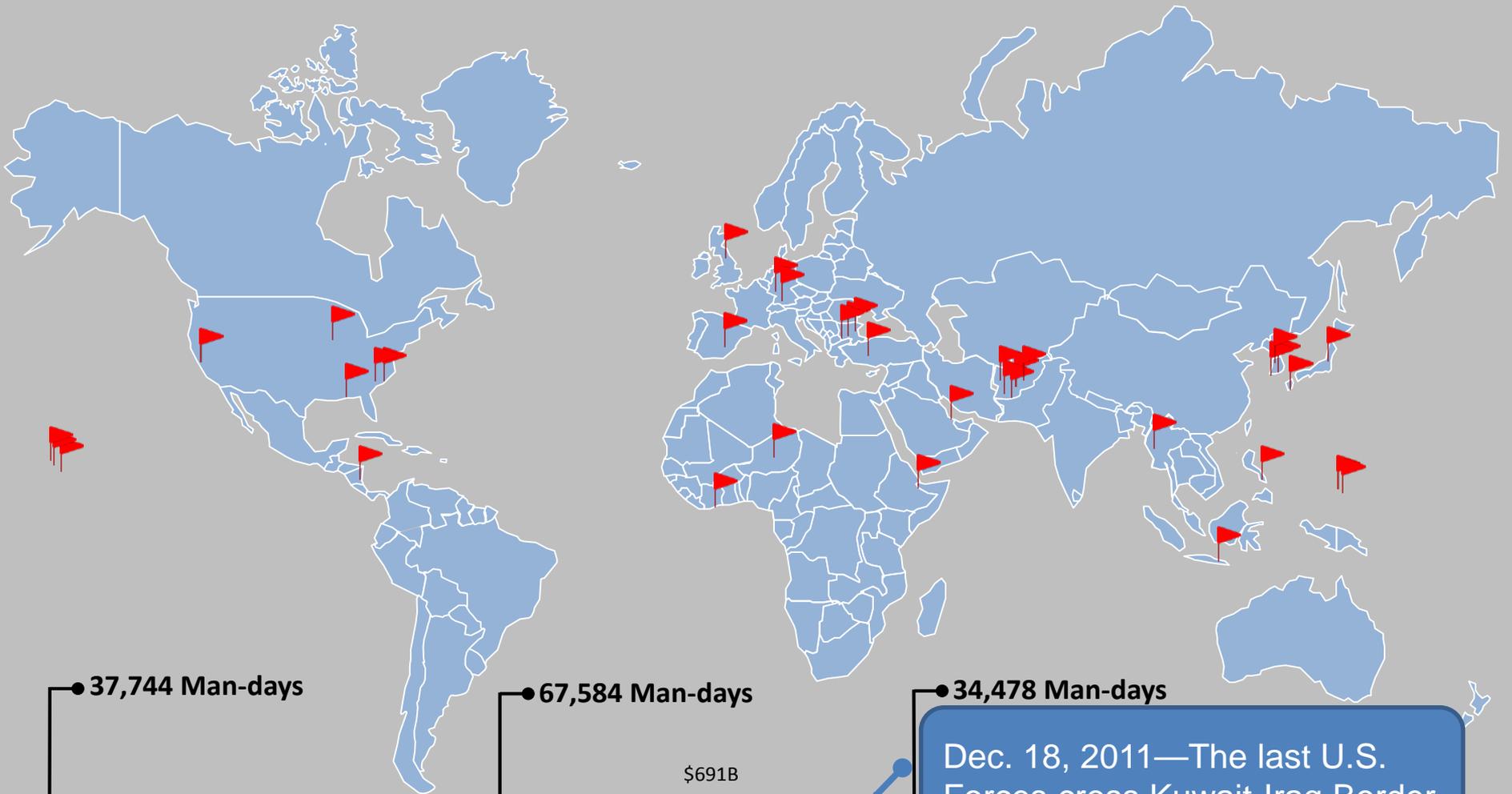
Combat Comm Deployments



