DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DoD Mobility

Mobility Product Security Certification Processes

Greg Youst

DISA Chief Mobility Engineer
25 May 2017

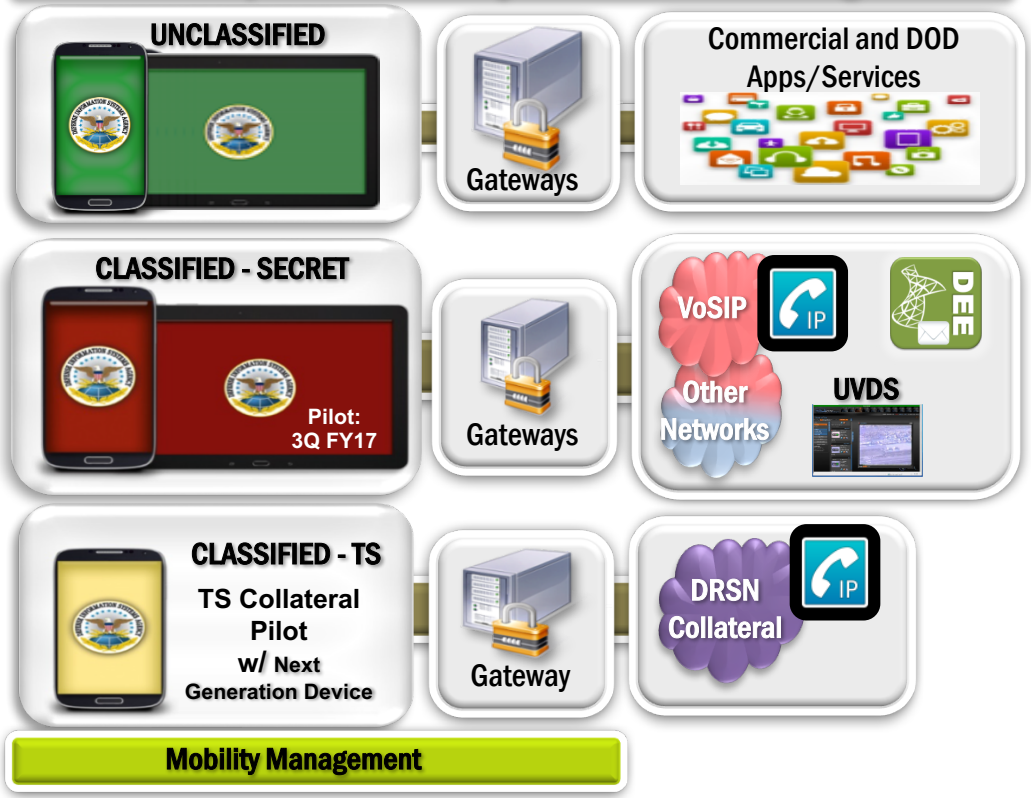
Agenda

- DoD Mobility
- Unclassified Mobility Certification Process
- Main DoD Approved Product List (APL) Process Steps
- Classified Mobility Certification Process
- CSfC System Deployment Process
- Application Vetting Requirement/Certification
- Appropriate URLs

NOTE: All information either already presented publicly or presently available via the Internet

DoD Mobility

Enterprise Mobility Service Offerings



FUTURES

Access to Tactical & COI Networks

Access to C2 Services

GCCS-J

Next Generation Assured Identity

VDI & Cloud

Unclassified Mobility Certification Process

- **Unclassified mobile devices and Mobile Device Management are National Information Assurance Partnership (NIAP) certified.**
- **Tested to the respective NIAP Protection Profile**
- **NIAP certification requires FIPS 140-2 Certification to complete**
- **Successful mobility equipment listed on the DoD Approved Products List (APL)**
- **Mobility Unified Capability products are tested in accordance with the Mobility Use Case #3 APL Process per the Unified Capability Requirements (UCR) document Section #8 MULTIFUNCTION MOBILE DEVICES (MMD)**

Main DoD Approved Product List (APL) Process Steps

1. Vendor obtains FIPS 140 and National Information Assurance Partnership (NIAP) Protection Profile (PP) certification if applicable (Mobile Device and MDM).
2. Vendor develops STIG for submittal to DISA Risk Management Executive (RME)
3. DISA RME validates STIG and gets DISA Approving Officer (AO), signed approval
4. Vendor complete the SF328 Foreign Interest Form if first time submitted or submit a VP signed SF328 “No Change Letter”
5. Vendor completes the appropriate IPv6 Letter of Compliance (IPv6LOC) VP Memorandum and Section 5 as Use Case #2 requirements

Main DoD Approved Product List (APL) Process Steps

(Continued)

6. Vendor obtains Mobile Device, Mobile Device Management, Mobile Support System signed STIG memorandum from IASE web site
7. Vendor submits MD, MDM or Mobile Support System on Approved Products Integrated Tracking List (APLITS) with supporting documentation
8. DoD Approved Products List (APL) Mobility Manager approves mobility product submittal
9. Product placed on the DoD Approved Products List

Classified Mobility Certification Process

The NSA/CSS's Commercial Solutions for Classified (CSfC) process enables commercial products to be used in layered solutions to protect classified NSS information. This provides the ability to securely communicate, based on commercial standards, with a solution that can be fielded in months, versus years.

