Headquarters U.S. Air Force

Integrity - Service - Excellence

Task Force Cyber Secure

U.S. AIR FORCE

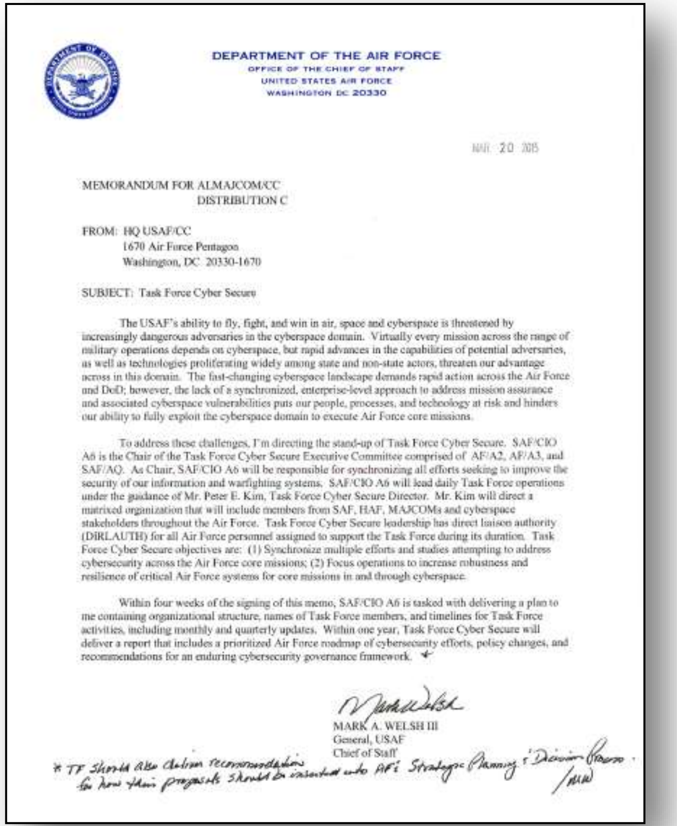
Colonel Bill “Data” Bryant
Task Force Cyber Secure
Deputy Director

Task Force Objectives

- 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

CSAF Memo



DEPARTMENT OF THE AIR FORCE
OFFICE OF THE CHIEF OF STAFF
UNITED STATES AIR FORCE
WASHINGTON DC 20330

MAR 20 2015

MEMORANDUM FOR ALMAJCOM/CC
DISTRIBUTION C

FROM: HQ USAF/CC
1670 Air Force Pentagon
Washington, DC 20330-1670

SUBJECT: Task Force Cyber Secure

The USAF's ability to fly, fight, and win in air, space and cyberspace is threatened by increasingly dangerous adversaries in the cyberspace domain. Virtually every mission across the range of military operations depends on cyberspace, but rapid advances in the capabilities of potential adversaries, as well as technologies proliferating widely among state and non-state actors, threaten our advantage across in this domain. The fast-changing cyberspace landscape demands rapid action across the Air Force and DoD; however, the lack of a synchronized, enterprise-level approach to address mission assurance and associated cyberspace vulnerabilities puts our people, processes, and technology at risk and hinders our ability to fully exploit the cyberspace domain to execute Air Force core missions.

To address these challenges, I'm directing the stand-up of Task Force Cyber Secure. SAF/CIO A6 is the Chair of the Task Force Cyber Secure Executive Committee comprised of AF/A2, AF/A3, and SAF/AQ. As Chair, SAF/CIO A6 will be responsible for synchronizing all efforts seeking to improve the security of our information and warfighting systems. SAF/CIO A6 will lead daily Task Force operations under the guidance of Mr. Peter E. Kim, Task Force Cyber Secure Director. Mr. Kim will direct a matrixed organization that will include members from SAF, HAF, MAJCOMs and cyberspace stakeholders throughout the Air Force. Task Force Cyber Secure leadership has direct liaison authority (DIRLAUTH) for all Air Force personnel assigned to support the Task Force during its duration. Task Force Cyber Secure objectives are: (1) Synchronize multiple efforts and studies attempting to address cybersecurity across the Air Force core missions; (2) Focus operations to increase robustness and resilience of critical Air Force systems for core missions in and through cyberspace.