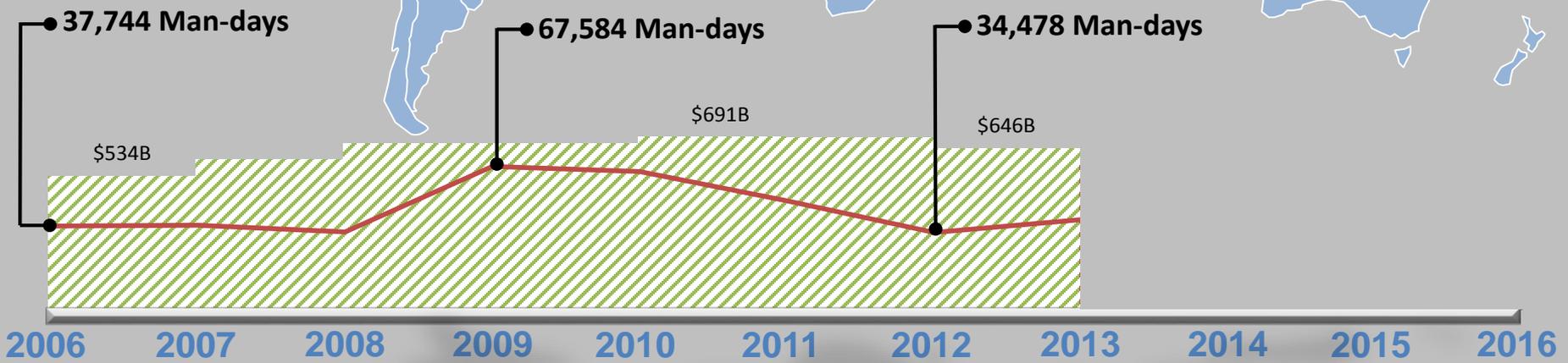
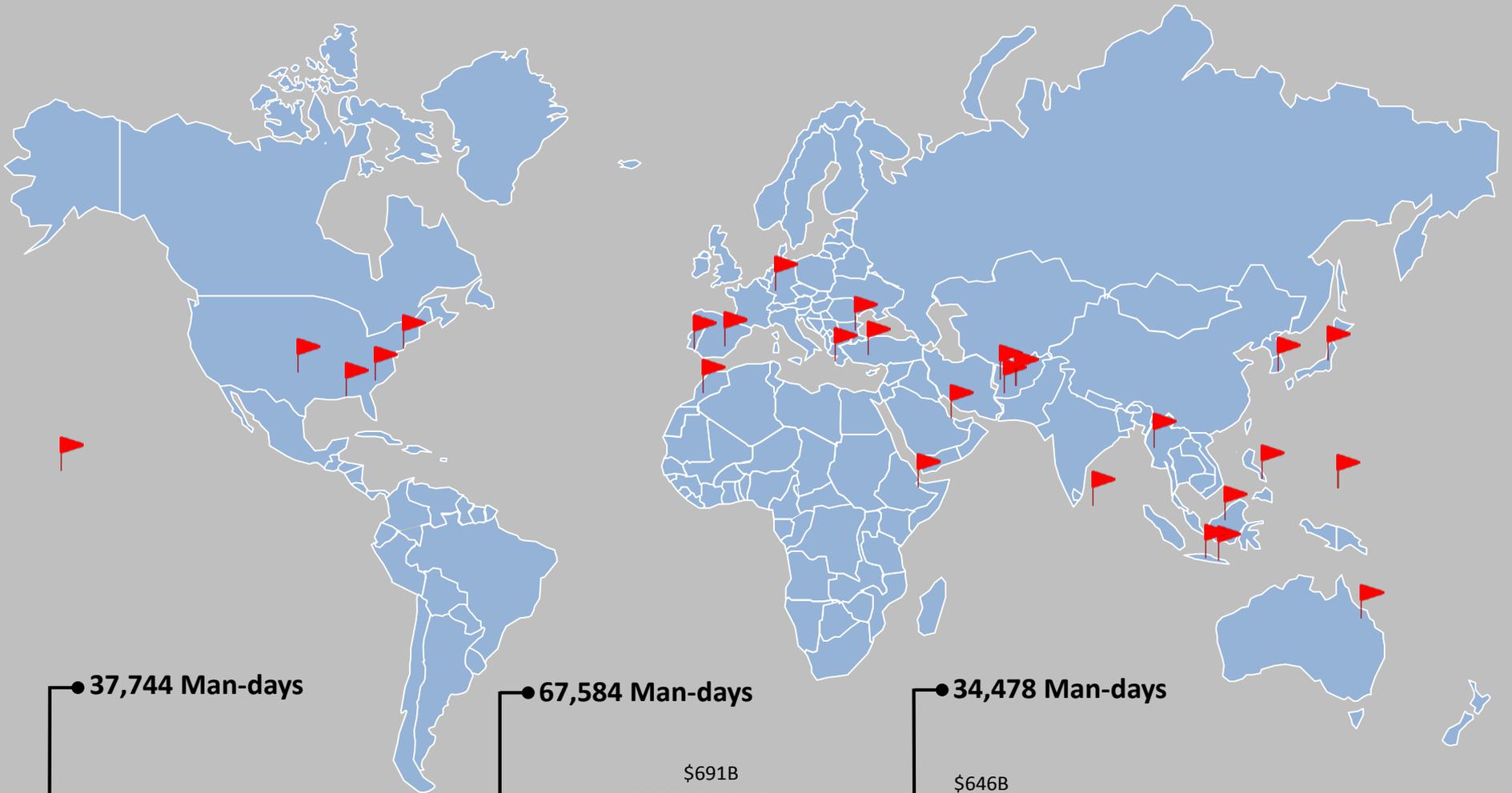
Combat Comm Deployments



