Department of Defense SHA-256 Migration Overview

18 March 2011

Tim Fong
DoD-CIO/ IIA
Timothy.Fong@osd.mil

General Observations

- **This is Important – *INFOSEC: Algorithms can be compromised over time. Crypto algorithms constantly move to higher levels of complexity***
- **This is a Challenge – Transition to SHA-256 with limited or no mission operations breakage**
- **This will be Hard – Large complex DoD Network of Networks with SHA-1 implementations (workstations, applications, web services, etc…)**
- **This is just the beginning – Planning takes time, DoD & vendors are not ready, impacts not fully understood**

Directives

- **NIST SP 800-78,** *Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV)*
  - **Eff 1 JAN 2011 Federal Agencies will migrate their PKI cert from SHA-1 to SHA-256**

- **HSPD-12 and FIPS Pub 201-1** *PIV Standard*
  - **States PKI will be used for authentication**
  - **All new PIV credentials will have PKI certificates w/SHA-256**

- **OMB 11-11 (3 Feb 2011)** *Con't Guidance HSPD-12*
  - **Full use of the PIV credentials for access to federal facilities and information systems**

- **DoD-CIO Memo (14 OCT 2010)** *DoD's Migration … Cryptographic Algorithms*
  - **Components conduct portfolio assessment and develop a POAM**

Improving Security by supporting stronger cryptographic keys and more robust algorithms.

DoD CAC/PKI today …

- **Successful Deployment and Implementation**
  - ✓ **> 90% of target Population has a DoD CAC w/SHA-1 certs (ID, Email, Encryption)**
  - ✓ **Provides digital identities that are unique and un-forgeable**
    - **Used by ~3.7 million personnel**
    - **98% of DoD servers use certificates**
  - ✓ **Trusted for use in virtual network transactions:**
    - **Network Logon & Web Authentication**
    - **E-mail signing & encryption**
    - **Digital signing**

- **Most DoD Business Systems & Applications use PKI** (e.g.,DTS, ATAAPS, Military Efficiency Reports)

PKI is the key to Secure and Assured Information Sharing.

What has changed ?

- **Federal partners began issuing PKI certs with SHA-256 crypto algorithms and stopped issuing SHA-1 on 1 Jan 2011**
  - **Will impact systems & applications using PKI**
  - **Most current DoD systems & applications will not be able to process the new algorithm without software upgrades**
  - **Impacts already experienced at North Chicago, (DoD – VA)**

- **Immediate impact to DoD**
  - **Mission Assurance within the Department**
  - **Secure information sharing with our external partners (Federal and Industry)**

- **DoD is committed to maintaining the assurance of PKI credentials and supports need to migrate**

Potential Interoperability & Secure Information Sharing Challenge

What DoD Knows About SHA-256 Today

- **High level DoD assessment conducted in 4QFY10**
- **DoD Test & Evaluation WG initial findings**
  - **SHA- 256 is not supported in older version of Microsoft OS**
    - **Minimum MS OS is Windows XP SP3**
    - **Full functional support begins with MS Windows Vista/Win7**
  - **Most widely deployed CAC middleware currently does not support SHA-256 for MS OS/applications**
    - **Middleware does not implement MS mini drivers**
    - **Mini drivers must be used within MS cryptography architecture to access SHA-256 algorithms**
- **DoD is aware of other application problems documented by Federal Partners**

