SKL Wireless & Black Data Distribution System Overview

Jack Rogers
AF Tier 3 Program Lead
(210) 925-2428
DSN 945-2428

Let's Start With

THE BAD

Top 5 Signs The Economy is Bad

- **1. A truck full of Americans got caught sneaking into Mexico**
- **2. People in Beverly Hills forced to fire nannies and learn their children's names**
- **3. Motel 6 won't leave the lights on**
- **4. People in Africa are donating money to Americans**

Top 5 signs the economy is bad

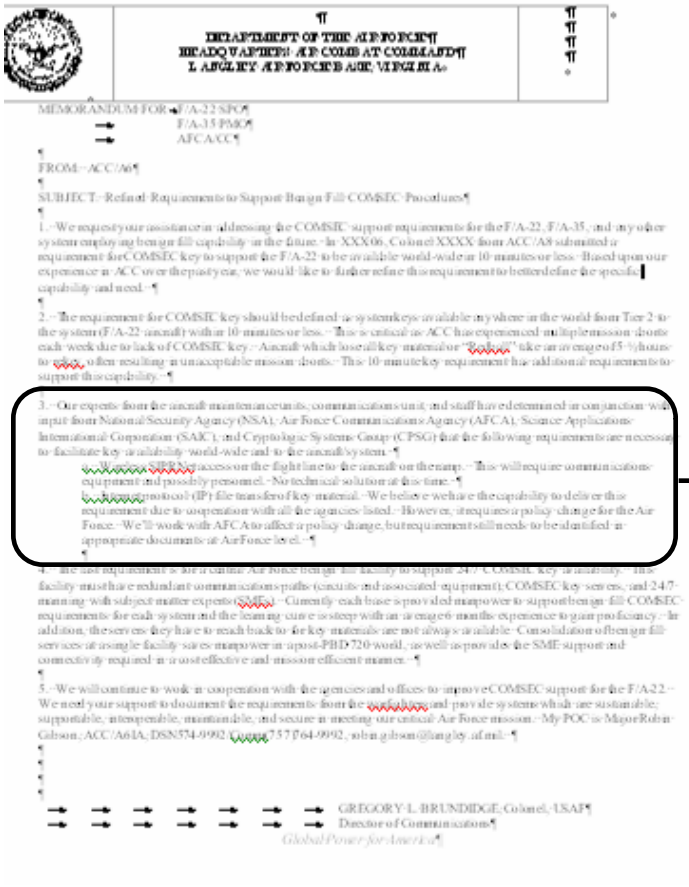
- 5. If the bank returns your check marked as “insufficient funds”, you have to call them and ask if they meant you or them

The Ugly

The Good

SKL –W Concept/Update

Letter from ACC/A6 for F-22:



3. **Our experts from the aircraft maintenance units, communications unit, and staff have determined in conjunction with input from National Security Agency (NSA), Air Force Communications Agency (AFCA), Science Applications International Corporation (SAIC), and Cryptologic Systems Group (CPSG) that the following requirements are necessary to facilitate key availability world-wide and to the aircraft/system.**

a. **Wireless SIPRNet access on the flight line to the aircraft on the ramp. This will require communications equipment and possibly personnel. No technical solution at this time.**

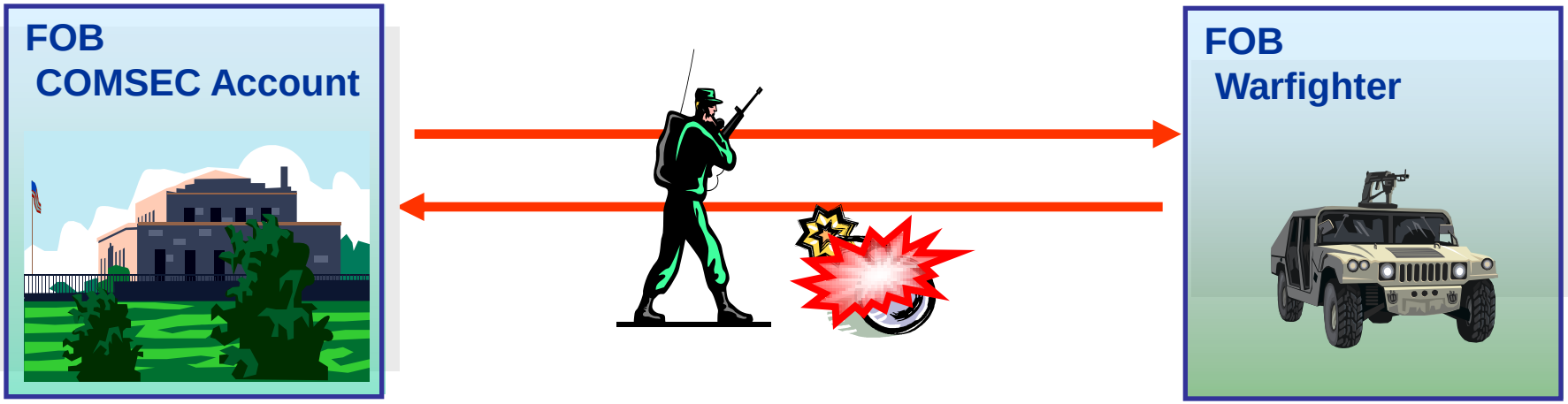
b. **Internet protocol (IP) file transfer of key material. We believe we have the capability to deliver this requirement due to cooperation with all the agencies listed. However, it requires a policy change for the Air Force. We'll work with AFCA to affect a policy change, but requirement still needs to be identified in appropriate documents at Air Force level.**