Within four weeks of the signing of this memo, SAF/CIO A6 is tasked with delivering a plan to me containing organizational structure, names of Task Force members, and timelines for Task Force activities, including monthly and quarterly updates. Within one year, Task Force Cyber Secure will deliver a report that includes a prioritized Air Force roadmap of cybersecurity efforts, policy changes, and recommendations for an enduring cybersecurity governance framework. *

Mark Welsh
MARK A. WELSH III
General, USAF
Chief of Staff

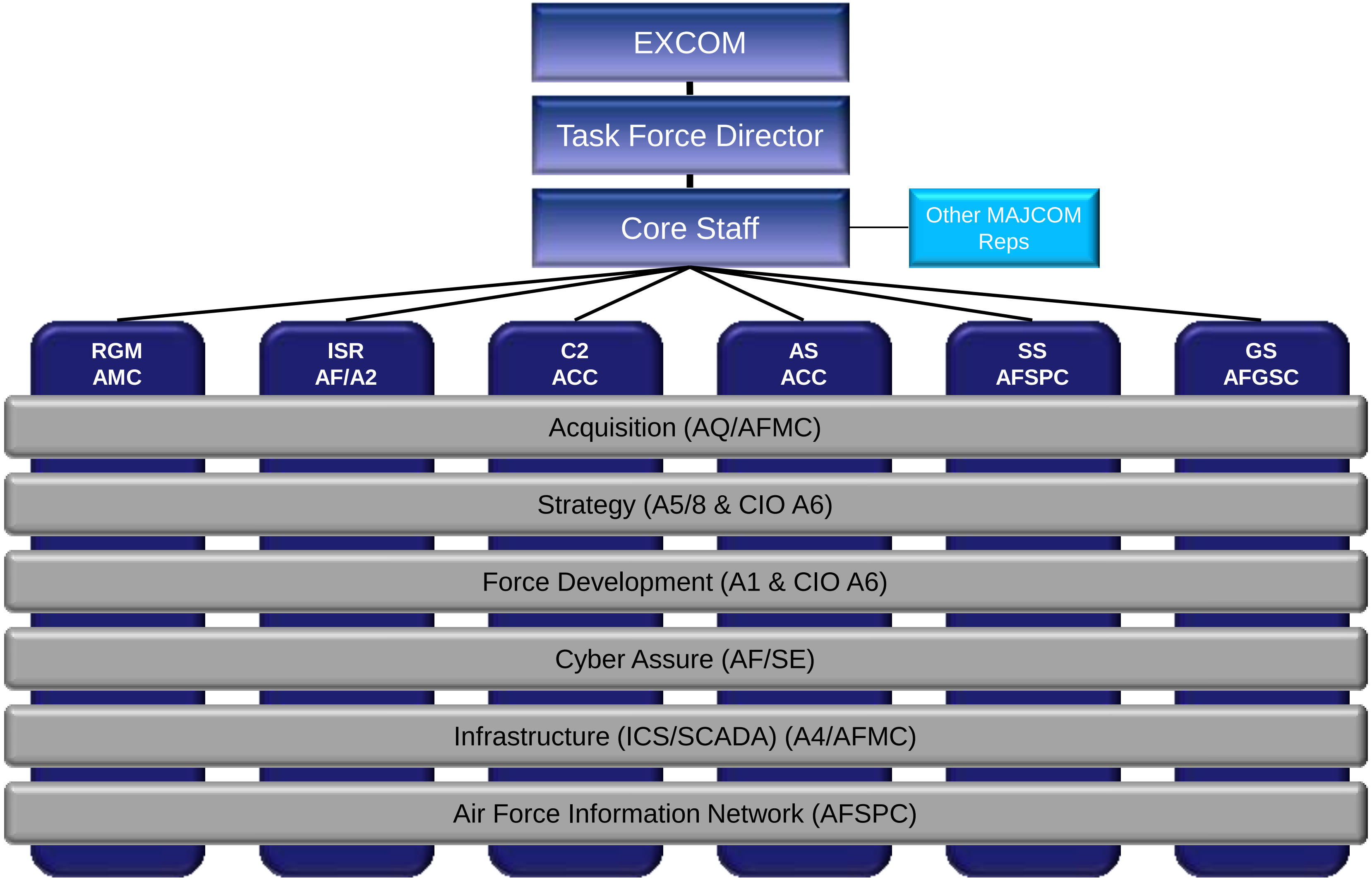
* TF should also deliver recommendations for how their proposals should be inserted into AF's Strategic Planning & Decision Process. /MW

