# Cryptologic Systems Group

*"Securing the Global Information Grid (GIG)"*

# Air Force Cryptographic Modernization


## Third Annual Layered Assurance Workshop

## 4 - 5 August 2009

**Mrs. Mary Anne Smith**

**Director, AF Crypto Mod Program Office**

**CPSG/ZX, Lackland AFB, TX**

# Purpose

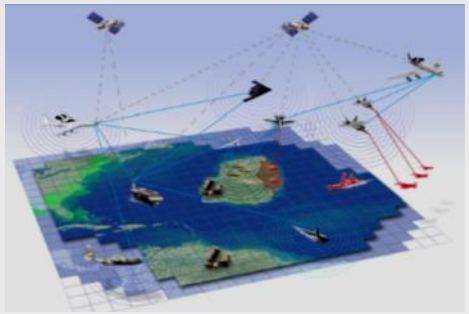
- Present an overview of Cryptologic Systems Group (CPSG) & Air Force Cryptographic Modernization Program Office (CMPO) to attendees at the Third Annual Layered Assurance Workshop

# Outline

- AF challenges
- AF Cryptologic Systems Group (CPSG)
- AF Cryptographic Modernization Program Office (CMPO)
  - AF CM acquisition & modernization approach
  - Programs & interest areas
  - CM challenges - technical, budget & programmatic

# Air Force Challenges

## Securing Today's Cyber Battlefield…



**More Complex Battlefield**

**Sophisticated Global Enemy**

**Dynamic & Evolving Environment**

# Cryptologic Systems Group

Crypto Modernization

Space Crypto

Air/Ground COMSEC

Force Protection

**Mission:**
**Assured Information Dominance**

**Vision:**
**Securing the Global Information Grid**

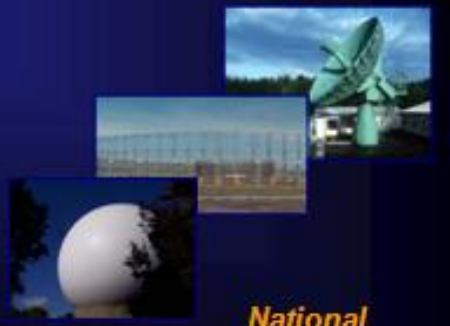
Public Key Infrastructure

Tech Apps


Key Management Infrastructure

AF Electronic Key Management & Voice Call Signs

Global Information Grid Information Assurance



National Intel

# CPSG Organization

**ESC/CC**
**Lt Gen Bowlds**

**653rd ELSW/CL**
**Mr. Mason**

**CPSG/CC**
**Col Collamore**

## FYDP $3B in Cyber Acquisition

- Public Key Infrastructure (PKI)
- Key Management Infrastructure (KMI)
- Crypto Mod - 9 ACAT III programs

### *Information Assurance*
### *NI*
### *Mr. Collazo*

- PKI
- AF EKMS (III)
- KMI
- GIG-IA

### *Special Projects*
### *ZJ*
### *Mr. Friesenhahn*

- KG-327, TT&C AVE (III)
- KS-252, TT&C GOE (III)
- Space Mission Data (III)
- Space COMSEC

### *Crypto Modernization*
### *ZX*
### *Ms. Smith*

- Crypto Modernization
- KS-60 ICU (III)
- KG-3X (III)
- ROME
- Crypto Transformation

### *COMSEC Products*
### *ZC*
### *Ms. Moncus*

- IFF Mode 5 CM (III)
- RRK (III)
- CKG (III)
- VACM (III)
- Air / Ground COMSEC
- ITAC

### *Intel & Force Protect*
### *ZI*
### *Mr. Aguirre*

- Consolidated SIGINT Support Activity
- Technical Applications
- Tactical Intel
- Force Protection

