

THE FORCE MATERIEL CON

"Ensuring Information Superiority and Agile Combat Support"



FOR OFFICIAL USE ONLY

SKL Wireless & Black Data Distribution System Overview

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

THEORONG SISTEMS



The Good, The Bad and The Ugly



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:





DETARTMENT OF THE ALEROPANT BEADO VARIER: AR COMBAT COMMAND'S LANGLEY AR FORCES AND VIRGINIA.

ข ข ข ข

MEMORANDUM FOR F/A-22 SPO F/A-35 PMO AFCA/CC1

FROM:-ACC/A65

SUBJECT: Refinal Requirements to Support Banga Fill COMSEC Procedures (

1.—We exposity our issistance in addressing the COMSEC support equivements for the FIA-22, FIA-35, and any other system employing being in fill capitality in the future. In XXX00, Colonel XXXX from ACC/A8 submitted in equivement for COMSEC key to support the FIA-22 to be available until violent Normalities or less. Therefore our exposition in ACC are the protyce, we would like to during refine this requirement to better define the specific qualitative and need. §

2.— The requirement for COMSEC key should be defined in system keys would be mywhere in the world from Tier 2 to the system (FA-22 menuff) within 10 minutes on less. "This we entired to ACC has experienced multiple mission should each week due to lack of COMSEC key." Amend, which has eithery materialism "water," also in manage of 5 "phouse to give, other resulting in unacceptable mission should. This 10 minute key requirement has additional requirements to support this certability. "§

3.—Our expects from the microfilm internance truits, communications stands that have determined for our junction—with part from National Security Agency (NSA), Air Force Communications Agency (AFCA), Science Applications International Corporation (SAK), and Cryptologic Systems Group (CFSG) has the following requirements are necess to facilitate key availability world-water and to the microfile systems—[4].

 Worker SPRNet access on the flight line to the anenal on the ramp. This will require communication equipment and possibly personnel. No technical solution at this time.

by Argung protocol (IP) file transfer of key material. We believe we have the capability to deliver this requirement due to cooperation with all the requirementation of the capability to deliver this requirement still need to be almost due to the Air Force. We lit work with AFC Atoraffect a policy change, but requirement still needs to be almosted in appropriate documents at AirForce for el. 9

facility must have redundant communications paths (circuits and associated equipment); COMSEC key series, and 2447manning with subject matter expents of the committy each base spoor and manyower to support the age full COMSEC key equipments for each system and the learning curse is steep with an average of manths experience to gain path control of a addition, the services they have to reach back to far key materials are not always as addition. Consolidation of the age full services at using the facility state or manyower in upone PBD 720-world, neverth re-provides the SME support and connectivity required in a roasted facility care.

5. We will continue to work in cooperation with the operative and offices to improve COMSEC support for the F/A22 - We need your supports to document the requirements from the configuration and provide systems which are sustainable; supportable, manuscript and secure in meeting our entirely Air Force mission. My POC is Migor Robin-Gibson; ACC/A61A, DSN574-992 (2002) 571764-992, when gibson/Gibson; ACC/A61A, DSN574-992 (2002) 571764-992, when gibson/Gibson; ACC/A61A.

GREGORY-L-BRUNDIDGE, Colonel, USAF(
Dassing of Communications)

Global Power Systems (A)

- 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 caircraft 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



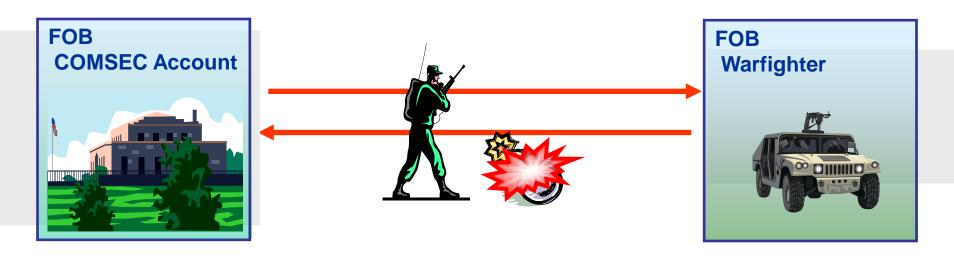
- ◆ Operational suitability of benign fill exchange
 - Operational impacts incurred due to multiple physical trips
 - Enhancements could cut tactical rekey time
 - Can't wait for single trip benign fill
 - KMI CI-3
 - Redesign of ECUs



