

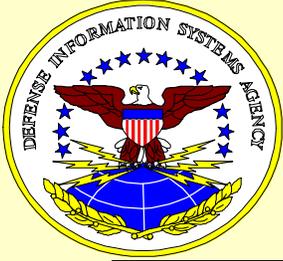


DISA / NSA DOD PKI



DOD Medium Assurance PKI



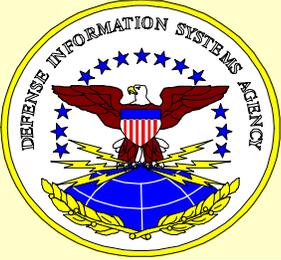


Why DOD PKI?



- **DOD PKI allows you to send documents electronically with the confidence that:**
 - The person sending the transaction is actually the originator
 - The person receiving the transaction is the intended recipient
 - Data integrity has been not been compromised

Note: DOD PKI is based on commercial standards.



PKI Assurance Levels

DOD PKI

BASIC

- Commercial

No DOD
infrastructure
planned

Selection based on:

- Security policy
- Legal requirements
- Cost of implementation
- Cost of information loss

MEDIUM

- Business Processes
- SBU Data

Pilot PKI System
fielded using
COTS products

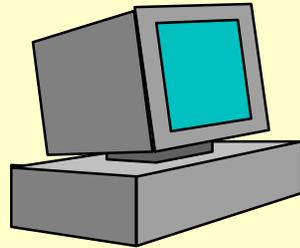
HIGH

- Command and Control
- National Security

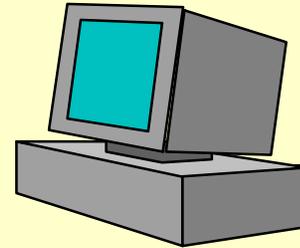
Operational PKI System
fielded:
(DMS/Fortezza)



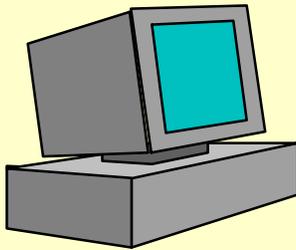
Technical Strategy - One Digital ID for DoD



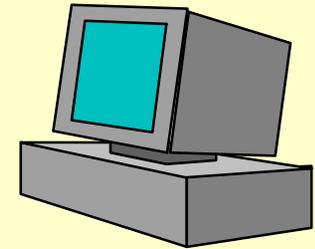
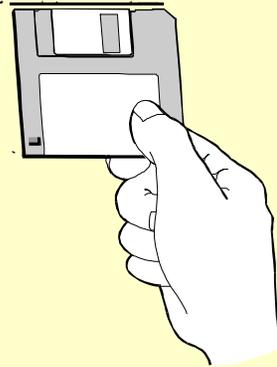
Procurement



Travel

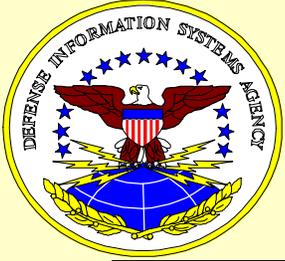


Medical



Personnel

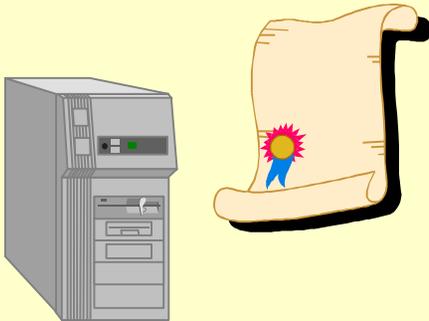
**Medium Assurance PKI Certificates
that prove identity only**