### *Contracting*
### *PK*
### *Ms. Hair*

### *Financial Mgmt*
### *FM*
### *Mr. Kane*

### *Mission Support*
### *OM*
### *Mr. Dietert*

### *Engineering*
### *EN*
### *Ms. Moncus (A)*

### *Maintenance*
### *MA*
### *Mr. Parmigiani*

### *Logistics*
### *LG*
### *Mr. Jandt*

# Current Cryptographic Inventory

- Security & component technologies are aged/aging
- Typically point-to-point with little to no net-centric/ Internet Protocol capability
- Bandwidth & processing speed constrained
- Challenged with regard to:
  - Logistics
  - Interoperability
  - Flexibility
  - Compatibility with modernized key management (EKMS & KMI)

# DoD Crypto Mod Initiative (CMI)

- **Vital effort to transform all NSA-certified, Type 1 Crypto solutions to meet the needs of the next generation warfighting environment – cannot fight & win without crypto that protects C2 & data in transit**
- **DoD Type 1 Crypto Equipment transformation goals:**
  - **Net-centric & Global-Information-Grid (GIG) compatibility**
  - **Compatible w/ next generation Key Management Infrastructure (KMI)**
  - **More robust, stronger algorithms**
  - **Releasable versions of algorithms to warfighting partners**
  - **Higher data rates & larger downloads**
  - **Over-The-Network Re-keying (OTNR) capability**
  - **Reprogrammable H/W enabling easier & less expensive upgrades**
  - **Logistically supportable**

**NSA Executive Agent -- all Services actively participating**

# AF Crypto Modernization

**Legacy Systems**

**Modernized Systems**

**Transparent, Cross-Cutting Solutions**

Platforms

Equipment (Radio)

Device (Crypto Hardware)

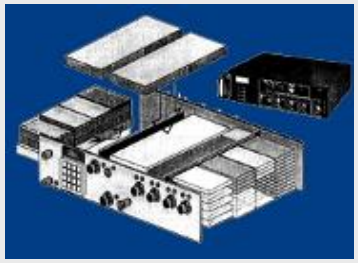
Engine (Chip)

