AGENDA

* Purpose
* Background
* Design /Configuration
* Concepts of Operation
* Hardware Requirements
* Software Requirements
* Security Precautions
PURPOSE

Seeking SRB approval for dial-up connectivity from the CIA-approved JFK SCIF to the ADSN.

Access to SQL Server and Lotus Notes Server
Background

The JFK SCIF is a CIA-Approved SCIF located at 600 E. Street N.W. and has been in operation for over a year.

The SCIF is located in the Department of Justice Building and has 24 hour guard protection. This location has been approved by the Agency for TS/SI/TK operations.
Background

The JFK Program is a Congressional Mandated Program and has been active since 1992.

* The Presidentially-appointed

√ The Assassinations Records Review Board is mandated by Congress, to complete its review and release of assassination records prior to October 1998.

* Due to this activity, Congressional oversight of this program has been raised to a higher level.
Background

To support this program DCI/CSI has established working documents on its systems that are critical to assure congressional compliance.

* SQL Server is the platform for the working documents.

* Lotus Notes is the communications medium of the Agency.
Concepts of Operation

* The system within the JFK SCIF will consist of two desktop workstations each connected to a 1910 STU-III Secure Data Device.

* Data Communications access control is provided by the AT&T Secure Access Control System (SACS).

* The Headquarters configuration consists of two 1910 STU-III Secure Data Devices attached to the ADSN/Communications server in room 2U22 NHB.
Hardware Requirements

2 Workstations

DELL 5166

Networks Access capability through Stu-III
Shared Local Printer
CD/FloppyDisk /Hard Drive
Software Requirements

Windows NT 4.0, Service PAK 3
Office 95
Lotus Notes 4.13
McAfee (Anti-Virus Software)
Copy.EXE (NT Secure Copying Utility)
Dscan (Classified data locator Utility)
Diskwash (Classified data locator Utility)
Security Precautions

Demonstrate:
*Effective technical means that non-Agency users cannot access Agency systems*

- DOJ Building is a Government Facility with 24 hour security guards.
- Workstations and STU-III will be secured.
- Agency personnel have been assigned to JFK SCIF
Security Precautions

Demonstrate:

*Effective technical means that non-Agency users cannot access Agency systems*

- All users have **STAFF/STAFF-LIKE** clearances with TS/SI/TK/G

- STU-III Key will be required

- **CHAP** (Challenge-Handshake Authentication)

- NT, SQL SERVER, Lotus Notes **Logons Required**
Demonstrate:  
Security Precautions

Process(s) of informed-human review and audit for information that is to be released from an Agency system to a non-Agency.

* Staff maintain ADP Badges for magnetic media handling.

* Diskettes will be created using the NT COPY, DISKWASH and DSCAN Utilities.

* Diskettes will be Virus-Scanned using Agency approved Virus protection software.

* AUDIT Procedures are in place. NT, SQL SERVER and Lotus Notes will have Audit utilities active.
Security Precautions

Demonstrate:
Identification of, and effective safeguards minimizing, risks of inadvertent or unwitting release of classified information.

- DOJ Building is a Government Facility with 24 hour security guards

- Workstations and 1910 STU-III will be secured within JFK SCIF

- All users have STAFF/STAFFLIKE clearances with TS/SI/TK/G

- 1910 STU-III and CHAP (Challenge-Handshake Authentication)

- NT, SQL SERVER, Lotus Notes Logons Required
Security Precautions

Demonstrated: Technical safeguards to avoid malicious code (that is, viruses).
Security Precautions

Demonstrate:
Procedural and technical safeguards controlling secondary interconnections to unauthorized systems.

- AUDIT Procedures are in place. NT, SQL SERVER and Lotus Notes have Audit utilities active. Audit logs will be reviewed weekly.

- All users have STAFF/STAFFLIKE clearances with TS/SI/TK/G

- 1910 STU-III and CHAP (Challenge-Handshake Authentication)

- NT, SQL SERVER, Lotus Notes Logons Required