> "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)

Deliverables

- "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

TFCS Structure



EXCOM

Task Force Director

Core Staff

Other MAJCOM Reps

RGM AMC

ISR AF/A2

C2 ACC

AS ACC

SS AFSPC

GS AFGSC

Acquisition (AQ/AFMC)

Strategy (A5/8 & CIO A6)

Force Development (A1 & CIO A6)

Cyber Assure (AF/SE)

Infrastructure (ICS/SCADA) (A4/AFMC)

Air Force Information Network (AFSPC)

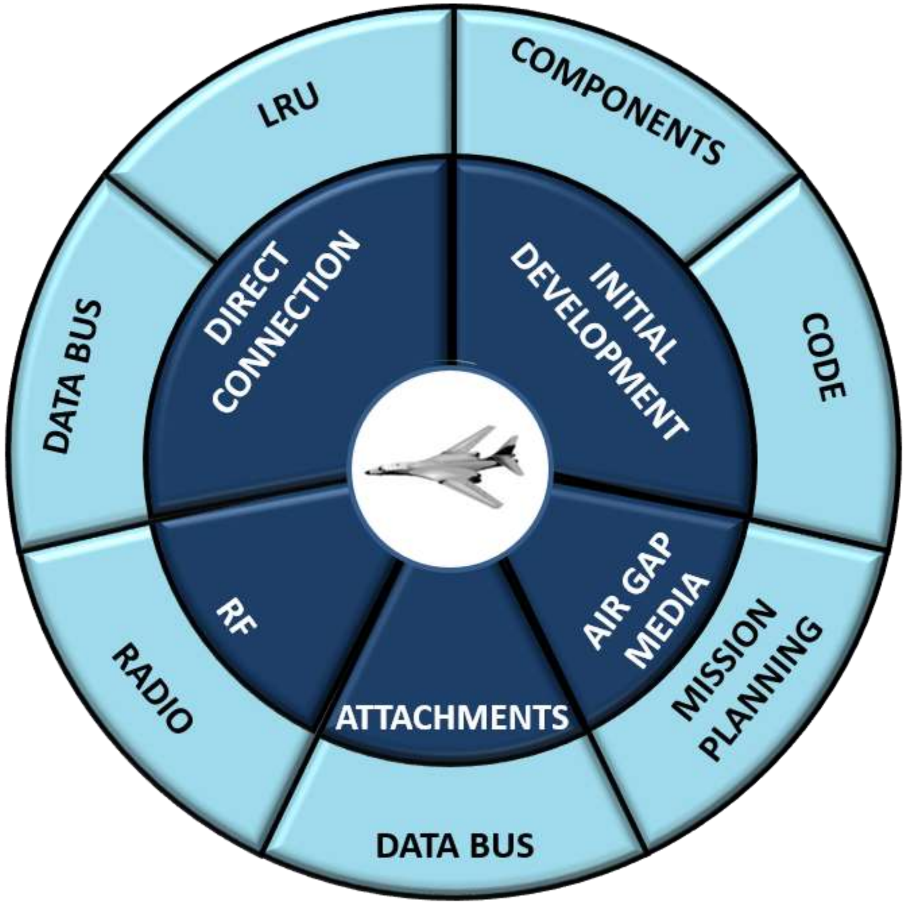
Why is this Important?

- 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

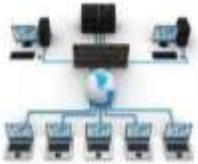
Mission Assurance Focus

AF Cyber Physical Systems

- 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

	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

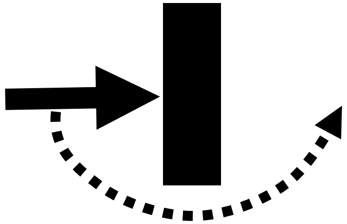
***OT = Operational Technology – Computer controlled physical processes such as ICS (i.e. power, water) logistics (i.e. fuel systems) or other control systems (i.e. building automation, security alarms)**