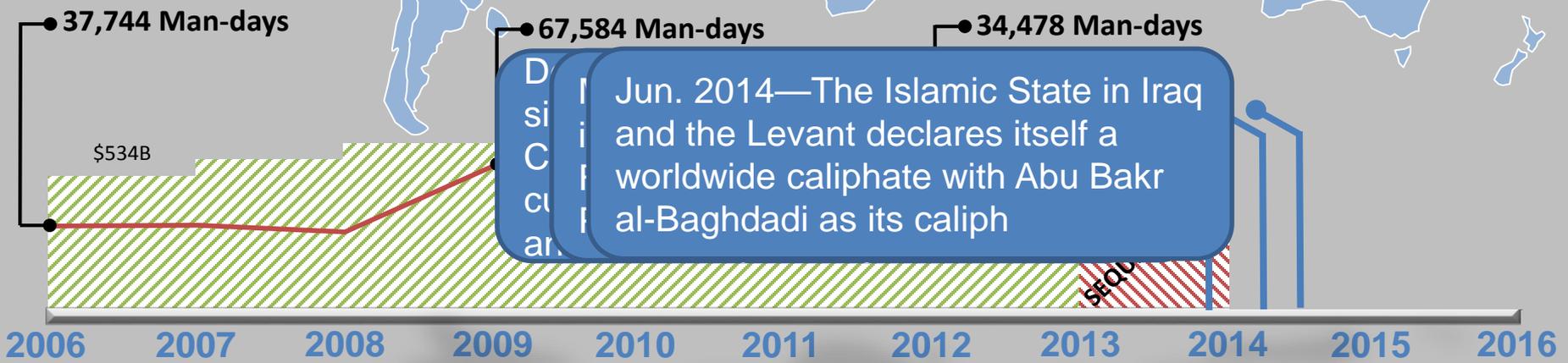
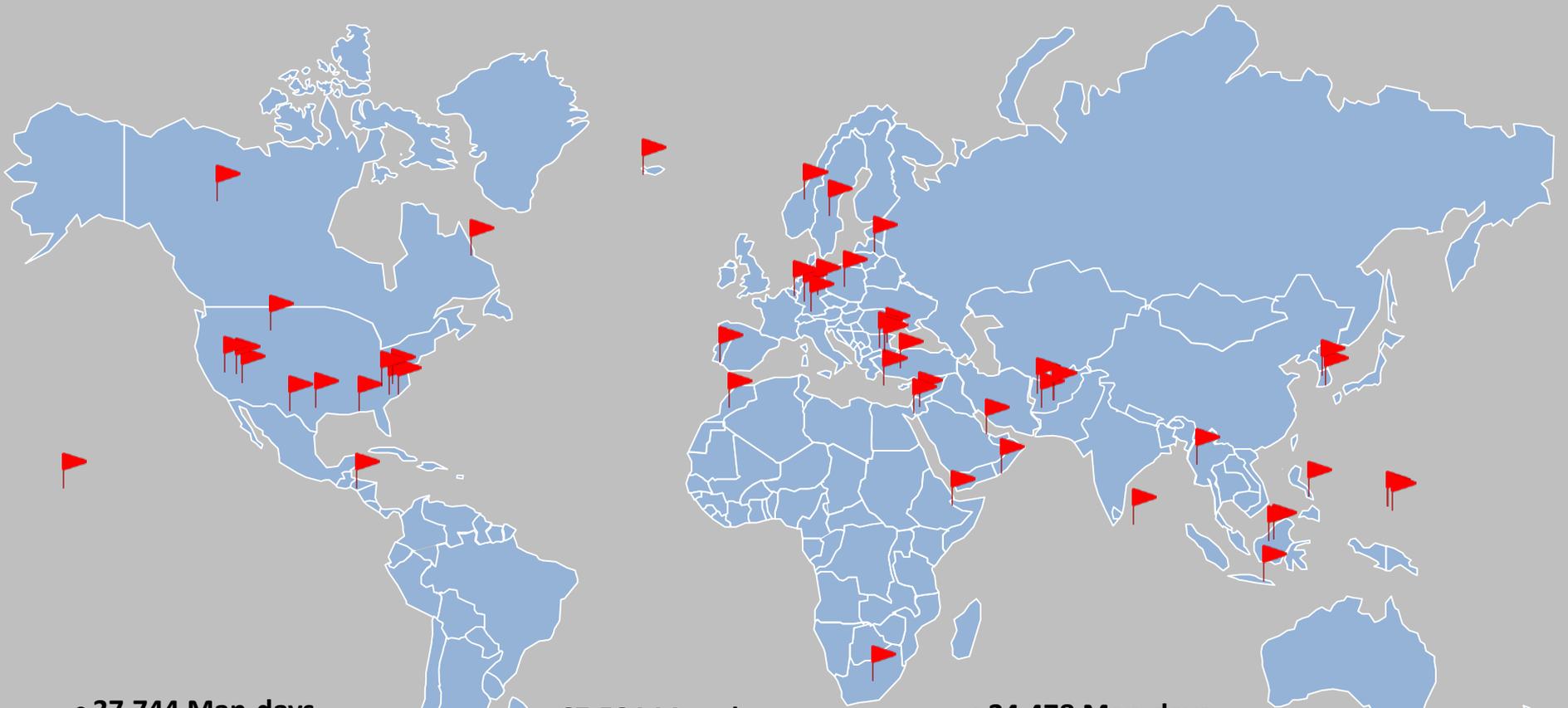
Combat Comm Deployments