AF Capability Gap

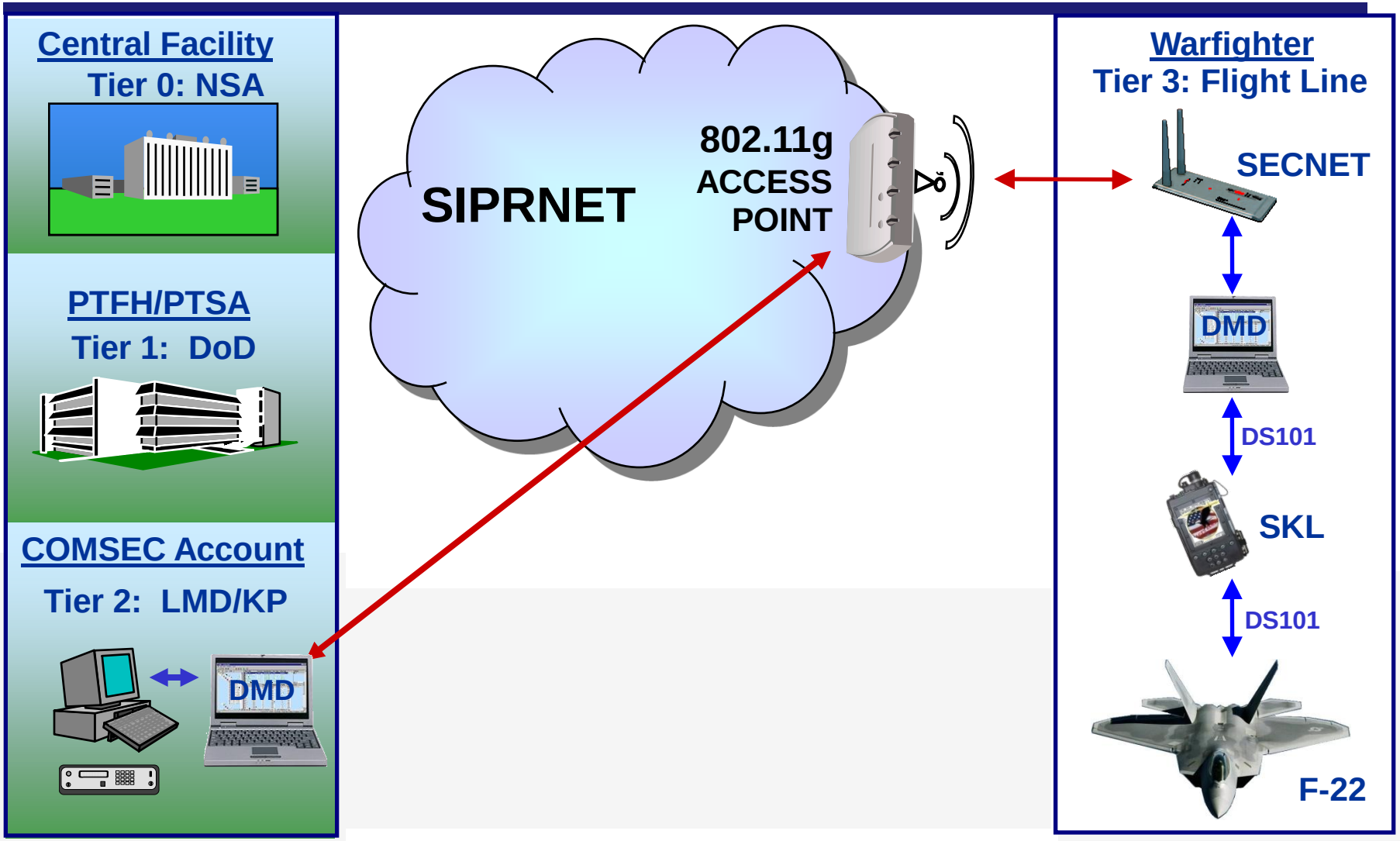
- Operational suitability of benign fill exchange
  - Operational impacts incurred due to multiple physical trips
  - Enhancements could cut tactical rekey time
  - Can't wait for single trip benign fill
    - KMI CI-3
    - Redesign of ECUs

Army Capability Gap

- **Army Deployed Operations**
  - **Delivering Keys to forward deployed forces is difficult and dangerous**
  - **Leads to trips through potentially hazardous terrain exposing war fighters to ambush and IED's**