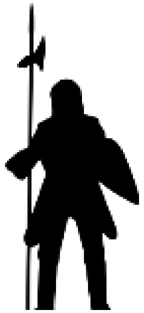
Problem

- 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

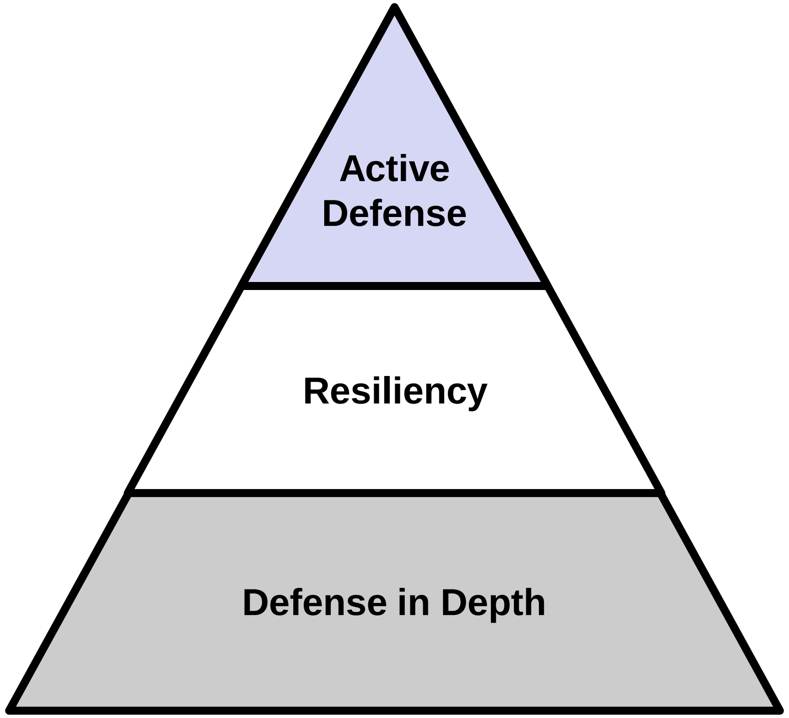




- Cyber operations communities focus on detection and response
  - Cyberspace maneuver emphasis

Solution & TFCS Framework

- 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

Draft Recommendations

- 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)**

- CISO Vision
  - ***The Air Force can accomplish the five core missions in a contested cyberspace environment.***
- CISO Mission Statement
  - ***The CISO Organization will assist with transforming the Air Force from reactive cybersecurity to proactive cybersecurity through changes, processes, and strategic communications.***
  - ***CISO will provide support to implement a new cyber security governance structure to inform senior leaders of cybersecurity challenges and help them make agile, effective, and informed decisions regarding cybersecurity risk implementation.***

Enduring Cybersecurity – Missions, Functions & Tasks

SAF/CIO A6
Lt Gen William Bender
Deputy CIO: Mr. Bill Marion (SES)

Chief Information Security Officer
Mr. Peter Kim (SES)

- JIE Governance
- ITGEG / ITGEB / WFI - GOSG
- Information Dominance Flight Plan

Cybersecurity Program

Cybersecurity Oversight

Effective RMF Performance

- Implement DoD's Cybersecurity Program
- Establish risk executive (function) for comprehensive, AF-wide risk management
- Establish risk management roles/responsibilities
- Implement risk management strategy
- Oversee consistent enterprise risk mgt activities
- **Manage threat & vulnerability information**
- Lead Cybersecurity Forums (AFCTAG & AFRMC)

Risk Posture

Policy & Strategy Guidance

- Develop/maintain policy & guidance (Risk Management Framework, COMSEC, TEMPEST, PKI, COMPUSEC, Crypto/Mod, etc.)
- Review/approve Cybersecurity strategies, H/VH, PIA and AFDAMO packages

Cybersecurity Support

Culture

Shape Air Force Culture

- Develop recurring & robust cybersecurity training
- Inject standard cyberspace curriculum into all accession programs
- **Inform the force about realistic cyber threats**
- Develop strategic risk understanding (IDFP)

Strategy/Policy

Holistic Cybersecurity Strategy

- Develop AF Cybersecurity strategy
- Cybersecurity architecture liaison
- Gather aggregated risks (Balanced Scorecard, Enterprise Dashboard, Metrics, etc.)
- Support implementation of advanced defensive tools on Air Force networks
- Support improved protection of weapons and mission systems
- Secretariat AO Summit & Cybersecurity Scorecard