Combat Comm Deployments

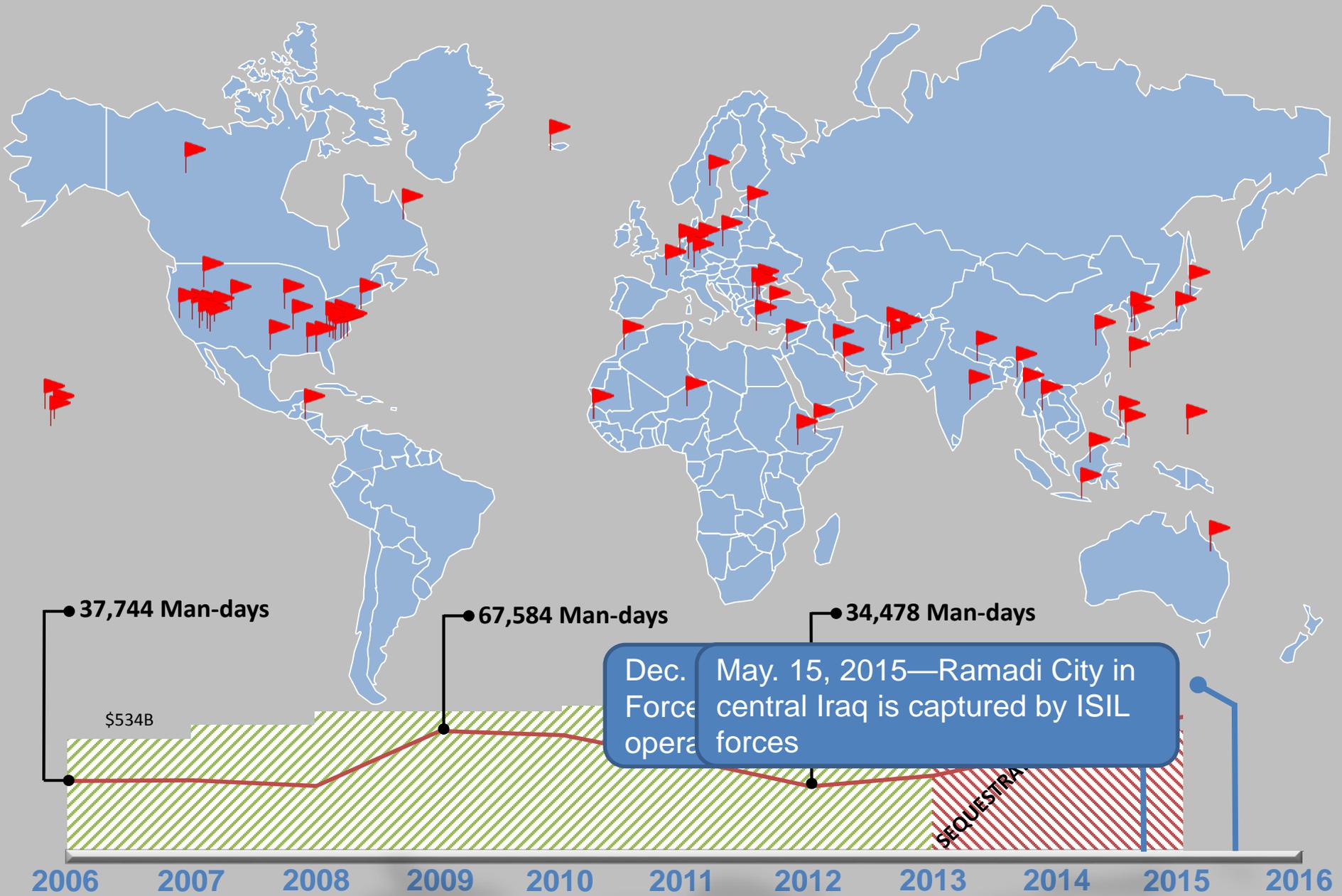


Combat Comm Deployments

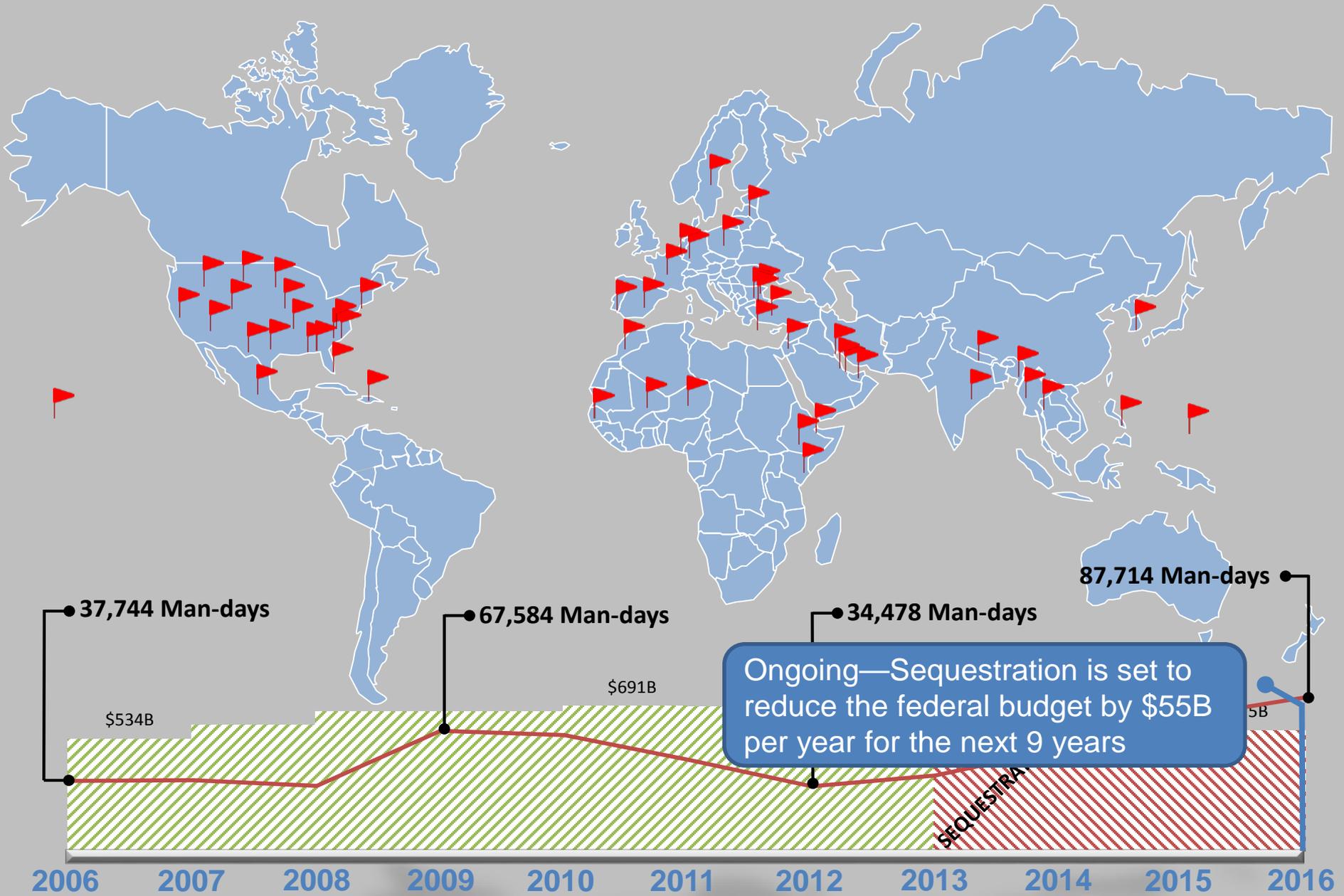


Jun. 2014—The Islamic State in Iraq and the Levant declares itself a worldwide caliphate with Abu Bakr al-Baghdadi as its caliph