Pilot Concept of Operations



DMD-W Concept of Operations
Client /Server Application

Central Facility
Tier 0: NSA

PTFH/PTSA
Tier 1: DoD

COMSEC Account
Tier 2: LMD/KP

SIPRNET

802.11
ACCESS
POINT

Phase I

Warfighter
Tier 3: Flight Line

DMD -
Wireless

DS101

F-22

SKL-W Concept of Operations

Central Facility
Tier 0: NSA

PTFH/PTSA
Tier 1: DoD

COMSEC Account
Tier 2: LMD/KP

DMD

SIPRNET

802.11
ACCESS
POINT

Phase II

Warfighter
Tier 3: Flight Line

SKL-
Wireless

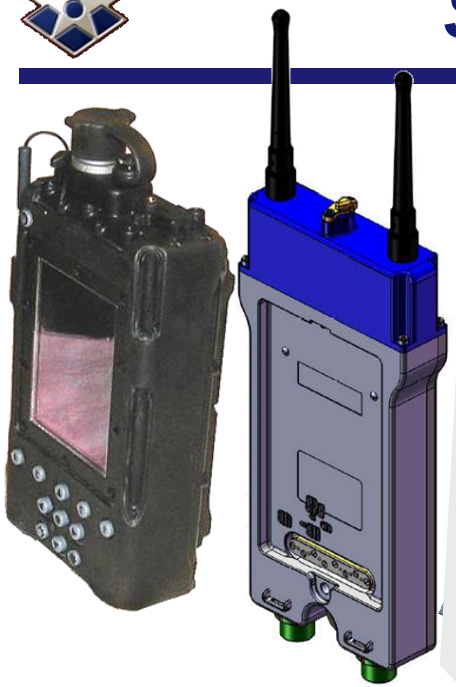
DS101

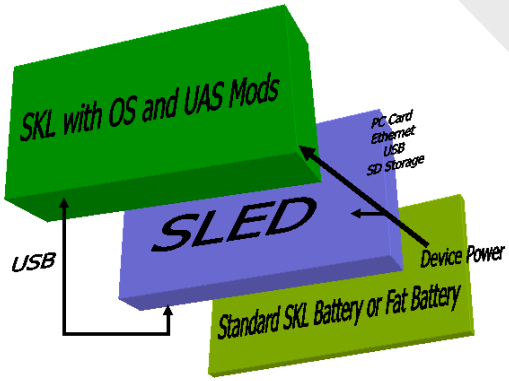
F-22

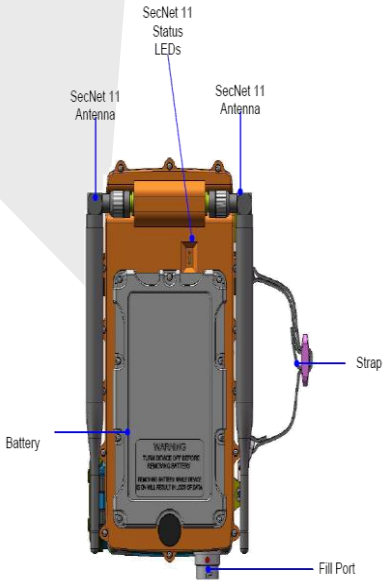
SKL-Wireless Concept

- Integration of SECNET 11, DMD and SKL led to the development of the SKL–W

SKL-W
SLED Wireless Enclosure







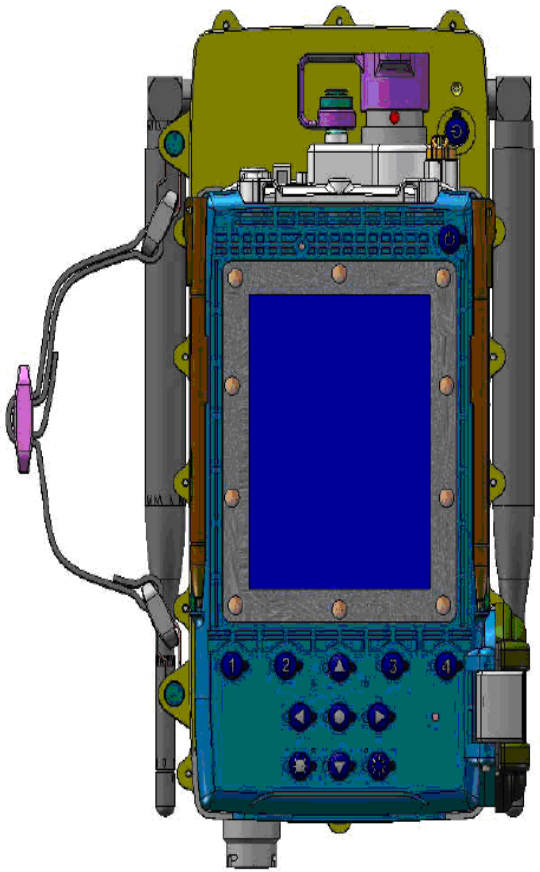
- **Army / Air Force Integration**

This SKL-W version connects by:

- **Removing SKL battery**
- **Attach the SKL-W Sled**
- **Attach the SKL battery to the back of Wireless device**

- **Enabling SKL wireless Sled to transmit <u>Black and Benign Fill Messages Wirelessly</u>**

SLED SECNET 11 Enclosure



Our enclosure design incorporates the following features

- **SN 11 dome extends above SKL form factor**
- **Zeroize buttons under battery…this is the only way to reach the zeroize buttons on the SN11 card**
- **Note - SN11 will also have s/w zeroize over PCMCIA interface**
- **Two 3dBi dipole antennas**
- **Standard 6 pin audio fill port to key SN11 card**
- **POGO PIN interface to SKL and SKL battery**
- **Light Pipes for SN11 Status**
- **SLED power on/off button for non-wireless SKL use**