Algorithm

Increased Security Robustness

Programmability

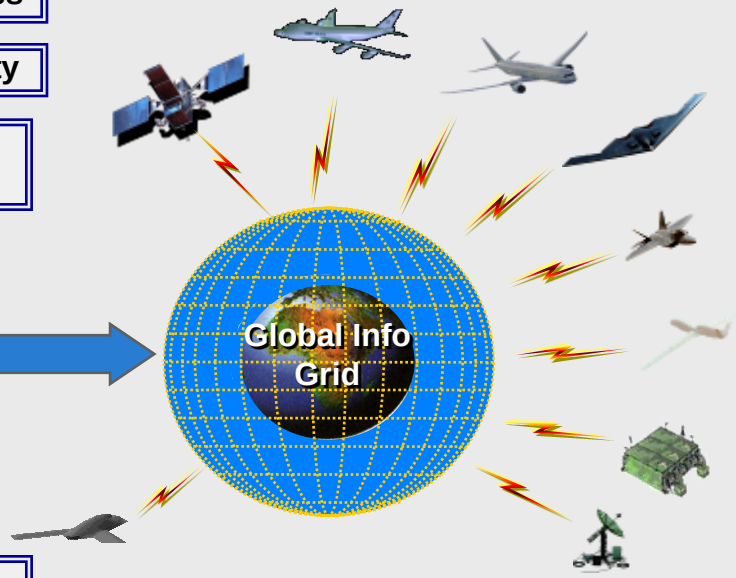
Advanced Algorithms



Interoperability

Releasability

Key Management Infrastructure Compatibility




**Secure Information for Net-Centric Ops**

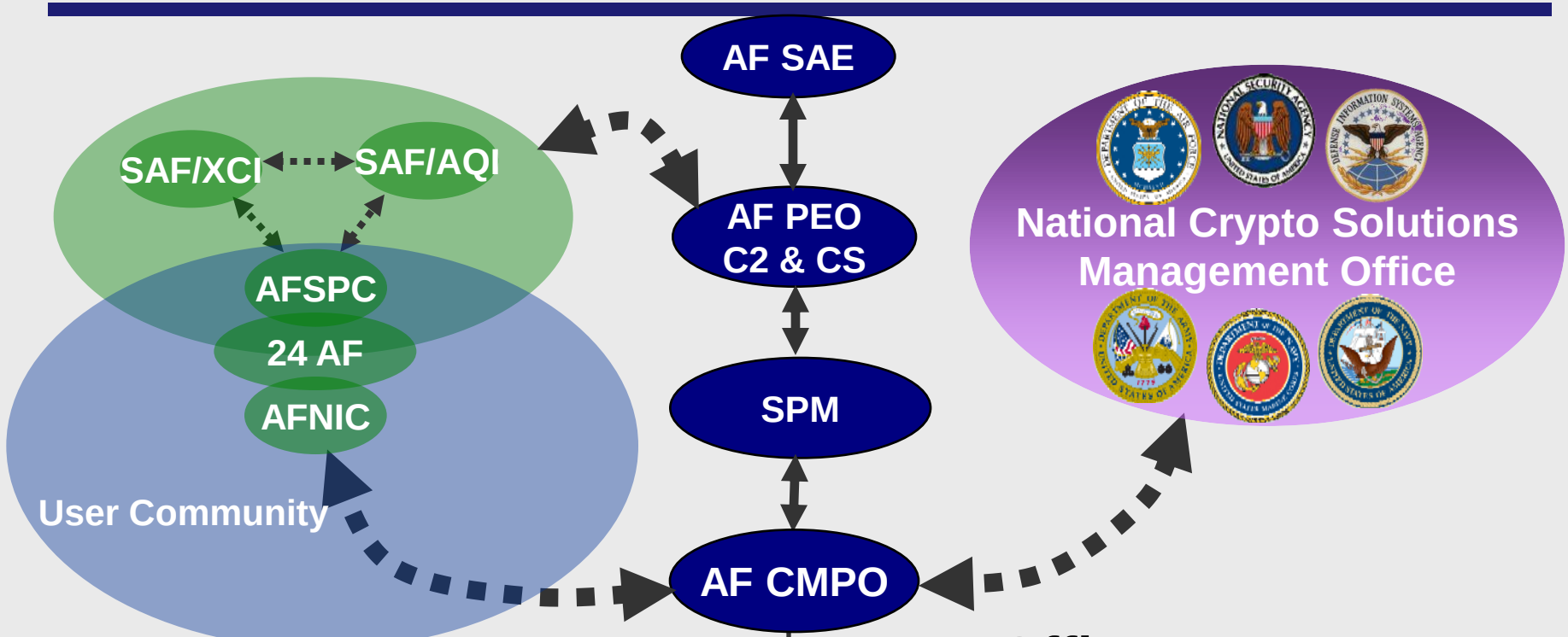
Technology Infusion

# AF Crypto Mod Program Office

*Est. 7 December 2001*

- **Enterprise management**
  - CM Acquisition Policy, Guidance, & Strategic Planning
  - Promote AF Awareness, coordinate w/ other Services & NSA
  - Manage portfolio funding w/ Lead Command & Air Staff
- **Analysis -- Ensure crypto is secure & supportable**
  - Understand crypto inventory & platform usage
  - Analyze decertification & AF way ahead
  - Track current / future tech development
  - Partner for risk reduction & concept technology development
  - Facilitate NSA security evaluation & certification
- **Program planning -- Initial planning for:**
  - Concept refinement
  - Development
  - Production & deployment

# AF Crypto Mod Acquisition Structure




## Program Management Offices

Industry

- KG-3X Crypto Mod
- ICBM Crypto Upgrade
- IFF Mode 5 Crypto
- Space TT&C AVE
- Space TT&C GOE
- Remote Re-Key
- Combat Key Generator
- Space Mission Data
- VINSON ANDVT Crypto