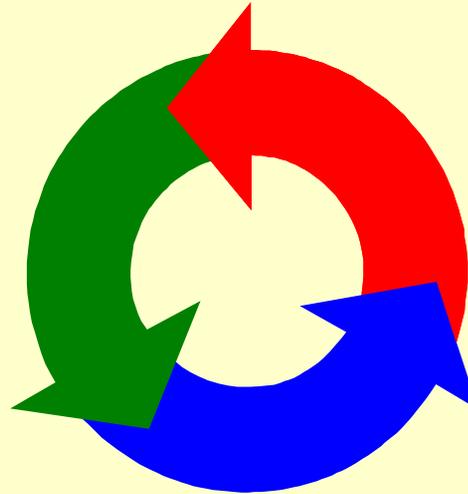
PKI-Enabled System Components



**CERTIFICATE
MANAGEMENT**

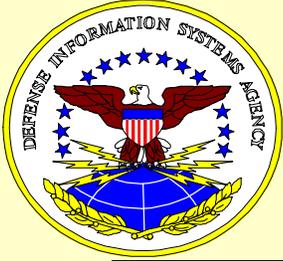


**REGISTRATION
PROCESS**



**PKI-ENABLED
APPLICATIONS**





DOD PKI Enabled Services

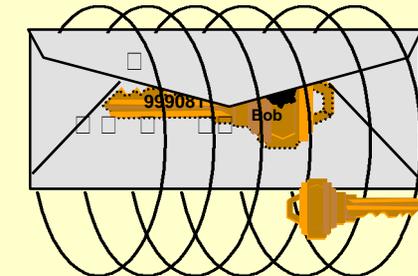
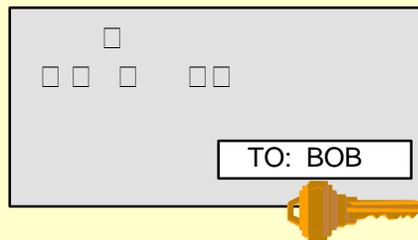
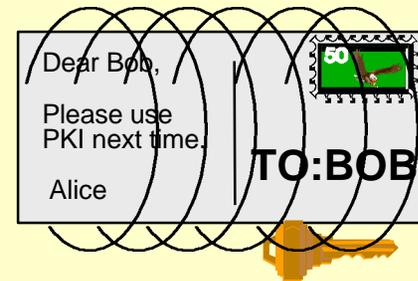
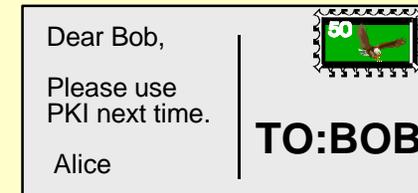


WITHOUT DOD PKI:

- No Protection

WITH DOD PKI:

- Digital Signature
- Encryption
- Encryption + Digital Signature





PKI Concepts

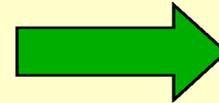
MATCHING PUBLIC/PRIVATE KEY PAIRS:



Public



Private



User
Tokens

PUBLIC KEY + NAME = CERTIFICATE

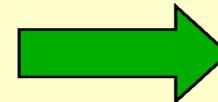


Public

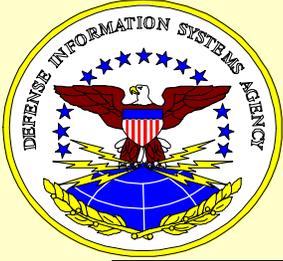
+



=



Electronic
Directory



What is a Digital Signature?