Phase I Test Results

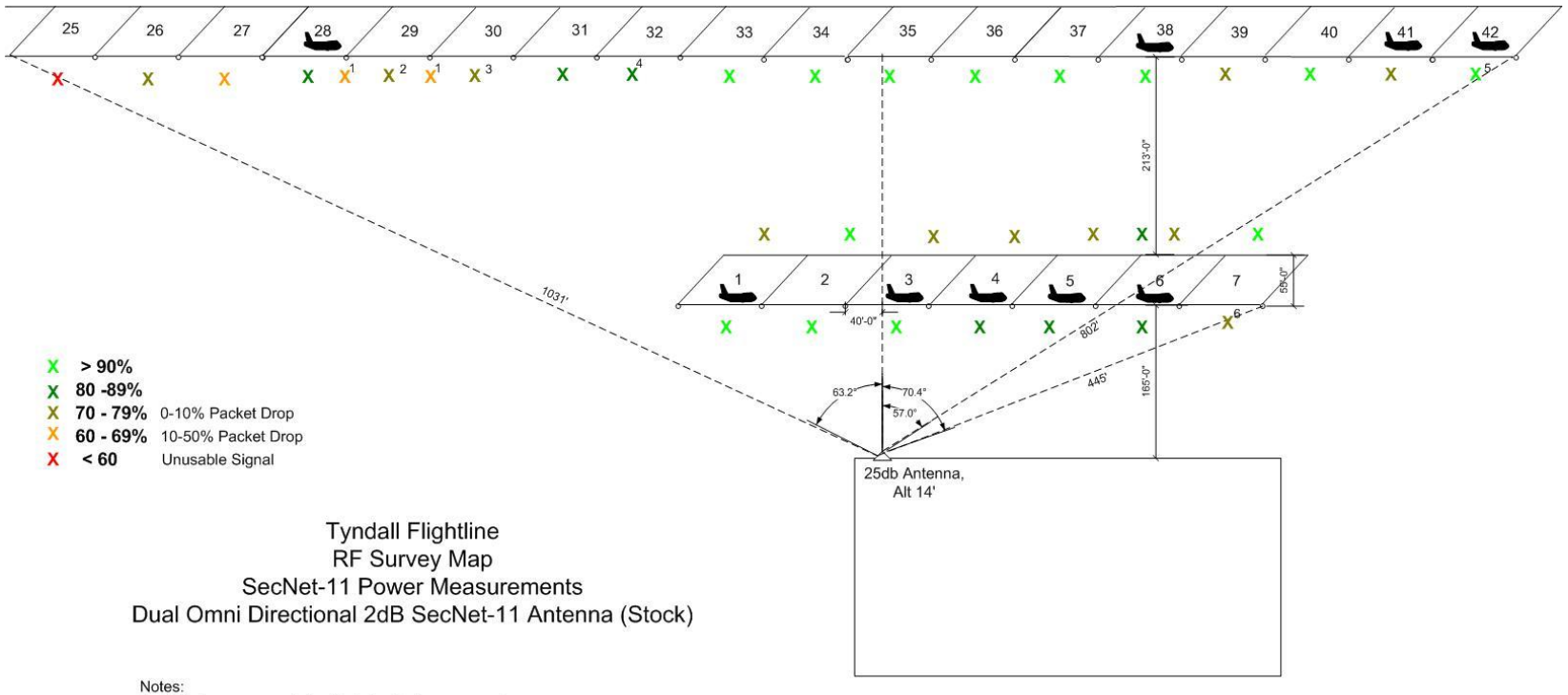
- Phase I has achieved the ACC/A6 10 min requirement
- CPSG will deliver the "Phase I DMD-W" to the war fighter this year, CPSG will provide operation and maintenance of the software and helpdesk support
- CPSG will provide the Secnet 11 infrastructure to the most critical F-22 bases as the Air Force CITS 2 Gen program becomes operational

Baseline	Time
Redball / Rekey SKL 4.0	36min 44sec
Redball / Rekey SKL 5.0	32min 03sec

Wireless	Time
Redball / Rekey SKL 5.0	16min 35sec
Redball / Rekey SKL 5.0 – Requesting Creds	16min 25sec
Redball / Rekey SKL 5.0 – Loading only Master ECU	8min 14sec

Tyndall Test Flightline

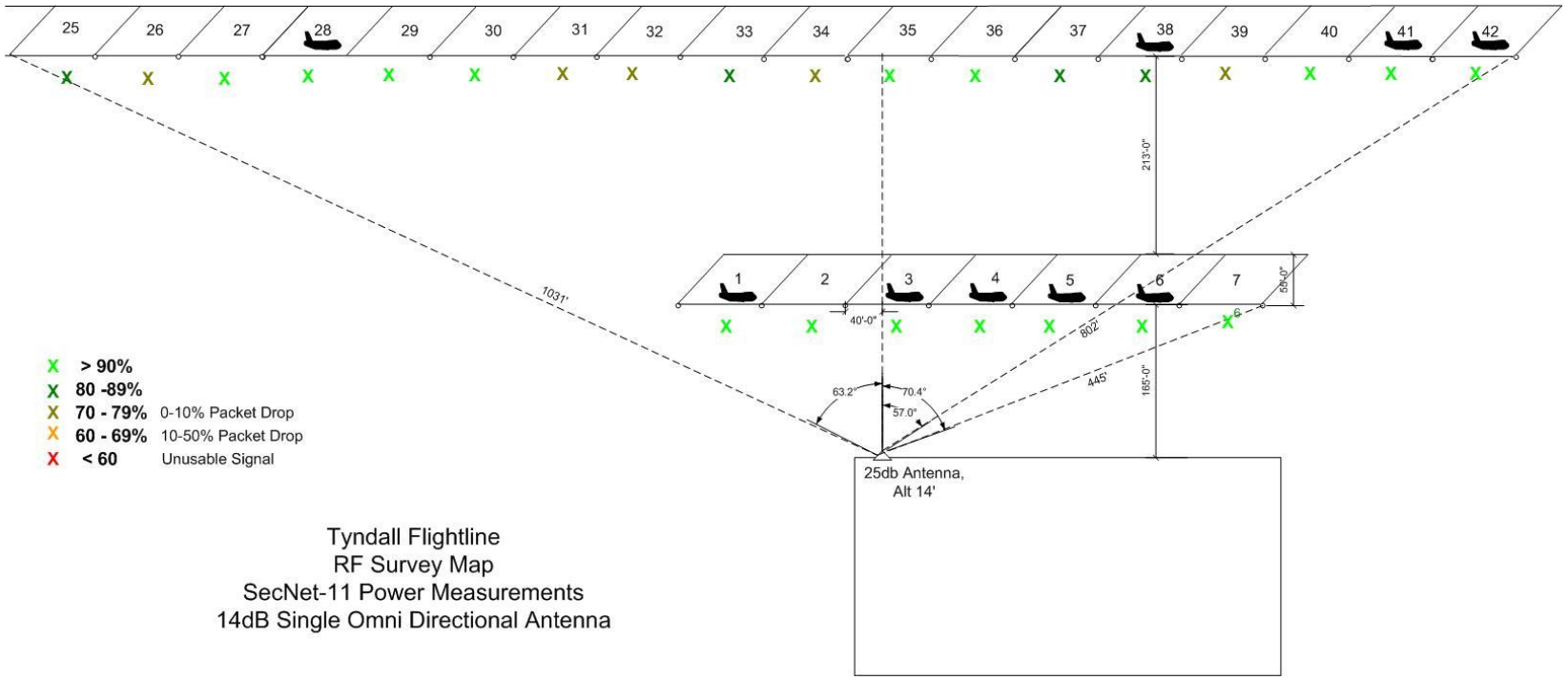
SKL –W Concept/Update



Tyndall Flightline
RF Survey Map
SecNet-11 Power Measurements
Dual Omni Directional 2dB SecNet-11 Antenna (Stock)