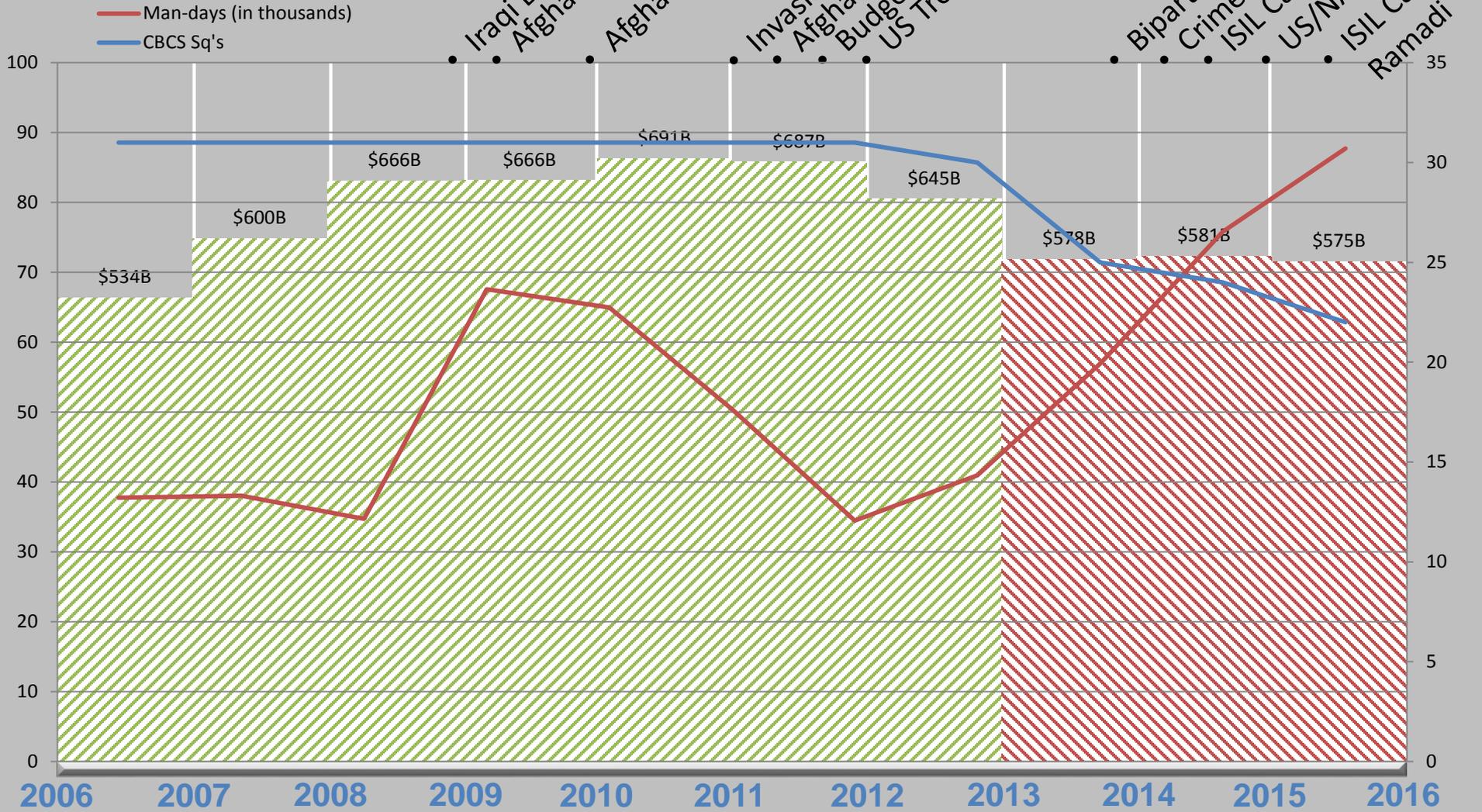
Combat Comm Deployments



Combat Comm Deployments



Summary





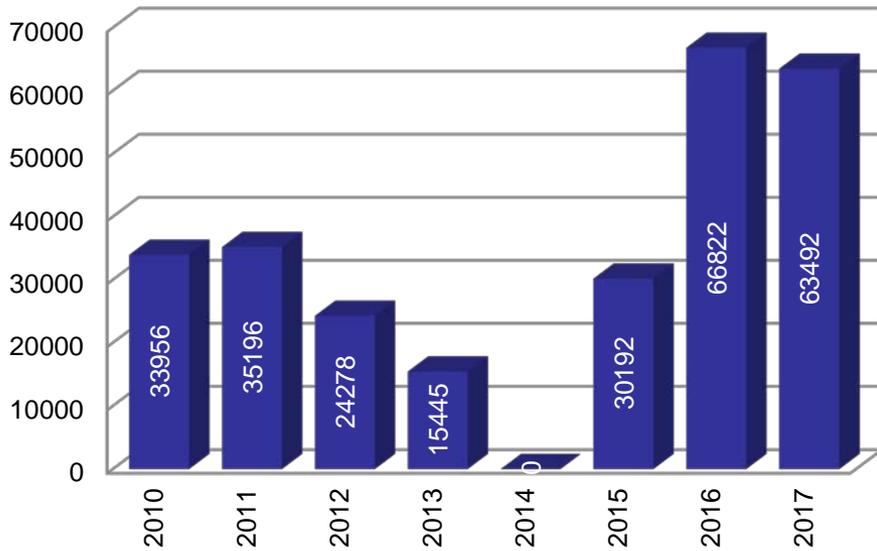
EUCOM FY15 vs FY16 ARC Support

<p><u>FY15 1 CBCS SUPPORT</u> NOBLE ARROW, Oct 14 JUNIPER THUNDER, Jan 15 A-10 TSP, Mar 15 Icelandic Air Surveillance, Mar 15 AV-DET Poland, Mar 15 HEDGEHOG, Apr 15 Icelandic Air Surveillance, Apr 15 ARCTIC CHALLENGE, May 15 SAD Support, May 15 ANATOLIAN EAGLE, May 15 TSP Romania, Jun 15 BALTOPS, Jun 15 SABRE STRIKE, Jun 15 TSP Estonia, Aug 15 JUNIPER THUNDER, Aug 15 IMMEDIATE RESPONSE, Sep 15 African Air Chief Symp, Sep 15</p>	<p><u>FY15 ARC SUPPORT</u> AFRICAN LION, May 15 (55 CBCS)</p>	<p style="text-align: center;"><u>Bottom Line</u></p> <hr/> <p>Exercise Relief: 0.06%</p> <p>Equipment Savings: 1x BRE</p> <p>Manpower Savings: 8 Pax</p>
<p><u>FY16 1 CBCS SUPPORT</u> TSP 16.1 Oct 15 BLUE FLAG FTD, Oct 15 TRIDENT JUNCTURE, Oct 15 SAD SUPPORT, Nov 15 Greece FTD, Jan 16 JC-16, Feb 16 REAL THAW, Feb 16 