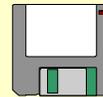
DOCUMENT



PRIVATE KEY

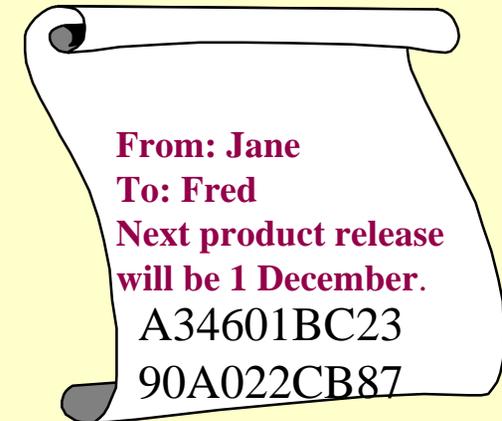
100101100

+

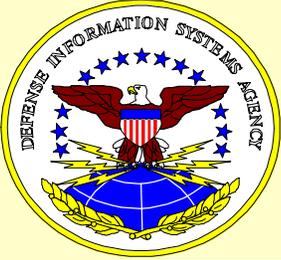


=

SIGNED DOCUMENT



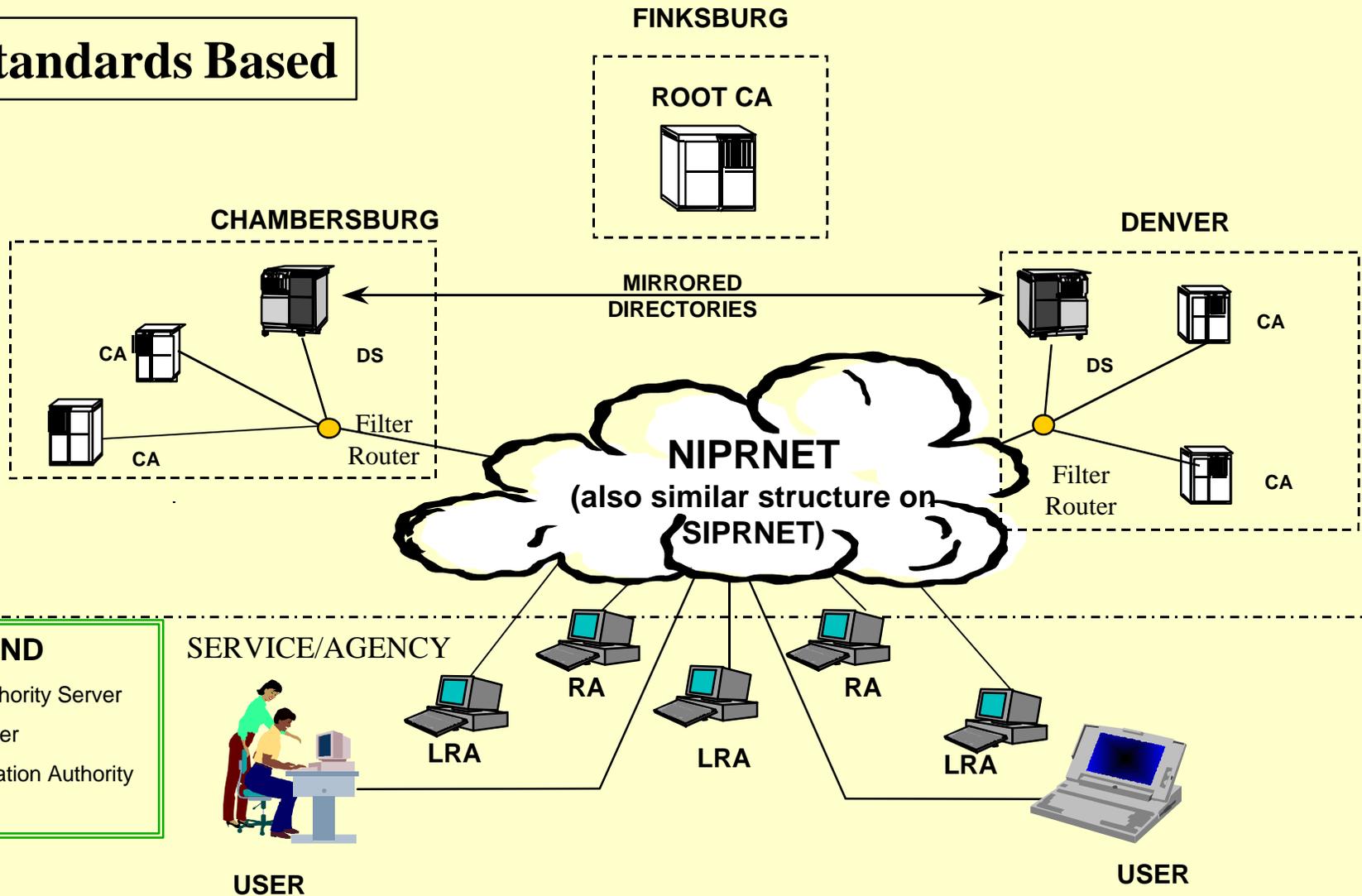
A digital signature is superior to a hand-written signature because the document can't be changed without detection.



Medium Assurance DOD PKI Pilot Architecture



Standards Based



LEGEND

- CA Certificate Authority Server
- DS Directory Server
- LRA Local Registration Authority



PKI Generic Components/Roles



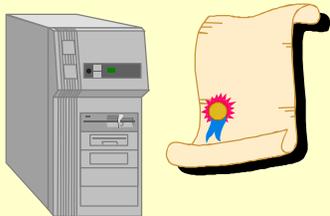
End User: requests certificates and uses keys in PKI-enabled applications



Local Registration Authority (LRA): authorizes creation of user certificates (sends to CA) and provides DOD PKI information to users



Registration Authority (RA): approves, registers, and oversees LRAs; performs user and LRA certificate revocation



Certificate Authority (CA): server that creates and signs certificates



DOD PKI Equipment Requirements



RA and LRA Workstations:

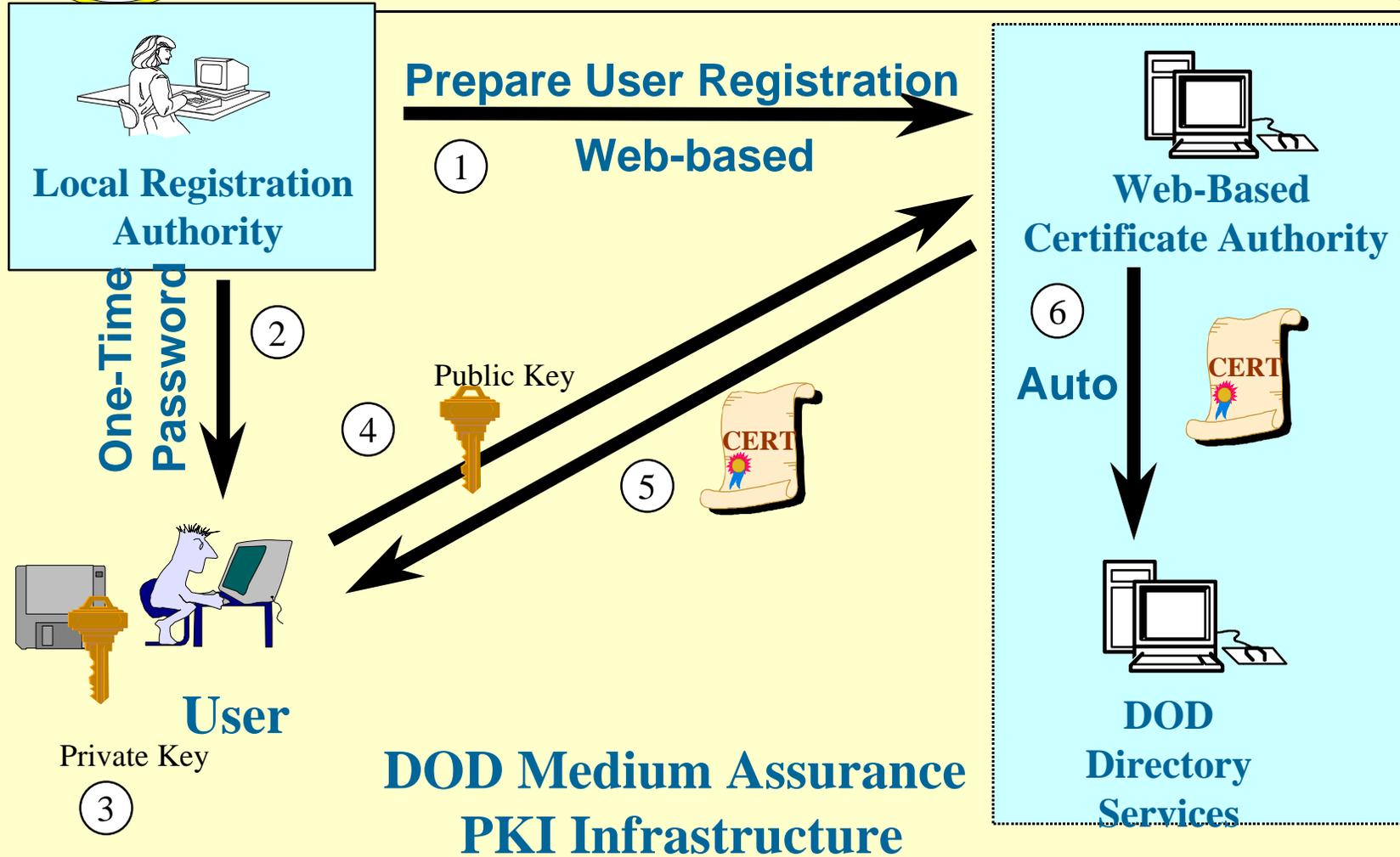
- ⇒ NT 4.0 Installed on Hardware
- ⇒ Litronic Card Reader (part # netsign 210 (050-1014-3NW) with Crypto Smartcards (part # 050 1105)
- ⇒ Dedicated (non-networked) printer
- ⇒ Netscape Version 4.05 (minimum for all)

End User Workstations:

- ⇒ Workstations with Netscape Version 4.05
- ⇒ 3.5" Diskette (or some other approved token)



Medium Assurance PKI User Registration

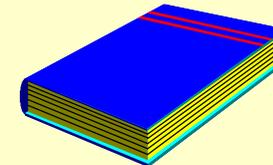


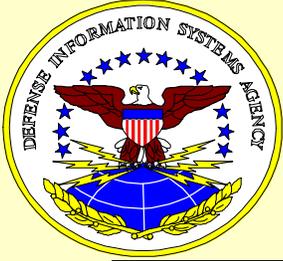


DOD Medium Assurance PKI: Available Now!