Army Capability Gap



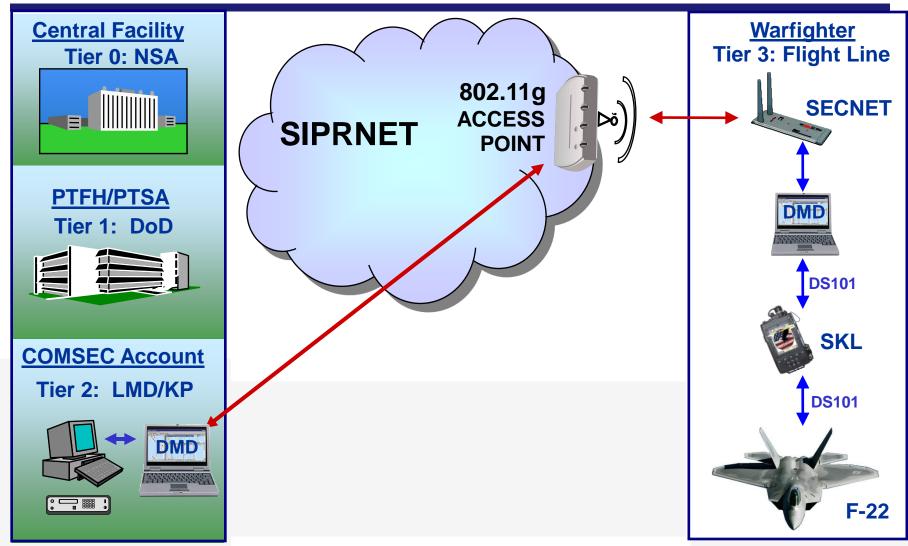
- Army Deployed Operations
 - Delivering Keys to forward deployed forces is difficult and dangerous
 - Leads to trips through potentially hazardous terrain exposing war fighters to ambush and IED's





