AFITC

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

2016

Headquarters U.S. Air Force

AF Chief Information Security Officer (CISO)

Mr. Pete Kim (SES)
AF Chief Information Security Officer
peter.e.kim2.civ@mail.mil
(703) 695-1835

CISO Mission Statement

Transform the Air Force from reactive to proactive cybersecurity through policy, processes, and strategic communications…and Cyber Secure Airmen.

Implement and enable a cybersecurity governance structure to inform senior leaders of cybersecurity challenges leading to agile, effective, and informed decisions regarding cybersecurity risk mitigation.

Continuing journey (work in progress…ever adapting and constantly improving)

AIR FORCE CORE MISSIONS

Of the three major Services, the Air Force has primary interest in all operations in the air.
– Key West Agreement, 1947

U.S. AIR FORCE

Enterprise Perspective

Education on the Risk
Share Information
Connect the Dots
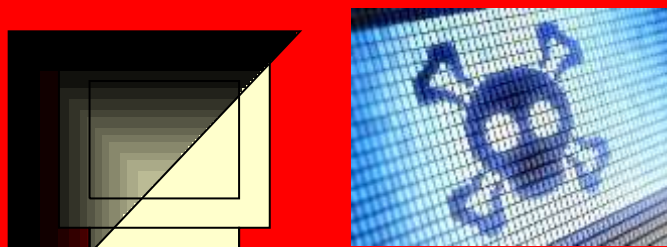**Make Decisions**

My Approach for Cybersecurity

Compliance Mindset

Adversary Mindset

**Policy Compliance
Performance Optimization
Configuration Baseline and
Standardization**

Administrator Perspective

Hacker Perspective

**Identify Vulnerabilities
Identify Intruders
Assess Defensive Response**

New Cybersecurity Paradigm: You need both mindsets on your mission systems 24/7

OV-1 of AF Cyber Defense-in-Depth
(Cyber Mission Assurance of AF Core Missions)

- AFCYBER leverages static and active defenses to identify, mitigate and remediate cyber vulnerabilities and detect/defeat cyber threats.
- USCYBERCOM, JFHQ DODIN, NSA, Cyber Protection Teams, AFCYBER, and Comm Squadron Next **work together** to defend AF Core Missions
- AFCYBER currently defends Key Terrain & critical assets for AF Core Mission (Air, Space, C2)
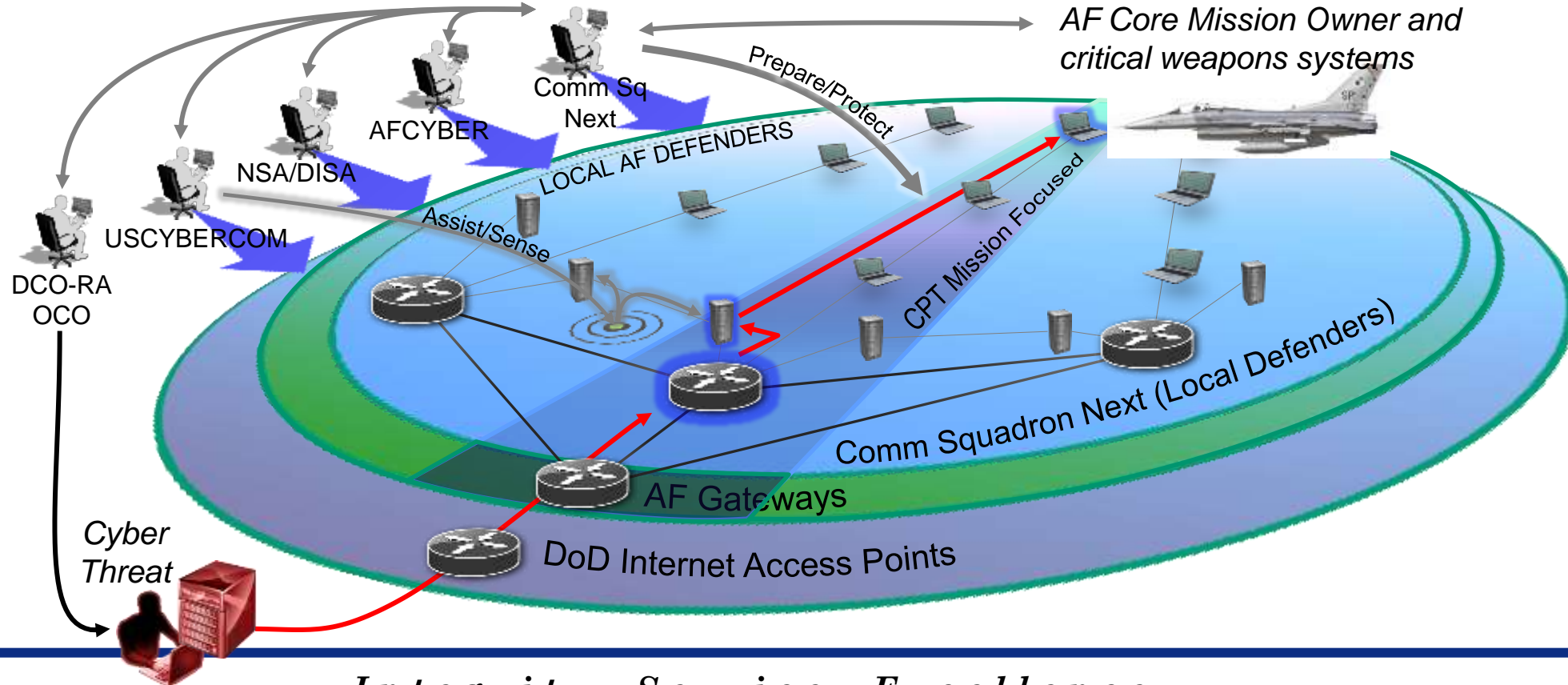
CISO Framework and Priorities

1. **Enterprise Approach:** Sets enterprise priorities, guidance and policy on cybersecurity for the Air Force...for Core Missions and the information technologies that enable those missions.