Capability Package

- **NSA has developed, approved, and published solution-level specifications called Capability Packages (CP)**

Protection Profiles

- **NIAP works with technical communities from across industry, governments, and academia to develop product-level requirements called USG Protection Profiles used by NIAP for certifications.**

Classified Mobility Certification Process

(Continued)

CSfC Certification

- Vendors who wish to have their products eligible as CSfC components of a composed, layered IA solution, must build their products in accordance with the applicable NIAP Protection Profiles and submit their products using the Common Criteria process.
- Vendors test to the appropriate NIAP Protection Profile but include the CSfC Selections for the specified Component listed on CSfC Components List. CSfC Selections are NIAP PP Objectives that are tested as "required"
- NSA then enters into an agreement with the vendor which may stipulate other requirements for that particular technology prior to listing.

CSfC System Deployment Process

1. **CAPABILITY PACKAGE (CP) PUBLICATION: NSA Publishes CP**
2. **CP EXECUTION: Govt. Customer Implements Solution Based on CP Requirements**
3. **SOLUTION TESTING: Government Customer Conducts Site Based Testing on Solution**
4. **CP REGISTRATION: Government Customer Registers with NSA to use CP**
5. **SOLUTION APPROVAL: NSA Provides Government Customer with Solution Approval Memo**
6. **APPROVING OFFICIAL (AO) AUTHORIZATION: Government Customer AO Grants Authority to Operate (ATO)**

Application Vetting Requirement/Certification

The mobility application vetting requirement is basically the same for both Unclassified and Classified, what varies is how it is implemented. Both processes utilize the same application security controls in the NIAP Application Software Protection Profile but who does the application testing is different. Note that Unified Capabilities (UC) mobile applications are still tested at the Joint Interoperability Test Center (JITC) for UC verification and approval while NIAP testing is conducted to determine threats.

Unclassified

- **The DoD component vets the application utilizing the NIAP App Protection Profile security controls and determines residual risk level**
- **Based on residual risk level the Approving Official either accepts or rejects the use of the application. If approved, application may be deployed**

Application Vetting Requirement/Certification

(Continued)

Classified

- **Application Vendor determines if any CSfC Selection security controls apply to the application based on its use and coordinates with CSfC office for validation**
- **Vendor submits application along with any identified CSfC Selection security controls to NIAP for independent test lab certification.**
- **Based on the test results, NIAP certifies the application with CSfC Selection controls.**
- **CSfC list the approved application on the CSfC Components List**

Appropriate URLs

The following Links will get you started:

- **Approved Products Integrated Tracking List: https://aplits.disa.m**
- **Approved Products List (APL): https://aplits.disa.mil/processAPList**
- **CSfC Background: https://www.nsa.gov/resources/everyone/csfc/**
- **CSfC Capability Packages: https://www.nsa.gov/resources/everyone/csfc/capability-package**
- **CSfC Components List: https://www.nsa.gov/resources/everyone/csfc/components-list/**
- **National Information Assurance Partnership (NIAP): https://www.niap-ccevs.org/**
- **NIAP Protection Profiles: https://www.niap-ccevs.org/Profile/PP.c**
- **NIAP Certified Products: https://www.niap-ccevs.org/Product/**

Appropriate URLs

(URLs Continued)

- **Unified Capability Requirements (UCR) document: http://www.disa.mil/Network-Services/UCCO/Policies-and-Procedures**
- **Cryptographic Module Validation Program (CMVP) [FIPS 140-2]: http://csrc.nist.gov/groups/STM/cmvp/**
- **FIPS 140 Cryptographic Algorithm Validation Program (CAVP): http://csrc.nist.gov/groups/STM/cavp/index.html**
- **CMPV FIPS 140 Module Validation List: http://csrc.nist.gov/groups/STM/cmvp/validation.html**
- **CMPV FIPS 140 Vendor List: http://csrc.nist.gov/groups/STM/cmvp/validation.html#01**

Questions?

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**