# AF Crypto Mod Phased Approach

- **Replacement: Near term sustainability issues**
  - Nuclear C2 Crypto (KG-3X & KS-60)
  - IFF Mode 5 Crypto
  - Remote Re-key (RRK)
  - Combat Key Generator (CKG)
- **Modernization: Incremental improvement & reduced logistics**
  - Space Telemetry, Tracking, & Commanding (TT&C)
  - Space Mission Data (SMD)
  - VINSON/ANDVT Crypto Mod (VACM)
- **Transformation: Common network-centric crypto solutions**
  - Remote Operational Management of End-Crypto-Units (ROME)
  - Multi-Level Security (MLS)
  - Dynamic Group Keying (DGK)
  - Common Interface to Cryptographic Modules (CICM)
  - Miniaturized & Software Crypto

# AF Crypto Mod
# Other Areas of Interest

- Link Encryption Family (LEF)
- F-22 Multi-Function Crypto
- Programmable Objective Encryption Technologies (POET)
- Navy-led Link-16 Encryption Modernization
- Multiple studies

# AF CM Challenges

- **Technical**
  - Size, Weight & Power (SWaP)
  - Software-based crypto
  - NSA certification / decertification requirements
- **Funding**
  - Cuts to military budget (-)
  - Increasing emphasis on security (+)
  - Increasing emphasis on cyber capabilities (+)
- **Programmatic**
  - Ever-changing acquisition process (-)
  - New acquisition framework (+)

# AF CM Way Ahead

- Common solutions for legacy & future systems
  - Reduced size, weight & power
  - High assurance, high speed & anti-tamper
  - Multi-Level Security & dynamic group keying
  - High assurance storage encryption
- Continue to evolve & capitalize on PKI
- Transition plan from EKMS to KMI
- Anticipate emerging threats & participate in Air Force Cyber response

# Point of Contact

## Crypto Mod Program Office

**Sue Hooker, CPSG/ZX**
**Crypto Mod Program Office**
**Program Action Group, Govt Lead**
**Commercial Phone: (210) 925-5277, DSN: 945-5277**
**Email: sue.hooker@lackland.af.mil**
**Or**
**CPSG.ZX.PAG@lackland.af.mil**