Notes:
1. 10% drop measured directly in front of canopy posts.
2. Coordinates measured at 30.067506N, 85.580781W
3. Coordinates measured at 30.067131N, 85.580260W, obstruction by tail of A/C in spot 1.
4. Taxing A/C obstructing antenna caused 40% signal loss at this point.
5. Measurement taken at 30.065180N, 85.577978W.
6. Measurement taken at 30.065176N, 85.579200W

SKL –W Concept/Update



Tyndall Flightline
RF Survey Map
SecNet-11 Power Measurements
14dB Single Omni Directional Antenna

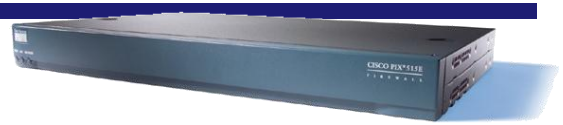
SKL – Wireless Testing – 2009

- **Nellis AFB, Jul 22-31**
- **Tyndall AFB, August 24-28 (tentative)**
- **Demonstration of Operational capability – Langley AFB, Nov 2009**

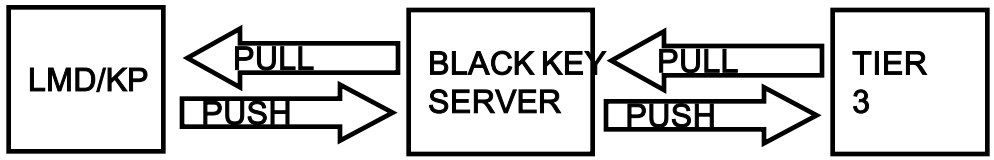
Black Data Distribution System (BDDS) Cross Domain Solution

- Enable key distribution across multiple domains
- Direct connect of Secret COMSEC to SECRET platforms
- Concept allows for 24/7 key operations from geographically separated locations
- Direct connect to Tier I devise (LMD/KP). Eliminating manual processing
- Allows for key distribution to multiple Tier III devises i.e. SMEPED, DMD, SKL, SKL/W
- Proof of concept servers are built, and have been tested at ITEC lab

Black Data Distribution System
Key Server



- Based on NRL NKMS Web Server
- Provides all automation for key distribution
- Data is relayed between LMD and SKL via access-limited drop points on the server (mailboxes / ftp directories / etc)
- Server allows for multiple Comsec accounts to be hosted and accessed by certified users across the globe
- Distributes black and benign fill key using a push and pull paradigm



- Can be a stand alone device or part of a integrated Cross Domain Solution

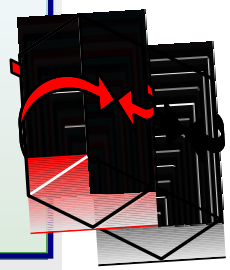
Black and Benign Fill Key Server Cross Domain Solution