2. **Team:** Orchestrates the AF Team approach to field cyber-resilient capabilities and enhance the protection of critical warfighter/business information with public and private industry for enterprise cybersecurity and coordinated response actions.

3. **Educate:** Trained and educated CyberSafe Airmen who understand cybersecurity implications and linkages to mission assurance in, through and from cyberspace.

4. **Innovate:** Innovative approaches to critical cyber defense and resiliency challenges for air, space and cyberspace.

5. **Manage Risk:** Enable executive discussions on risk management to protect Airmen, Core Missions and to defeat adversaries' effectiveness.

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)

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
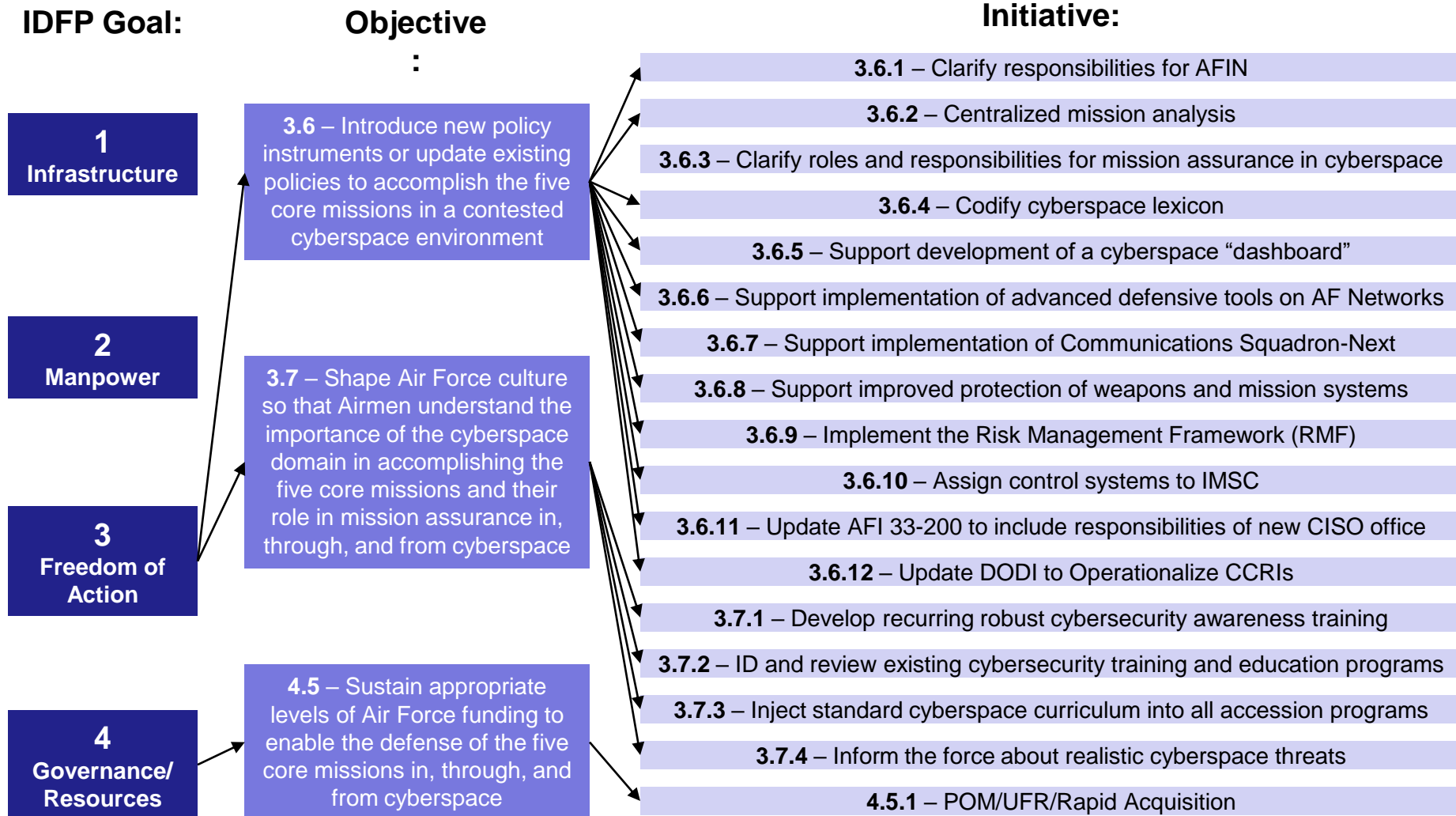- ✓ Does not duplicate work
- ✓ Spans entire AF

CISO Initiative Linkages

IDFP Goal:

Objective:

Initiative:

IDFP Goal	Objective	Initiative
1 Infrastructure	**3.6** – Introduce new policy instruments or update existing policies to accomplish the five core missions in a contested cyberspace environment	**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
2 Manpower		**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
	3.7 – 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	**3.6.8** – Support improved protection of weapons and mission systems
		3.6.9 – Implement the Risk Management Framework (RMF)
3 Freedom of Action		**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
	4.5 – Sustain appropriate levels of Air Force funding to enable the defense of the five core missions in, through, and from cyberspace	**3.7.3** – Inject standard cyberspace curriculum into all accession programs
4 Governance/ Resources		**3.7.4** – Inform the force about realistic cyberspace threats
		4.5.1 – POM/UFR/Rapid Acquisition

To ask questions during or after the presentation, please email them to:

AFITC2016QA@gmail.com

Your questions will be read aloud for the audience and speaker