# *Questions?*

# Back-Ups

# Electronic Key Management System(EKMS) Key Management Infrastructure(KMI)

## SCOPE:

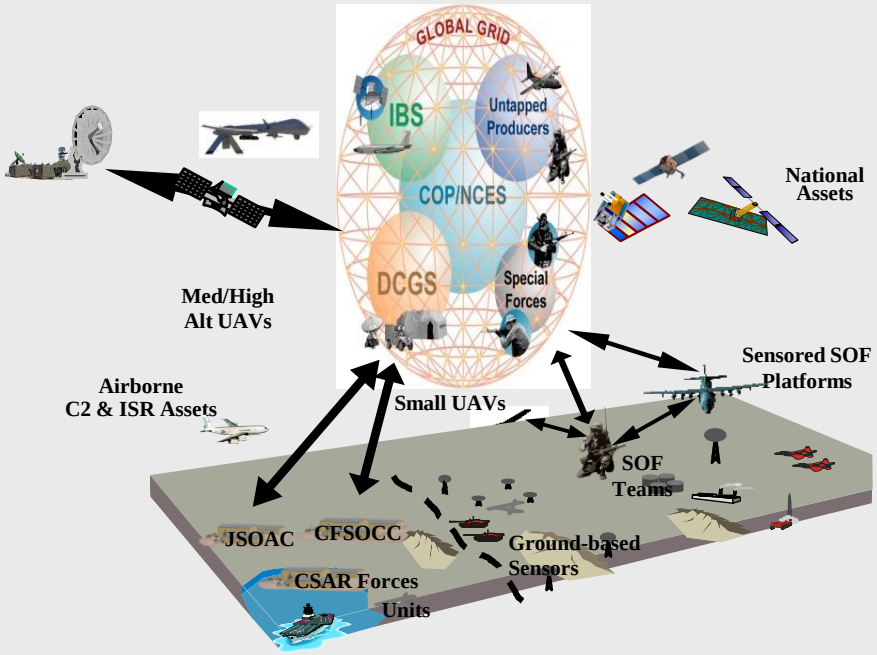
### Transactions per month

- F-15 requires 18 keys
- F-22 & JSF: 450 keys
- AEHF: 100,000 keys

## PROGRAM CONTENT:

- Provides electronic key generation, distribution, accounting, & management
- EKMS based on phone networks & requires significant human hands-on management
- KMI ensures modernized, AF-compliant networked operation for cryptographic key management
  - Enables warfighter Joint interoperability/ reachback
  - Decreases human intelligence threat (HUMINT)
  - Cuts production costs for NSA & shipment costs for Services
- AF Key Management growth areas: GPS equipment, secure cell phones, network encryptors, national agency & Coalition customers

# Space COMSEC



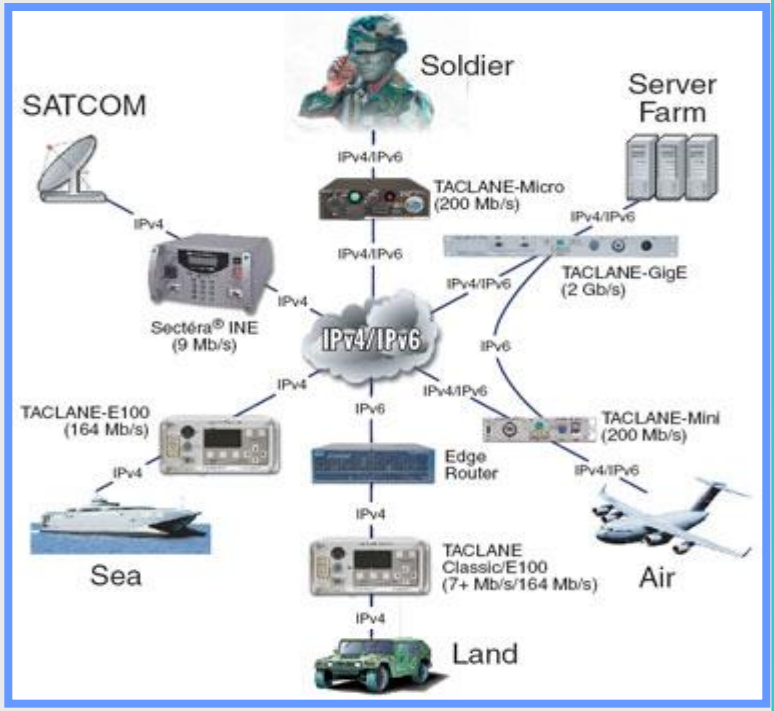

## SCOPE:

**Supports development, production, launch & operations of 15 satellite programs**

## PROGRAM CONTENT:

- **Provides warfighter secure, uninterrupted satellite communications, 24/7 ISR, & near real-time NAV / positioning & weather data**
- **Protects Command & Control of critical national assets**
- **Encrypts information collected or passed by satellite (mission data)**

# Air & Ground COMSEC




## SCOPE:

**- Sustains entire AF cryptographic inventory – over 1,200 device types**
**-Supports all AF bases – fixed & deployed**

## PROGRAM CONTENT:

**– Ensures AF warfighters communicate securely in any environment or media**

**– Replaces legacy link encryptors & aging in- line network encryptors**

- **– Modernized KIV-7M & KIV-19M point-to-point encryptors**
- **– High Assurance IP Encryptors (HAIPE) In-line encryptors**

**– HAIPEs ensure compliancy with the National Security Telecom & Information Systems Security Policy (NSTISSP) No. 11**