Central Facility
Tier 0: NSA

PTFH/PTSA
Tier 1: DoD

COMSEC Account
Tier 2: LMD/KP

CDS

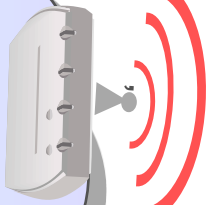


Black Key Server

SIPRNET

NIPRNET

802.11g ACCESS POINT



Phase III

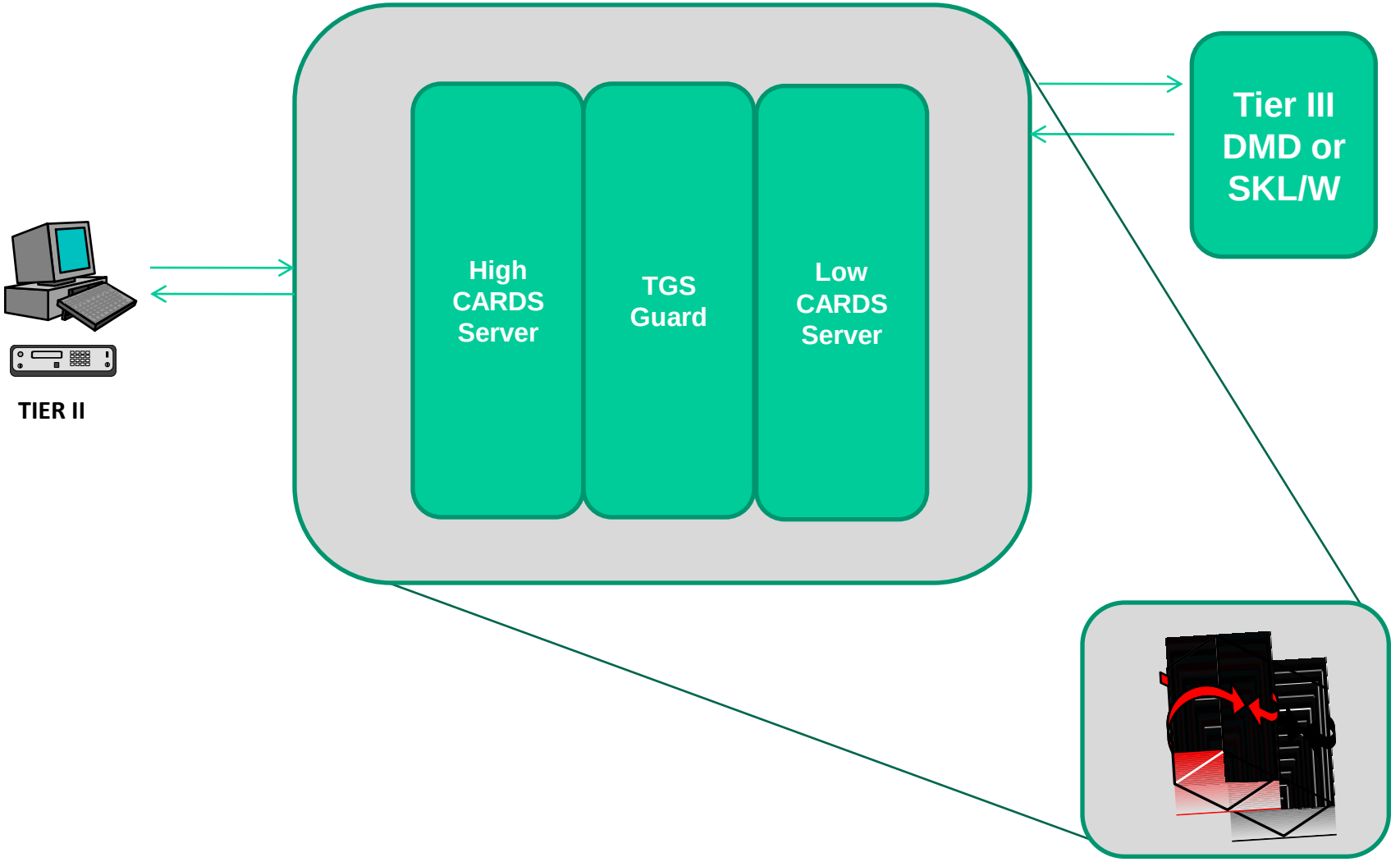
Warfighter
Tier 3: Flight Line

SKL-Wireless

DS101

F-22

Black Key Server



Point to Point Terrestrial

Lab Configuration

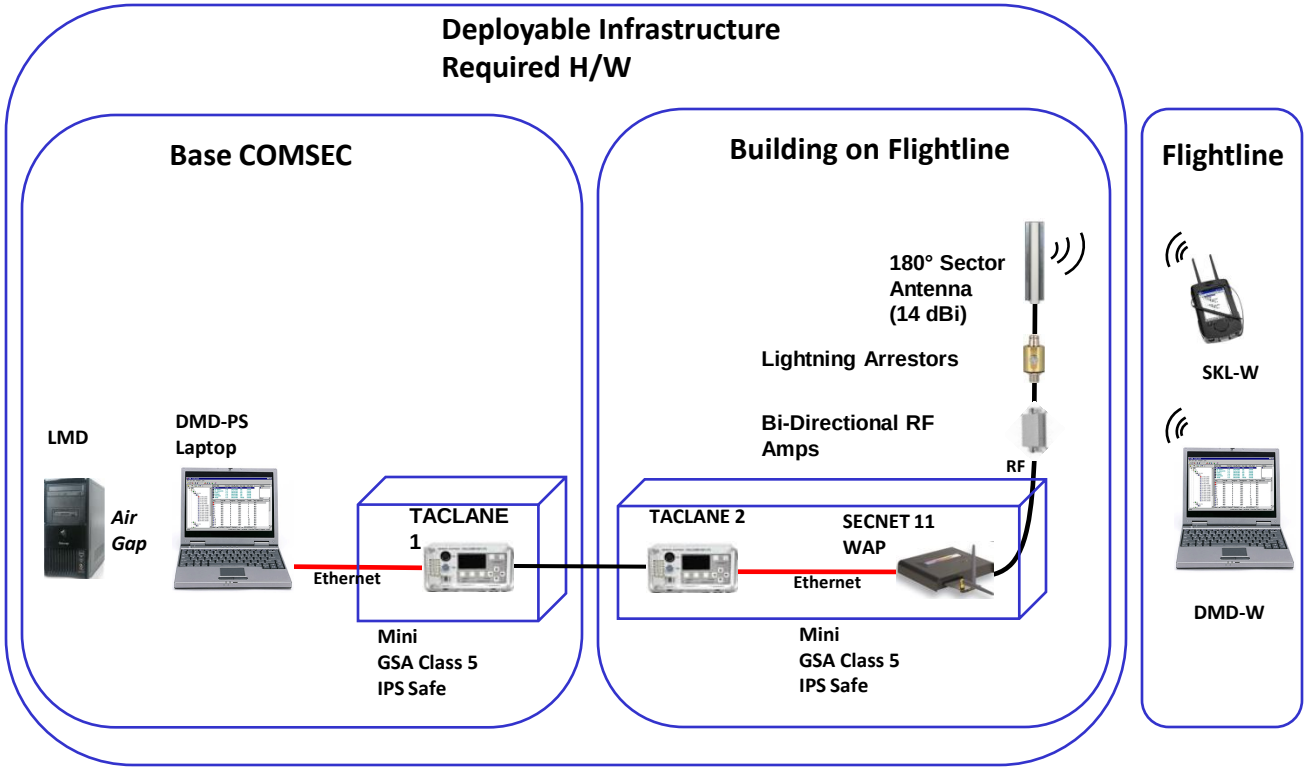
DMD PS (COMSEC)
IP: 172.16.2.26

TACLANE 1
IP (R): 172.16.2.1
IP (B):