Pilot Concept of Operations

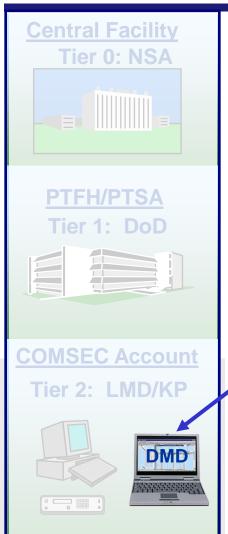


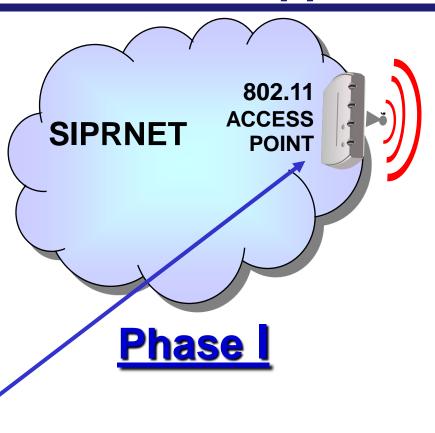




DMD-W Concept of Operations Client /Server Application





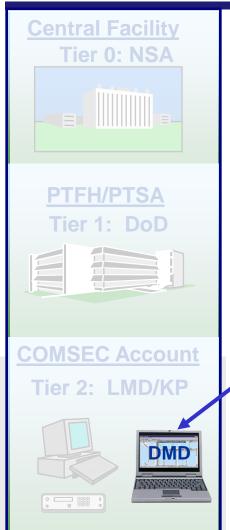


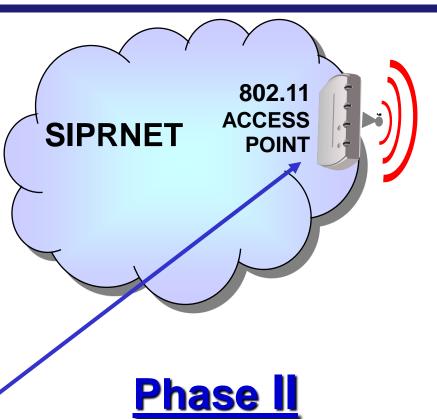




SKL-W Concept of Operations







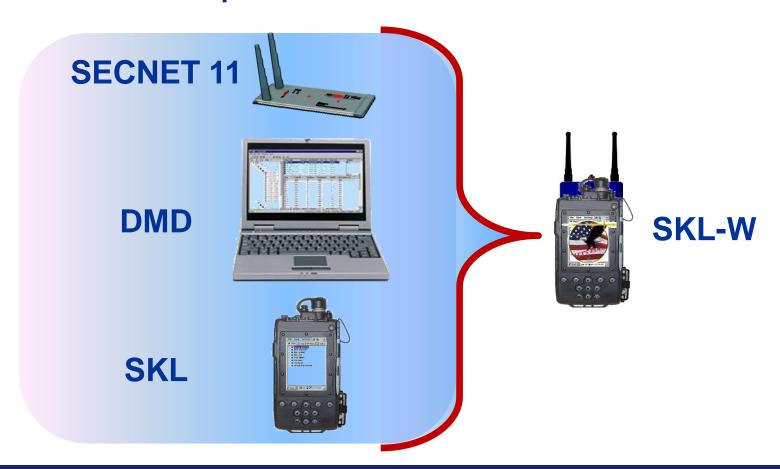




SKL-Wireless Concept



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





SecNet 11





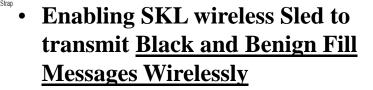


Standard SKL Battery or Fat Battery



This SKL-W version connects by:

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



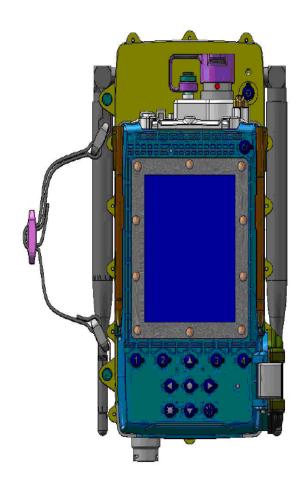
SNC Proprietary Information

USB



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 nonwireless 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





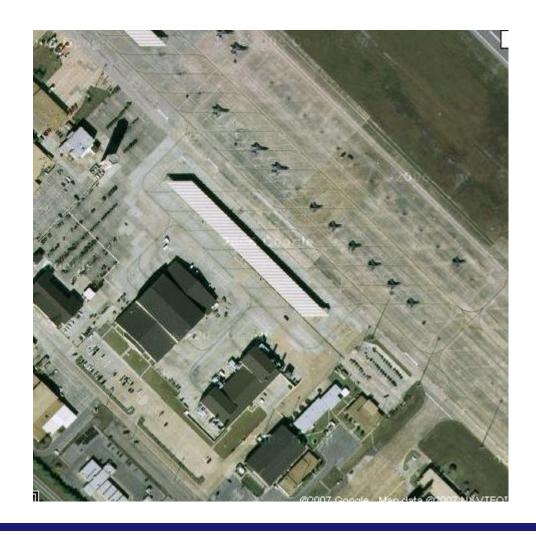
Baseline	Time
Redball / Rekey SKL 4.0	36min 44sec
Redball / Rekey SKL 5.0	32min 03sec