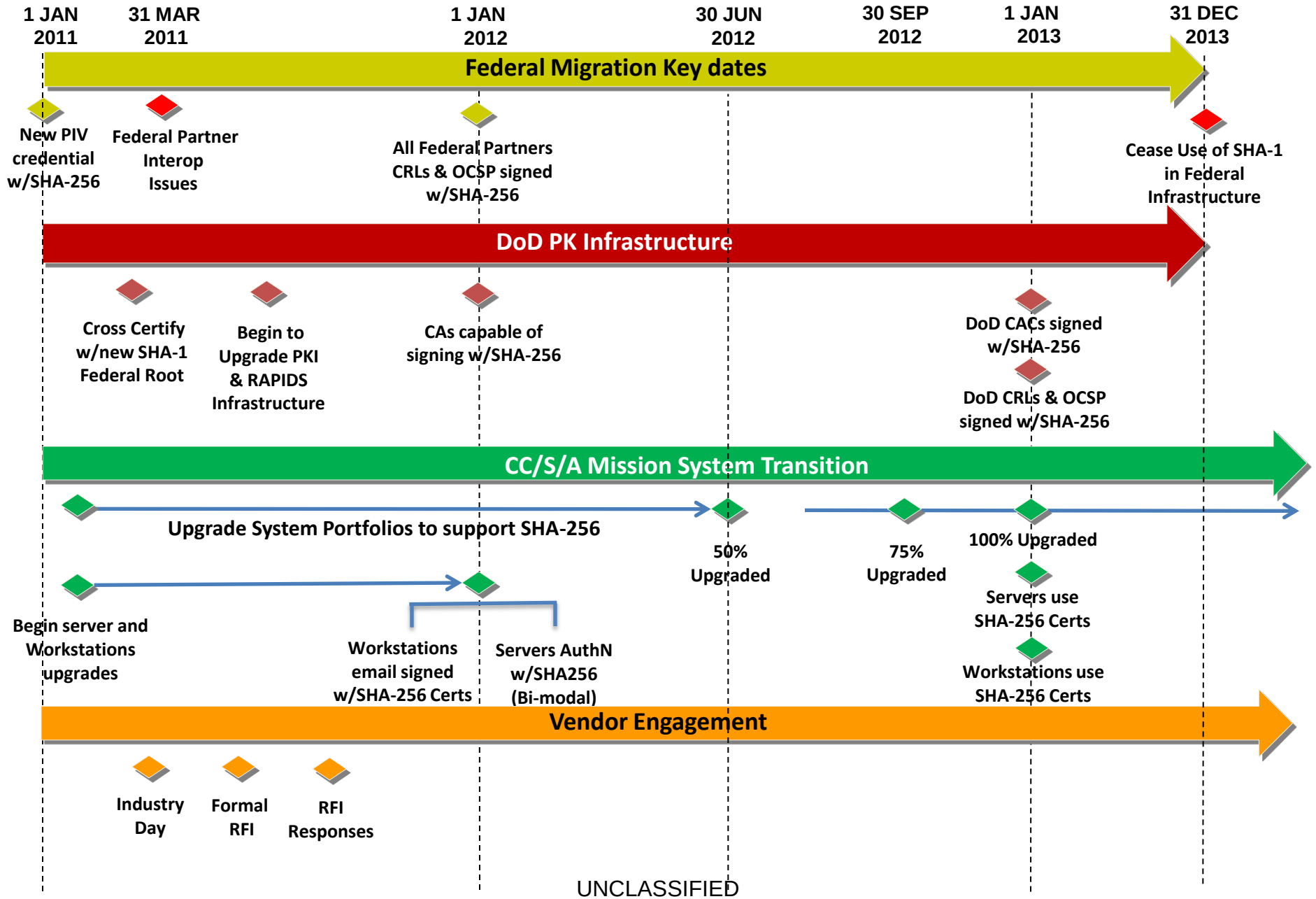
What we're planning to do …

- **Strategy: Transition DoD IT environment over time**
  - **Provide DoD Guidance w/Roadmap and Milestones**
  - **Engage Vendors & Manufacturers to determine plans for product support of SHA-256**
  - **Upgrade systems & applications to handle SHA-256 as soon as possible but NLT 31 Dec 2012**
  - **PKI/CAC infrastructure can begin to issue SHA-256 as soon as IT infrastructure can support its use but NLT 1 Jan 2013**
  - **Once SHA-256 issuance begins in DoD, users will receive CACs with SHA-256 through the normal CAC 3-Year Lifecycle**
  - ***Goal: Implement transition plan as quickly as possible***

- **Resource Owners**
  - **Develop detailed Plan of Actions & Milestones (POAM)**
  - **Upgrade affected systems & applications NLT 31 Dec 2012**
  - **Follow the Guidance**

Supporting Operations: Internal and External Customers.
"Don't Break Anything"