TACLANE 2
IP (R): 172.16.1.1
IP (B):

SECNet11 WAP
IP: 172.16.1.3
SSID; SLEDDEMO

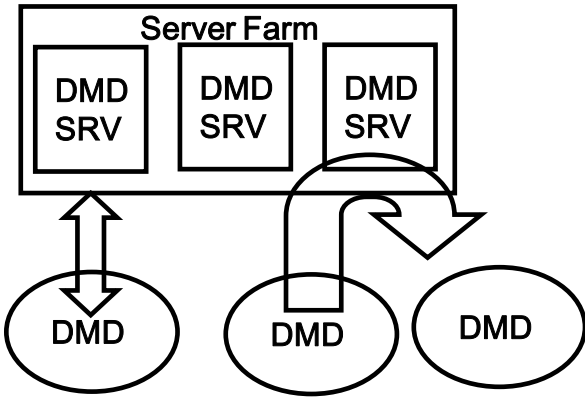
SKL-W
IP: 172.16.1.5
SSID: SLEDDEMO



QUESTIONS???

Black and Benign Client /Server Application (Phase I)

- Intelligent Store and Forward Server
- IP based Black Data and Benign Fill distribution
- Client Server communications can distribute to any DMD connected to SIPRNET
- SPECS
  - Windows Server 2003
  - .NET Framework
  - C Sharp
  - SQL 2005
  - Can be formed as Server Farm
  - Sockets Connection but moving towards a more reliable connection due to inconsistent RF communications
- 6-9 Month Development producing two spirals
  - Spiral 1 –Creation of single account server delivered March 2008
  - Spiral 2 – Multiple account server delivered August 2008
- Does not include C&A