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

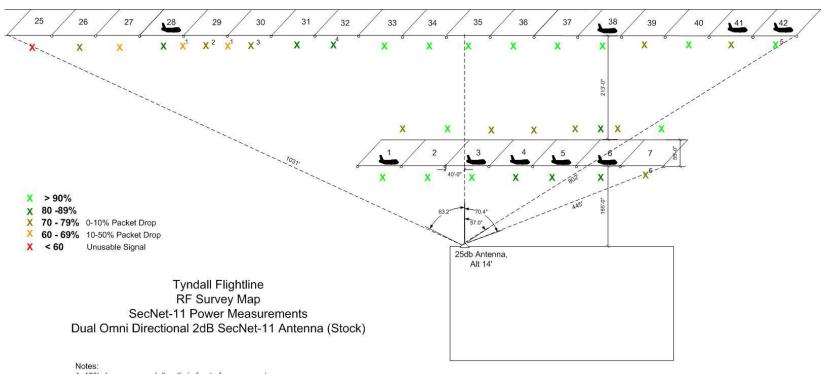






SKL –W Concept/Update



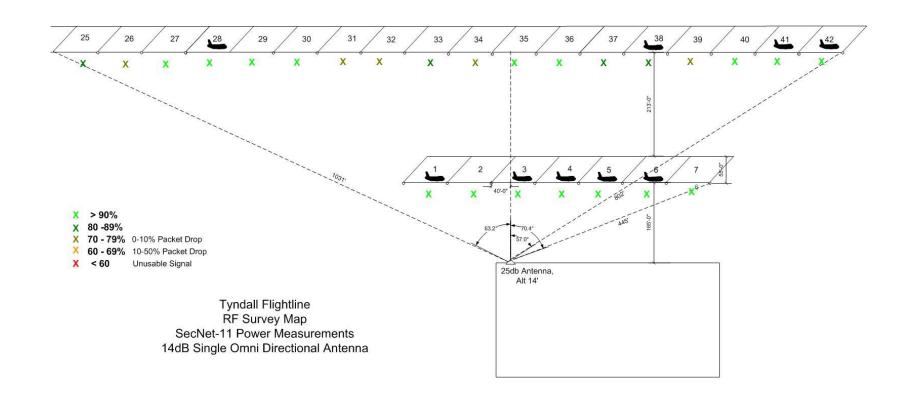


- 1. 10% drop measured directly in front of canopy posts.
- 2. Coordinates measured at 30.067506N, 85.580781W
- 3. Coordinates measured at 30.067131N, 85.580260W, obstruction by tail of A/C in spot 1.
- 4. Taxing A/C obstructing antenna caused 40% signal loss at this point.
- Measurement taken at 30.065180N,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