Cybersecurity Coordination

Core Mission Liaisons

Experts on Key Cyber Terrain for Core Missions

- Oversee compliance with cybersecurity program within info systems, PIT-control systems, **threat analysis**, policy, PPBE
- Transform mission needs into achievable cybersecurity requirements

Mission Assurance

Fly, Fight and Win

- Assess cybersecurity posture
- Oversee requirements within core missions and capabilities (RGM, ISR, C2, AS, SS, CS, GS, ACS)

Criteria

✓ Does not duplicate work
✓ Spans entire AF

Draft Recommendations

- 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)**

Draft Recommendations

- 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)**

Draft Recommendations

- 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)**

Draft Recommendations

- 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)**

Questions

U.S. AIR FORCE

AIR FORCE CYBERSECURITY ★ DEFENDING THE DOMAIN ★

Enduring Cyber Security – Missions, Functions & Tasks

REQUIREMENTS:

CS Program:
9 DAMO (9)
7 Compliance (7)
4 Governance (4)
2 Mgmt (2)

CS Support:
10 Support (9)

CS Coord:
9 LNO (0)

CISO:
1 CISO (1)

Total Current: 32
Total Required: 42

SAF/CIO A6
Lt Gen William Bender
Deputy CIO: Mr. Bill Marion (SES)

Chief Information Security Officer
Mr. Peter Kim (SES)

JIE Governance

ITGEG / ITGEB / WFI - GOSG

Information Dominance Flight Plan

Cybersecurity Program

Cybersecurity Oversight

Effective RMF Performance
- Implement DoD's Cybersecurity Campaign
- Establish risk executive (function) for comprehensive, AF-wide risk management
- Implement risk management strategy
- Establish risk management roles/responsibilities
- Oversee consistent enterprise risk mgt activities
- Manage threat & vulnerability information
- Lead Cybersecurity Forums (AFCTAG & AFRMC)

Risk Posture

Policy & Strategy Guidance
- Develop/maintain policy & guidance (Risk Management Framework, COMSEC, TEMPEST, PKI, COMPUSEC, Crypto/Mod, etc.)
- Review/approve Cybersecurity strategies, H/VH, PIA and AFDAMO packages

Cybersecurity Support

Strategy/Policy

Holistic Cybersecurity Strategy
- Develop AF Cybersecurity strategy
- Cybersecurity architecture liaison
- Gather aggregated risks (Balanced Scorecard, Enterprise Dashboard, Metrics, etc.)
- Support implementation of advanced defensive tools on Air Force networks
- Support improved protection of weapons and mission systems
- Secretariat AO Summit & Cybersecurity Scorecard

Culture

Shape Air Force Culture
- Develop recurring & robust cybersecurity training
- Inject standard cyberspace curriculum into all accession programs
- Inform the force about realistic cyber threats
- Develop strategic risk understanding (IDFP)