- **Certificates on NIPRNET**
- **Registration software and procedures**
- **Training**
- **24 Hour Help Desk Support**
- **Interface Spec for developers**
- **Test capability on SIPRNET**

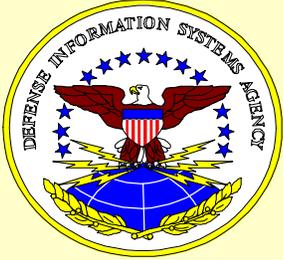




DoD Medium Assurance Pilots



Application Support	# of planned users	Initial Capability
Defense Travel System	400,000 (by 2QFY00)	May 99
Defense Security Service	300-2,500	May 98
Defense Information Systems Agency	20 → 8,000	Nov 98
WIPT (EDA)/ECA	6,000+	Feb 99
Army Chief of Staff	5,000	Oct 98
JEDMICS	26,000	Feb 99



Product Evolution

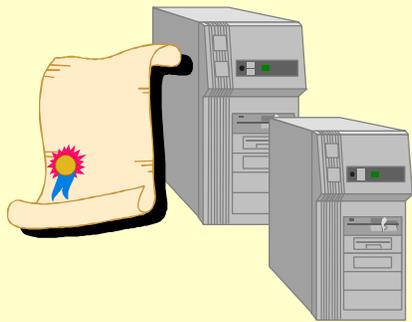
- **PKI Technology still emerging**
- **Medium Assurance Pilot uses first generation products**
 - **Basic capabilities**
 - **Interoperability issues between vendors**
- **Upgrades to be incorporated in future releases for pilot**
- **Second release expected to include:**
 - **Data recovery**
 - **Scalability improvements**
 - **Better interoperability between products**



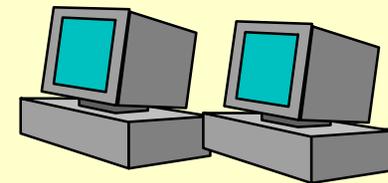
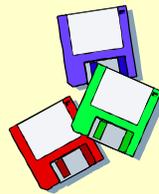
DOD PKI Medium Assurance Funding Strategy



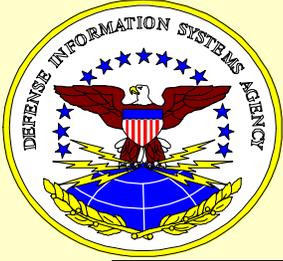
- **DISA/NSA: Infrastructure & Management**



- **Service/Agency: Registration & Application Enabling**



- **DISA/NSA: Infrastructure Operations & Maintenance thru FYDP**



Service/Agency Actions

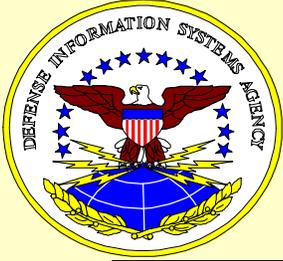


- **Coordinate PKI efforts thru Service/Agency PKI POC**
- **Plan for DOD-wide registration:**
 - **All DOD personnel should be registered**
 - **Decide on LRA functions:**



**Who?
Where?**

- **Consider LRA capacity**
- **Budget according to approach selected**



DOD PKI Working Group



The DII General Officers Steering Group (GOSC) established a DOD PKI WG (O-6 level) in December 1997

Chair: DISA D25

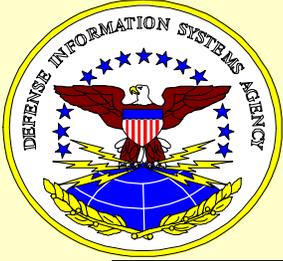
Service/Agency Representatives:

- Army: COL Michael Brown, ODISC4, (703) 604-7575
Gary Robison, ODISC4, (703) 604-7573
- Navy: Bob Buchanan, DCMS (202) 764-0003
CDR Chris Perry, CNO N64 (703) 601-1253
- Air Force: Roland Drumm, AFCA, (618) 256-2498
Neil Knowles, AFCIC (703) 697-2108
- Marine Corps: Gilda McKinnon, HQMC, (703) 693-3132
- Joint Staff: CDR Nick Harris, J6K, (703) 614-5990
- DLA: Stacy Hopkins, DLA/AQAC, (703) 767-3117
- DIA: Robert Cole, DIA, (202) 231-2182
- NSA: Gary Tater, X3, (410) 859-4527
- DISA: JP Angelone, DISA D25, (703) 681-7930



Backup Slides





Why Netscape?

- **Only FIPS 140-1 compliant product**
- **Netscape supports:**
 - **Open Standards**
 - **Multiple platform support**
 - **Data Recovery (next release)**
- **DISA Enterprise License w/Netscape provides:**
 - **DOD leverage in product features**
 - **Economies in fielding**
 - **Timeliness in meeting DTS fielding schedule**