SKL –W Concept/Update







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







- 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

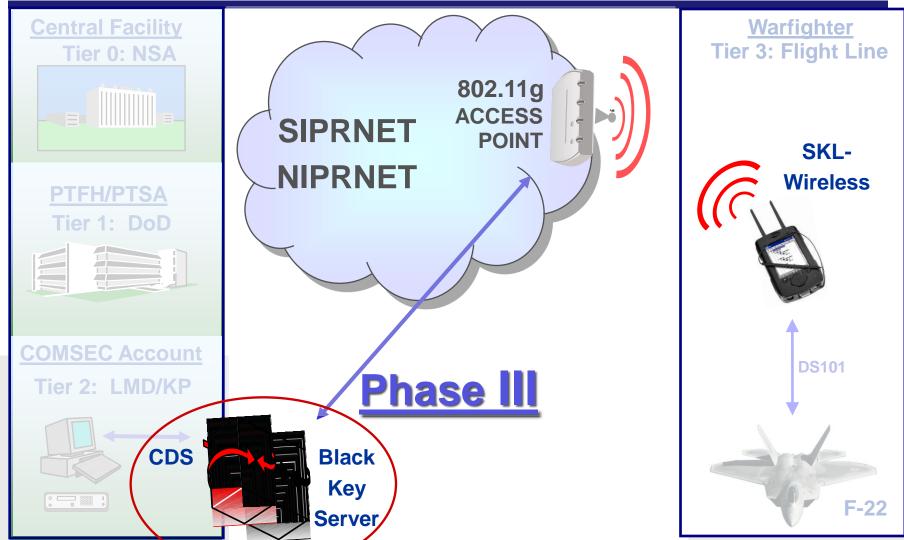


 Can be a stand alone device or part of a integrated Cross Domain Solution



Black and Benign Fill Key Server Cross Domain Solution

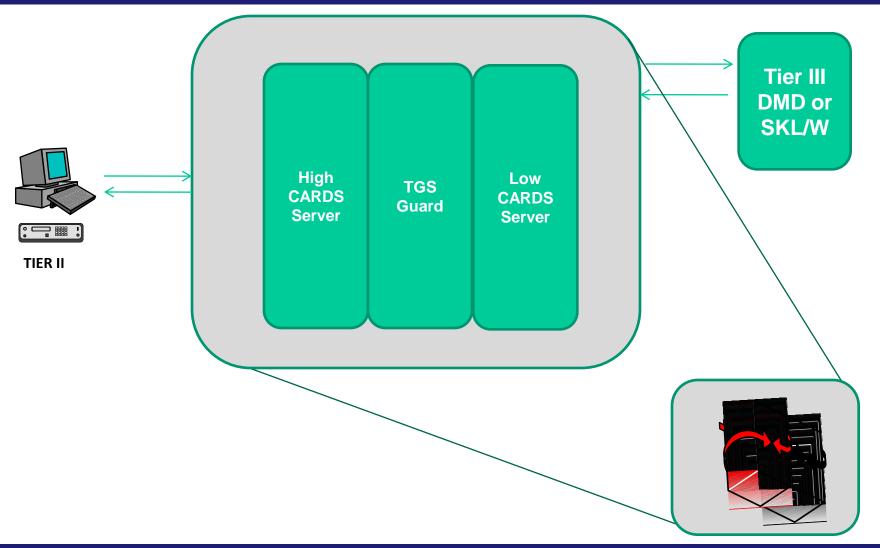






Black Key Server







Point to Point Terrestrial



Lab Configuration

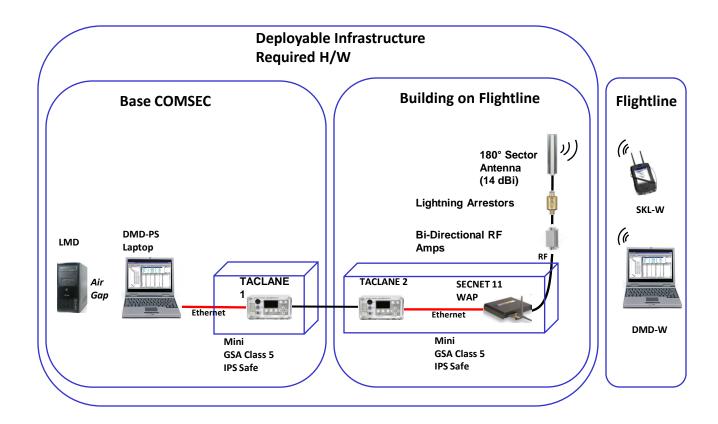
DMD PS (COMSEC) IP: 172.16.2.26

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???