INIOHOS, Apr 16 CAMDEX, Apr 16 ANATOLIAN FALCON, May 16 STEADFAST COBALT, May 16 SABER STRIKE, Jun 16 TSP 16-2, Mar 16 (5 Micro-Deployments)</p>	<p><u>FY16 ARC SUPPORT</u> DACIAN VIPER, Oct 15 (280 SOSC ANG) AV-DET 16-1, PO, Oct 15 (264 CBCS ANG) COLD RESPONSE, Feb 16 (265 CBCS ANG) AV-DET 16-2, PO, Mar 16 (23 CBCS AFRC) Finland FTD, May 16 (147 CBCS ANG) SABER STRIKE, Jun 15 (147 CBCS ANG) AV-DET 16-3, PO, Jun 16 (239 CBCS ANG) BALTOPS, Jun 16 (221 CBCS ANG) Romania OST, Jul 16 (35 CBCS AFRC) AV-DET 16-4, PO, Aug 16 (221 CBCS ANG) Slovakia FTD, Aug 16 (221 CBCS ANG) Hungary FTD, Jul 16 (221 ANG) A-10 Amari FTD, Jul 16 (23 CBCS AFRC) 493d Amari, Aug 16 (55 CBCS AFRC) Ample Strike, Aug 16 (55 CBCS AFRC)</p>	<p style="text-align: center;"><u>Bottom Line</u></p> <hr/> <p>Exercise Relief: 48%</p> <p>Equipment Savings: 13x BREs // 12x TFKs</p> <p>Manpower Savings 95 Pax</p>

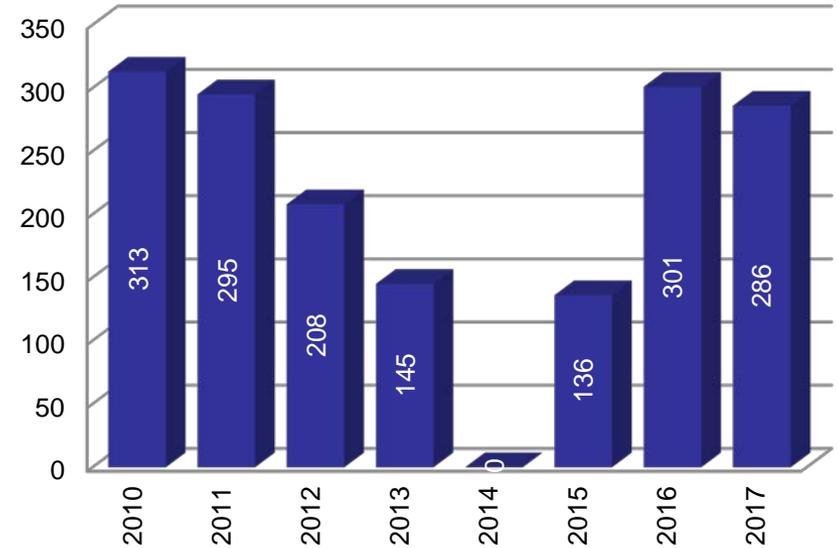
Delivering CONUS-based CBCS capacity ... Equivalent of a 2nd squadron for USAFE