Cybersecurity Coordination

Core Mission Liaisons

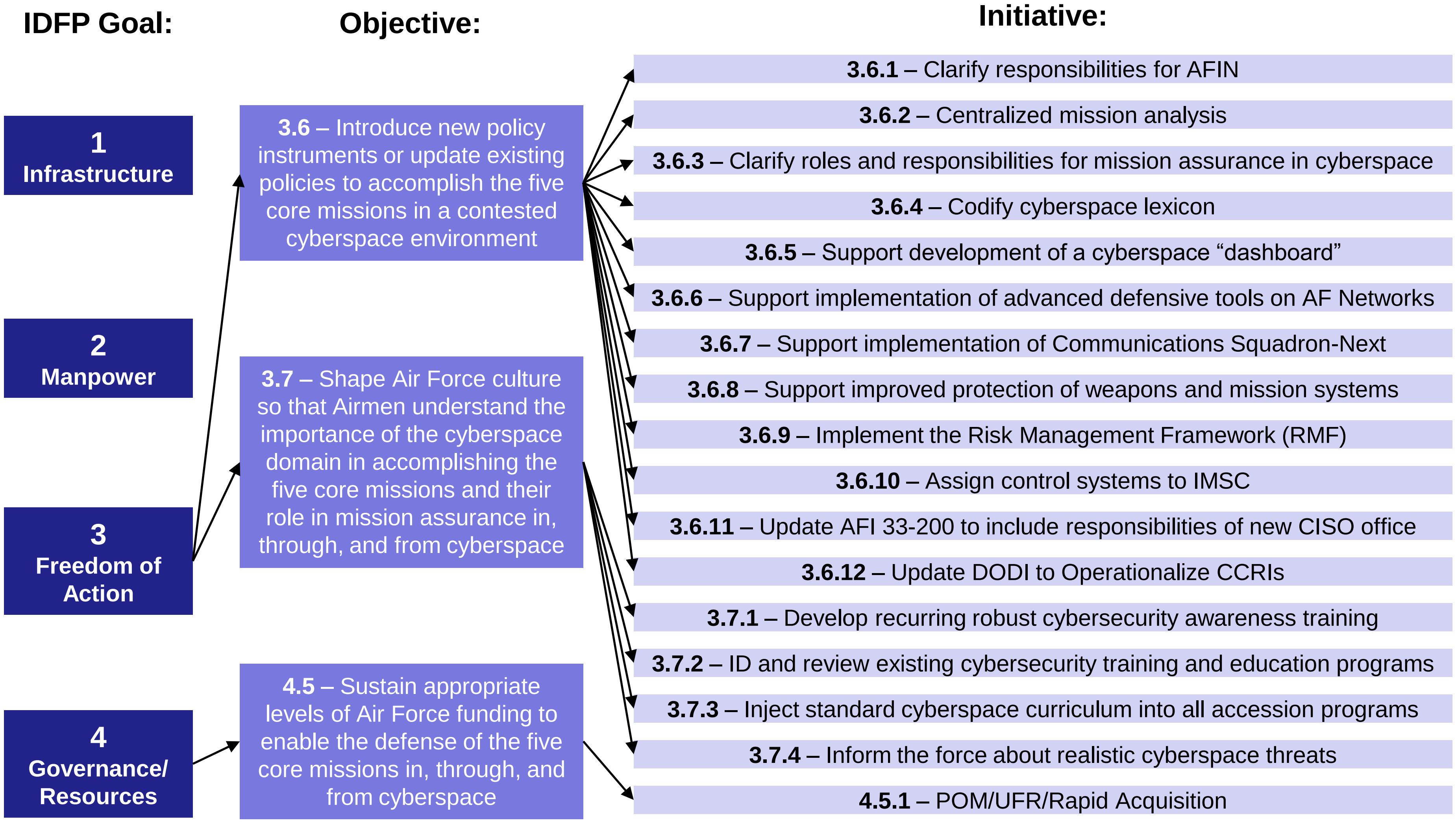
Expert Authorities on Critical Systems
- Oversee compliance with cybersecurity program within info systems, PIT-control systems, threat analysis, policy, PPBE
- Transform mission needs into achievable cybersecurity requirements

Mission Assurance

Maximized Mission Assurance
- Assess cybersecurity posture
- Oversee requirements within core missions and capabilities (RGM, ISR, C2, AS, SS, CS, GS, ACS)

Criteria
✓ Does not duplicate work
✓ Spans entire AF

CISO Initiative Linkages



IDFP Goal:

1
Infrastructure

2
Manpower

3
Freedom of Action

4
Governance/ Resources

Objective:

3.6 – Introduce new policy instruments or update existing policies to accomplish the five core missions in a contested cyberspace environment

3.7 – Shape Air Force culture so that Airmen understand the importance of the cyberspace domain in accomplishing the five core missions and their role in mission assurance in, through, and from cyberspace

4.5 – Sustain appropriate levels of Air Force funding to enable the defense of the five core missions in, through, and from cyberspace

Initiative:

3.6.1 – Clarify responsibilities for AFIN

3.6.2 – Centralized mission analysis

3.6.3 – Clarify roles and responsibilities for mission assurance in cyberspace

3.6.4 – Codify cyberspace lexicon

3.6.5 – Support development of a cyberspace “dashboard”

3.6.6 – Support implementation of advanced defensive tools on AF Networks

3.6.7 – Support implementation of Communications Squadron-Next

3.6.8 – Support improved protection of weapons and mission systems

3.6.9 – Implement the Risk Management Framework (RMF)