DoD SHA-256 Transition Major Milestones



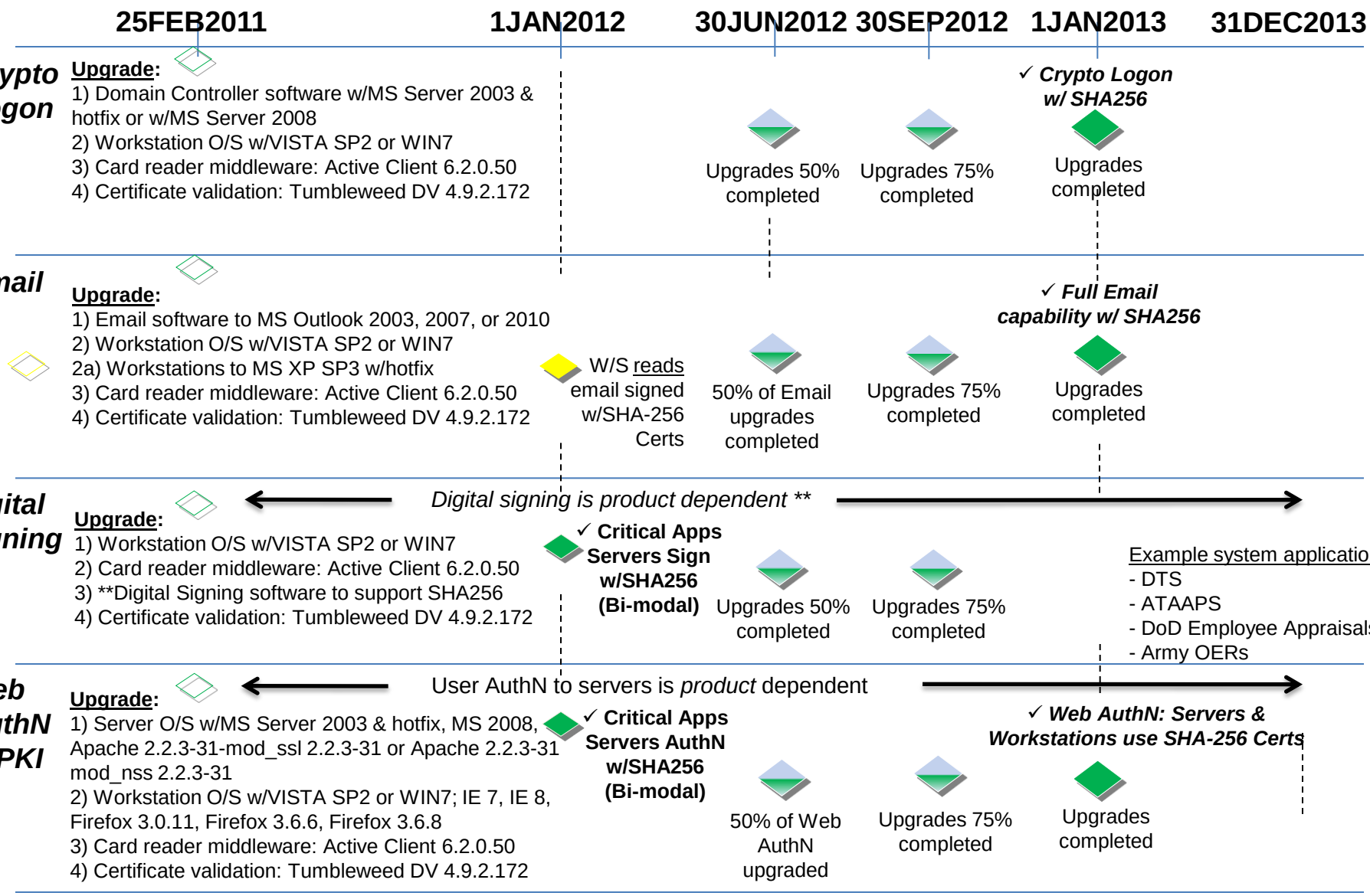
What we're going to do …

Operational Strategy: Bi-modal Operations Support

- **Minimize operational impact**
- **Efficiently migrate systems to support use of SHA-256.**
  - **Infrastructure will support both SHA-1 and SHA-256 for a period of time**
  - **Transition AuthN to bi-modal to support DoD and external customers**
  - **Phase in DoD use of SHA-256 signed certs while phasing out SHA-1**
- **Support basic capabilities: Crypto Logon, Email Signing, Digital Signing, Web Authentication**
- **Priorities: Operation of DoD systems, and Interoperability between DoD and approved external PKIs**

- **Major actions & milestones:**
  - **Upgrade affected Systems and Applications <u>NLT 31 DEC 2012</u>**
    - **Domain Controllers, AuthN servers, Web servers, Email servers**
    - **Workstations, CAC middleware, Email clients**
    - **Digital Signing and Certificate Validation software**
  - **Upgrade PKI and RAPIDS Infrastructure by 31 DEC 2012**
  - **Start issuing DoD certs w/SHA-256 NLT 01 JAN 2013**
  - **Stop issuing DoD certs w/SHA-1 NLT 31 DEC 2012**

What C/S/A need to do to use SHA-256 …



Current Migration Efforts

- **DoD Task Force: DRAFT DoD Guidance with Roadmap and Milestones**
- **DoD Coordination Cell: meets every Tuesday @1130**
- **Crypto Migration Team: Identify; Anecdotal Test ing**
  - **Commonly-used applications supporting internal Fns**
  - **Critical applications for external customers**
  - **DoD PKE team post results and guidance on PKE website**
- **Vendor Engagement**
  - **Contact primary application manufacturers and vendors regarding SHA-256 compliance developments**
  - **Include as a requirement in all contracts**

Next Steps

- **Issue DoD Guidance w/Roadmap**
- **Services and agencies Develop POAMs**
  - **Where are they today**
  - **Plans for upgrade**
  - **Resource requirements**
- **DoD CIO monitors progress and challenges**

What can you do?

1. What will be the Vendor concept for support during SHA-256 transition? (Also address initial support for RSA 2048 certificates and long-term plans for ECC support.)

2. Does your current product suite support SHA-256? If so, is the support version specific -- explain. If not, what is the projected timeframe for support? Do you anticipate having beta test suites available for customers prior to general public release and configuration guides?

3. How will the Vendor address COTS product minimum required versions for SHA-256 support, with backward compatibility for SHA-1?

4. What capability will the Vendor have to conduct product testing, evaluation and acceptance procedures to ensure complete compatibility?

5. How will the Vendor transition their products from SHA-1 to SHA-256 RSA 2048 and eventually to ECC (ie., general plan and milestones)?

6. How will the Vendor address validating product claims of compatibility? (ie., certification)

7. What are the vendor's anticipated impacts to their current DoD customers?

8. How can the vendor or manufacturer's product transition minimize the impact to the DoD's transition?

9. How will system integrators address these same questions?

Questions?

Tim Fong
Deputy Director, IdA/PKI
DoD-CIO/DASD IIA
703-604-3156
Timothy.Fong@osd.mil