ANG Combat Communications Deployment History

Deployed Mandays



Deployed Personnel



YEAR	2010	2011	2012	2013	2014	2015	2016	*2017
CCG	8	4	4	2	2	2	2	2
SQ	28	23	18	17	17	17	15	15
YEAR	2010	2011	2012	2013	2014	2015	2016	2017
Deployed PAX	313	295	208	145	0	136	301	286
TOTAL	33956	35196	24278	15445	0	30192	66822	63492

*Deployed Mandays (est)



2011

Force Strength: 44 AEW (LCP)

Combat Comm Sqdns: 10 AD / 17 ANG / 4 AFR

- AFMA Manpower Study 2011
- ISAG 2011
- CORONA 2011
- Deployable Comm CONOPS 2012
- 3 CCG/689 CCW Inactivation 2013
- PAD Dec 2013
- FY15 Alt POM

2016

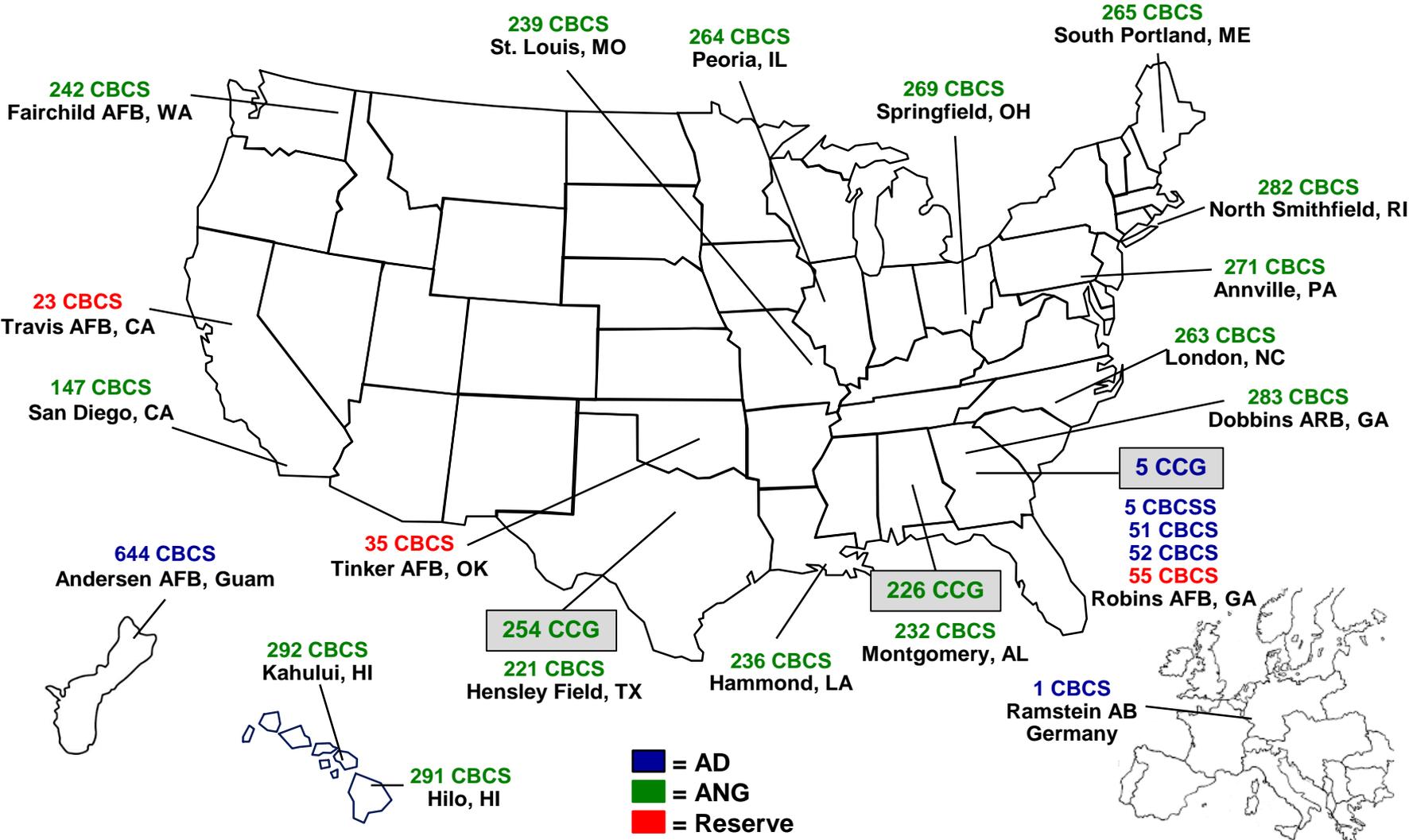
Force Strength: 22 LCP, 23 (27) MCP, 16 (55) SCP