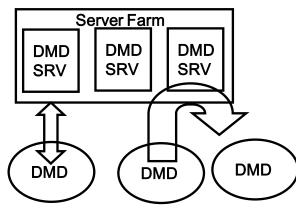


Black and Benign Client /Server Application (Phase I)

- 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 <u>August</u>
 2008

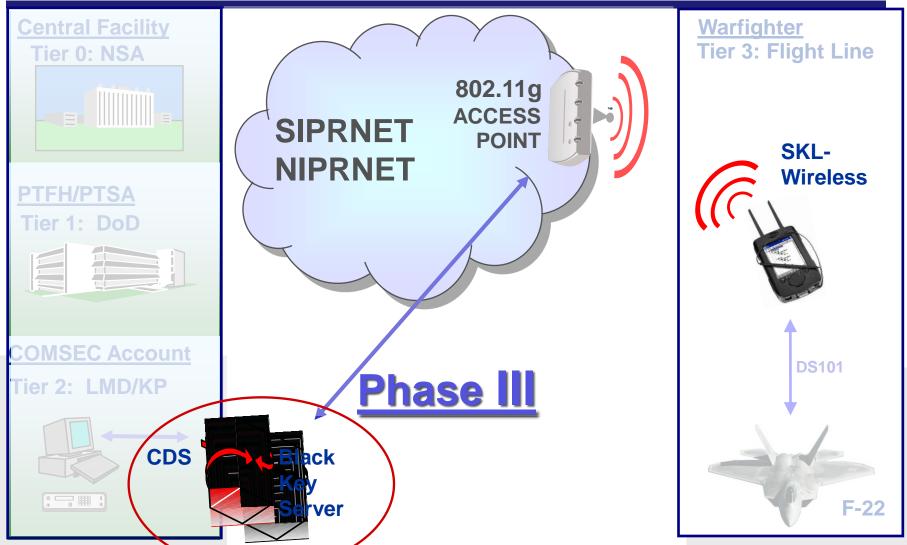


◆ Does not include C&A



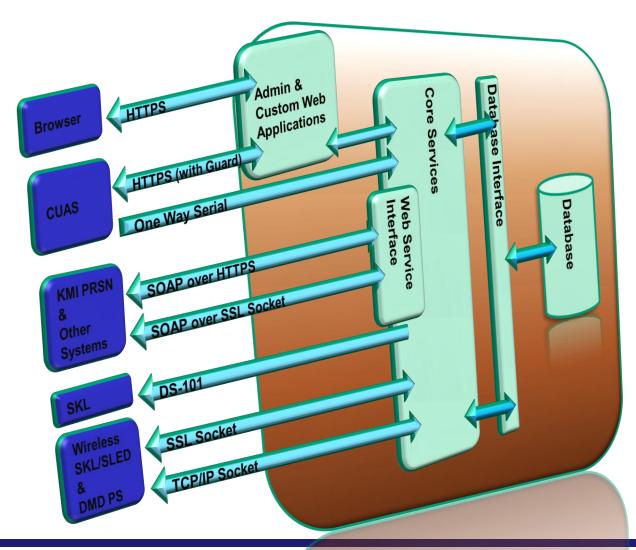
Black and Benign Fill Key Server **Cross Domain Solution**









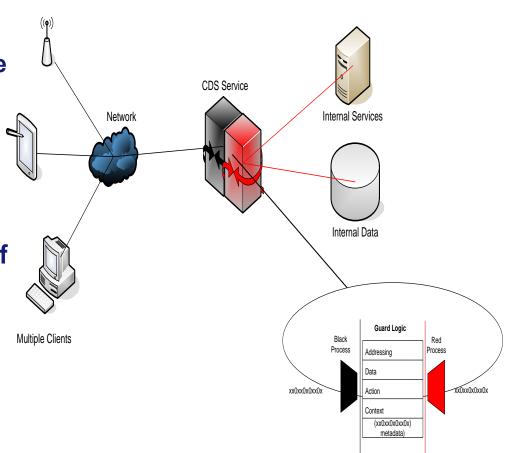




Cross Domain Solution



- "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.







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.