3.6.10 – Assign control systems to IMSC

3.6.11 – Update AFI 33-200 to include responsibilities of new CISO office

3.6.12 – Update DODI to Operationalize CCRIs

3.7.1 – Develop recurring robust cybersecurity awareness training

3.7.2 – ID and review existing cybersecurity training and education programs

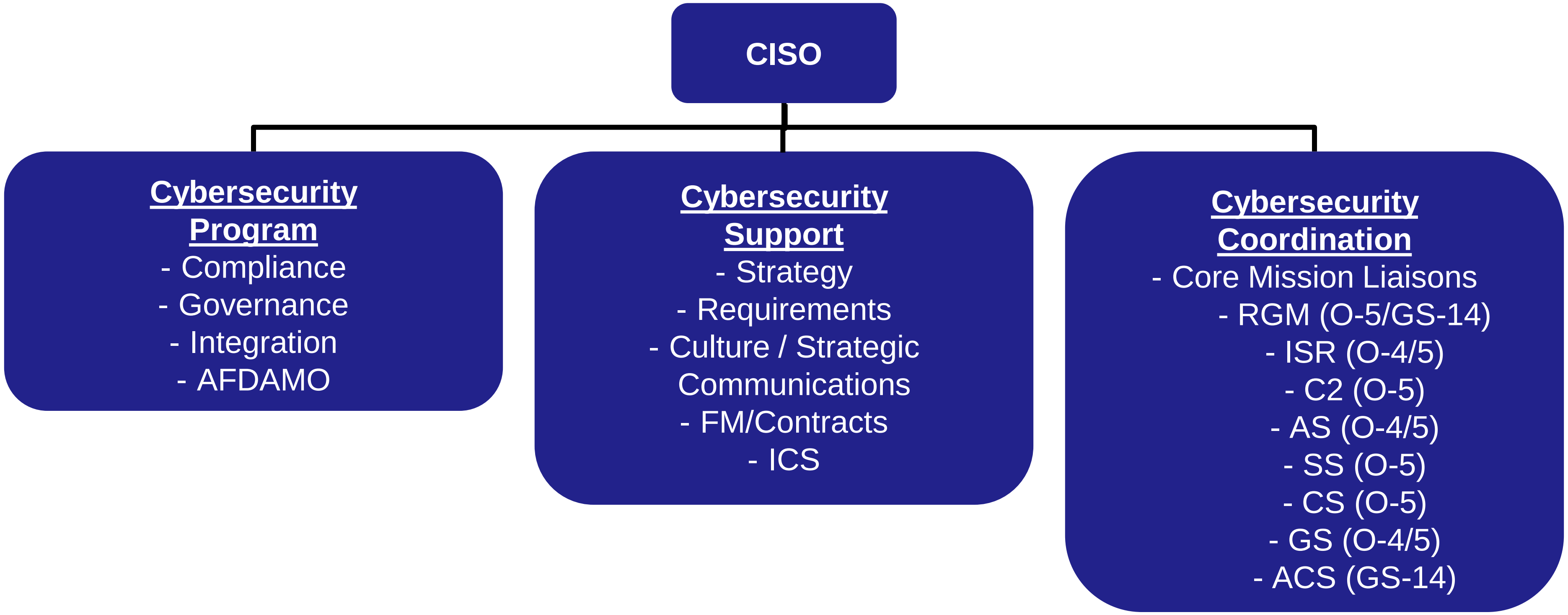
3.7.3 – Inject standard cyberspace curriculum into all accession programs

3.7.4 – Inform the force about realistic cyberspace threats

4.5.1 – POM/UFR/Rapid Acquisition

U.S. AIR FORCE

CISO Functions



CISO

Cybersecurity Program
- Compliance
- Governance
- Integration
- AFDAMO

Cybersecurity Support
- Strategy
- Requirements
- Culture / Strategic Communications
- FM/Contracts
- ICS

Cybersecurity Coordination
- Core Mission Liaisons
  - RGM (O-5/GS-14)
  - ISR (O-4/5)
  - C2 (O-5)
  - AS (O-4/5)
  - SS (O-5)
  - CS (O-5)
  - GS (O-4/5)
  - ACS (GS-14)

AFITC 2016

AMERICA: LIVING FREE, SECURE, AND PRODUCTIVE IN A CYBER WORLD