Combat Comm Sqdns: 4 AD / 15 ANG / 3 AFR

New Mission: "Extend the Net" for ACC Units

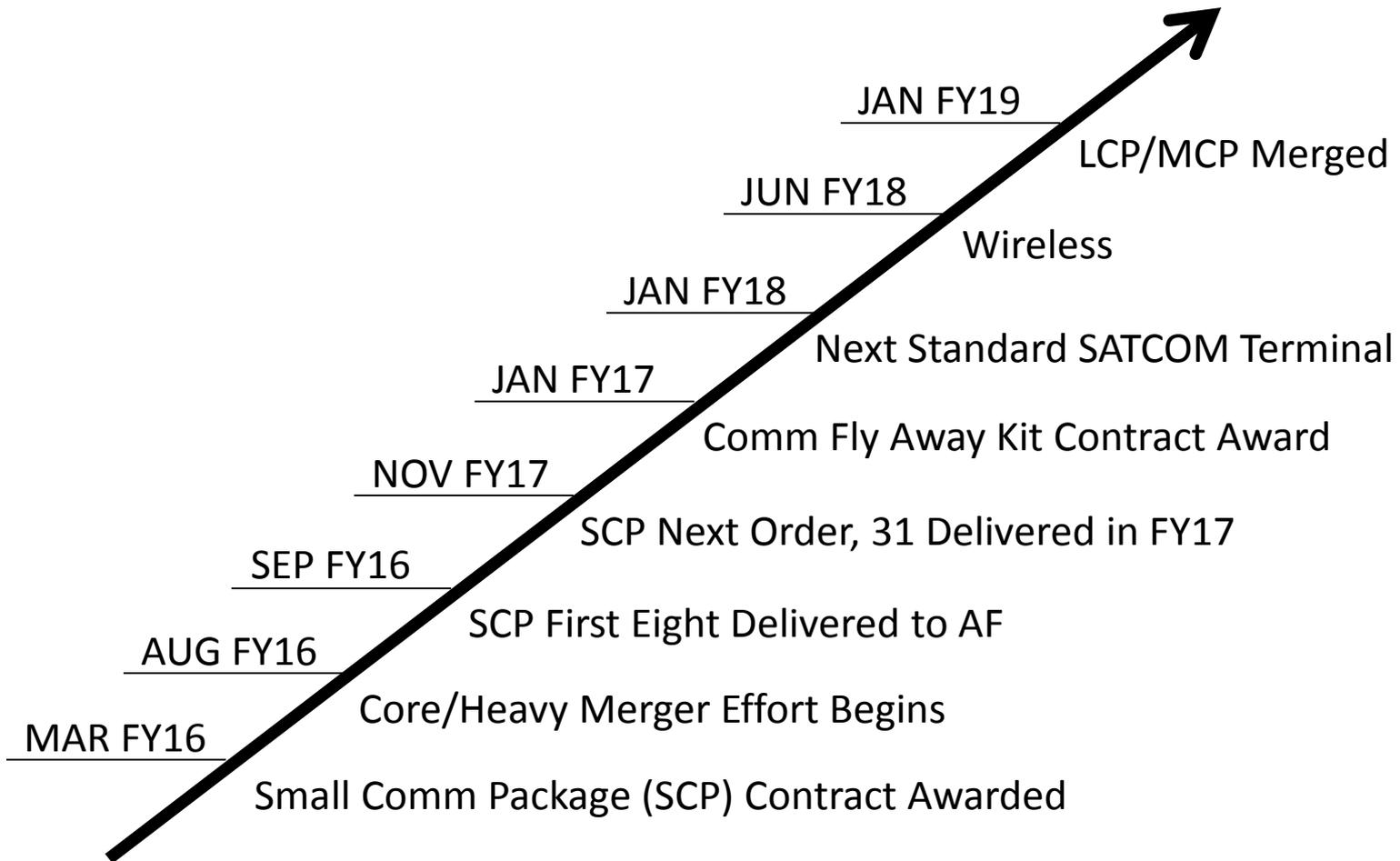


Combat Comm Laydown





TDC Schedule





Challenges & Issues

- **Lack of Formal Combat Communications Guidance**
- **Combat Communications Standardized Training**
- **Combat Communications Force Structure**
- **ASOC Expansion to 12 ASOCs**
- **Theater Deployable Comm Program Funding Reductions and Modernization**
- **Combat Comm SATCOM Dependency**
- **Cyber Squadron of the Future/Comm Sq Next**



CCSG Initiatives

- **Mission Directive**
- **Combat Communications AFI**
- **Update Deployable Communications CONOPS**
- **Centralized Combat Communications Training**
- **Coalition Networks**
- **Survivable Communications**
- **SIPRNET Tokens**

- **Total Force Combat Communications Wing**



Successes

- **Air Staff Engagement**
- **Medium Communications Package**
- **Small Communications Package**
- **COMACC Certification for ACS/ASOS Missions**
- **USAFE Use of Guard and Reserve**
- **Combat Communications Capability Manager**
- **FYDP Funding**
- **Ops, Ops and Ops**



Questions?





SCP Requirements

- **Support up to 40 personnel (16 concurrent users)**
- **NIPR, SIPR and 3rd Enclave Networks**
- **Secure and Non-Secure Voice over IP (VoIP)**
- **Radio over Internet Protocol (RoIP)**
- **NIPR and SIPR wireless network capable**
- **Virtual server management**
- **SATCOM terminal**
- **Wireless Commercial Data (e.g. 4G/LTE)**
- **Worldwide commercial power compatible**
- **Commercial Aircraft Transportable**