Black and Benign Fill Key Server Cross Domain Solution

Central Facility
Tier 0: NSA

PTFH/PTSA
Tier 1: DoD

COMSEC Account
Tier 2: LMD/KP

SIPRNET
NIPRNET

802.11g
ACCESS
POINT

Warfighter
Tier 3: Flight Line

SKL-
Wireless

DS101

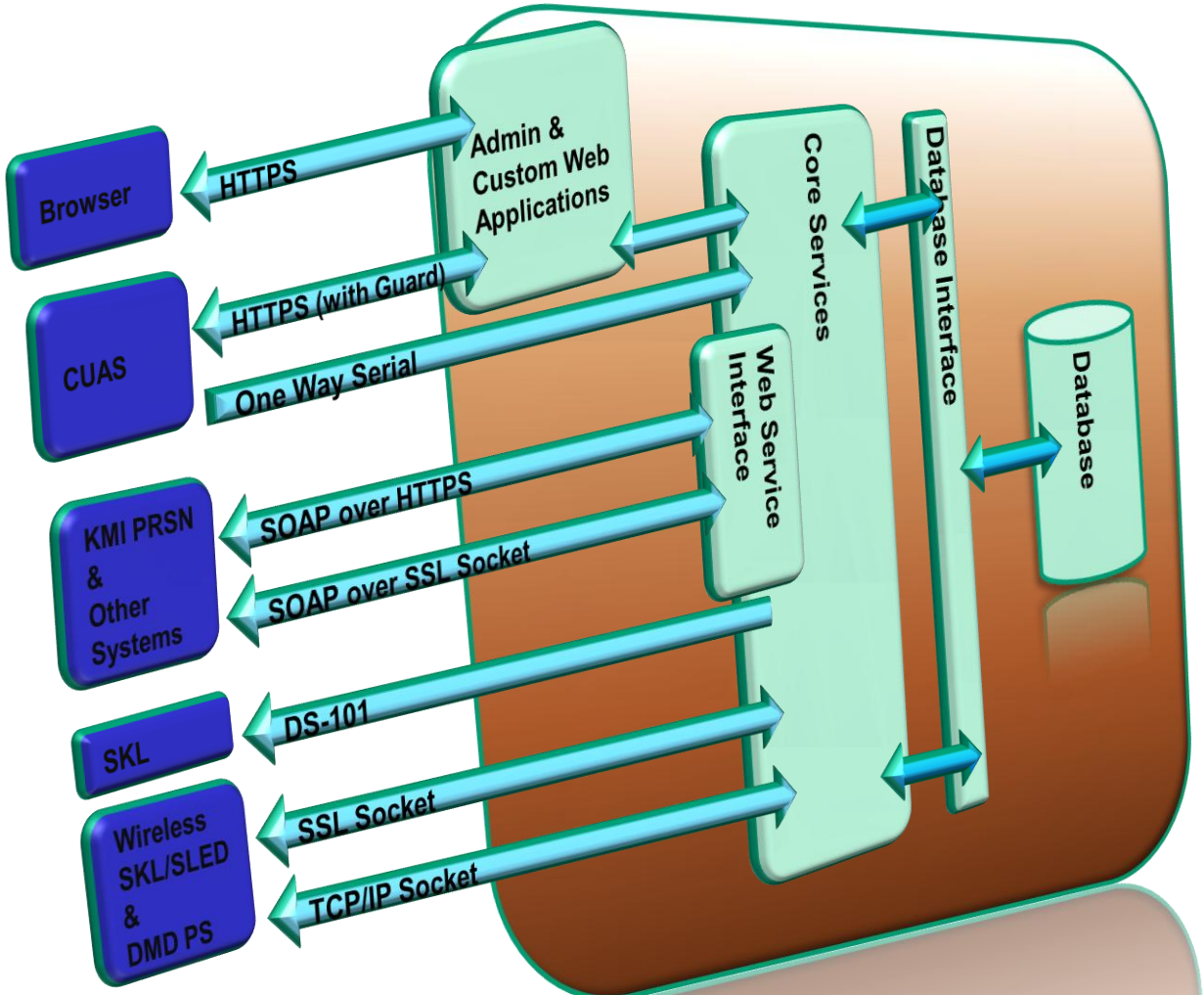
CDS

Black
Key
Server

F-22

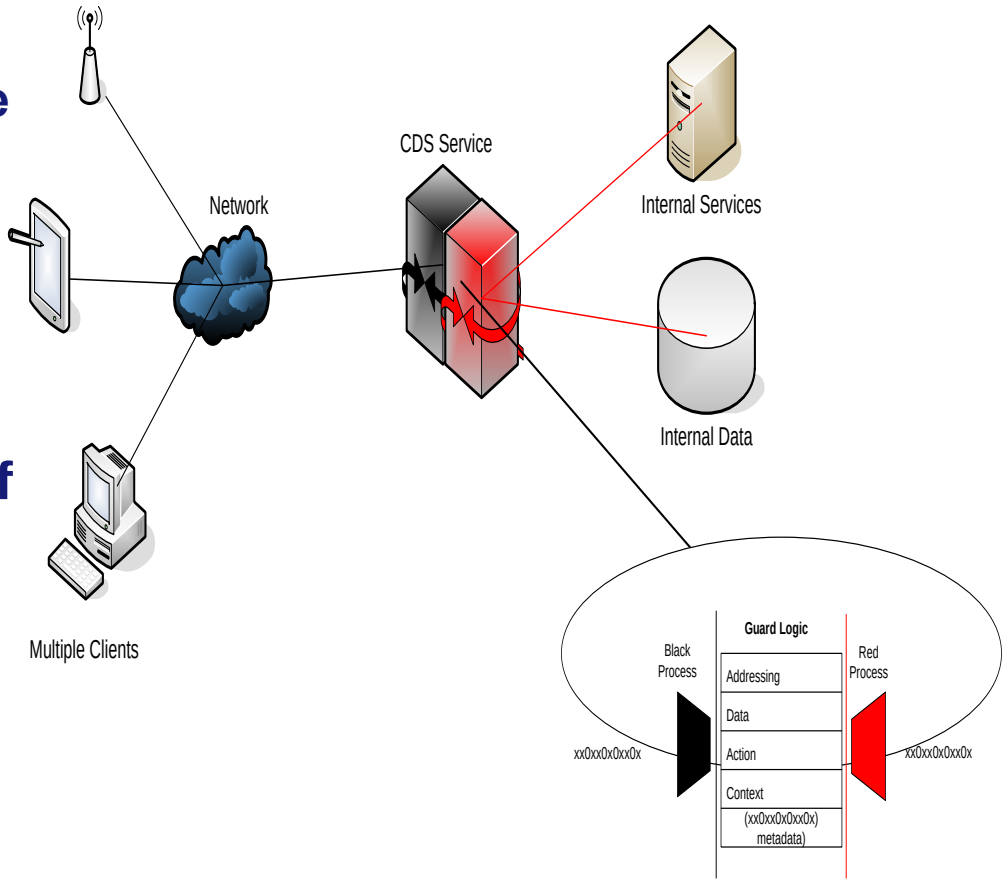
Phase III

Black and Benign Key Server Architecture



Cross Domain Solution

- "Official" Definition from the UCDMO –
  - "A form of controlled interface that provides the ability to manually or automatically access/transfer information between security domains"
- The newest Cross Domain Solutions are tools that attempt to allow the benefits of COTS software and services across information sensitivity levels.
- CDS solutions can utilize guard technologies, trusted systems, and COTS software to provide contemporary information services.



* Derived from David Carroll's CDS 101

Requirement #1 – Operational Zeroization

Threshold: Key Management Tier 2/3 systems shall be developed to provide COMSEC system keys to the F-22 End Cryptographic Units (ECU) during red ball zeroization within 10 minutes.

Objective: Tier 2/3 systems shall be developed to provide COMSEC system keys to the F-22 End Cryptographic Units (ECU) during red ball zeroization within 5 minutes.

Requirement #2 – Annual Re-key Initialization

Threshold: Key Management Tier 2/3 systems shall be developed to support an annual COMSEC Re-Key of all ECUs within the F-22 within 30 minutes or less.

Objective: Management Tier 2/3 systems shall be developed to support an annual COMSEC Re-Key of all ECUs within the F-22 within 15 minutes or less.

Requirement #3 – New/Spare ECU Initialization

Threshold: Key Management systems shall be developed to provide COMSEC system keys to the F-22 End Cryptographic Units (ECU) during ECU initialization within 15 minutes. This requirement is related to a maintenance/replacement event which causes a new ECU to be re-keyed.

Objective: Key Management systems shall be developed to provide COMSEC system keys to the F-22 End Cryptographic Units (ECU) during ECU initialization within 10 minutes or less. This requirement is related to a maintenance/replacement event which causes a new ECU to be keyed.

Requirement #4 – Rekey at Non-Host Base

Threshold: The mechanisms developed above shall not add more than 15 minutes procedurally when re-keying from a location other than the aircraft's host base.

Objective: The mechanisms developed above shall not add more than 5 minutes procedurally when re-keying from a location other than the aircraft's host base.

Rationale: It is anticipated that the F-22 may have emergency or other conditions which would cause the aircraft to land at locations other than the aircraft's host base. Those conditions must not impose excessive burdens on the aircraft maintainer in order to return the aircraft to flyable conditions.

Proposed Technical Solution (s)

- NSA Type 1 certified wireless device
- Leverage the SIPRNET to bridge the physical gap between the airframe and the COMSEC account.
- Designed to significantly reduce key distribution timelines and operational burden
- The technologies used are the Data Management Device (DMD), the Simple Key Loader (SKL), and the SECNET 11 wireless card and access point.