2013

Vendors User’s Guide to Approved Product Lists

Version 1.1

19 December 2013

Table of Contents

1. Approved Products Lists (APL)

The Approved Products Lists (APL) covers both interoperability with Unified Capabilities (UC) installed on the operational network and Information Assurance (IA). In accordance with CJCSI 6211.02D (24 Jan 2012) and DoDI 8100.4 (9 Dec 2010), most products purchased cannot be installed on the operational network unless they are from the UC APL. In accordance with federal laws, products cannot be purchased if they involve protecting information with encryption or use personal identity verification on systems. These programs are the Cryptographic Module Validation Program, Common Criteria Evaluation & Validation Scheme, Federal Identity, Credential and Access Management and HAIPE. In accordance with CNSS 300 – National Policy on Control of Compromising Emanations, DOD Directive C-5200.19 and NSTISSAM TEMPEST 2-95, commercial telecommunications products that process classified information are required to be certified by the NSA Certified TEMPEST Products Program.

The UC APL tests the interoperability of the product, not the NSA cryptography or FIPS standards required for personal identification. If the product is listed on the UC APL, the product is certified for both interoperability and information assurance. If there is not a product listed on the UC APL to meet your requirement, then see DoDI 8100.4 for how to sponsor the product for approval. If there is not a product listed on an IA APL to meet your requirement, follow the guidelines on each IA APL for how to sponsor the product for approval. In some cases, the APLs are lagging behind current and emerging technology that may be needed to meet a requirement. The NETCENTS-2 contract does not prohibit customers from purchasing products that are not yet on an APL, but if it is required, then IAW with DoD policies and federal laws, you may have to sponsor the product through the process before it can be utilized.

If your product category is listed on the applicable APL, and the APL contains products that meet your requirements, then mandate the offeror "shall" provide a product from the applicable APLs to meet your requirement by stating it as a standard in your SOO/TRP. You cannot specify a specific brand name, only the specifications and standards that need to be met (unless you accomplish a brand name justification). If your product category is listed on the UC APL but no products are listed yet, then it is not required to come from this APL. **The absence of a product from the UC APL does not preclude the use of the IA APLs; therefore you must check these APLs when applicable.**

IT, security, connection, and DOD CIO waiver requirements for non-DISN DOD networks such as the Defense Research Engineering Network (DREN), SECRET Defense Research Engineering Network (SDREN), Combined Enterprise Regional Information Exchange System (CENTRIXS), or other DOD networks (e.g., standalone or training enclaves) **not connected to the DISN are outside the scope of CJCSI 6211.02D.** For guidance on these networks, contact the DOD CIO and/or network owners (e.g., Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) for DREN and SDREN). **Research and Development, testing facilities and other certain entities are not required to follow these APLs and can follow their applicable acquisition policies.**

In accordance with CJCSI 6211.02D (24 Jan 2012) and DoDI 8100.4 (9 Dec 2010) most products purchased cannot be installed on the operational network unless they are from the appropriate Approved Products List (APL). This appendix is provided to assist customers in documenting their requirements related to the APLs. Consult the applicable APL outlined below prior to ordering equipment to see if the products from the applicable APL meet your requirements. If there is not a product listed on the APL to meet your requirement, then see section 1.1.4 for guidance on how to sponsor the product to be approved. In some cases, the APLs are lagging behind current and emerging technology that may be needed to meet a requirement. The NETCENTS-2 contract does not prohibit customers from purchasing products that are not yet on an APL, but if it is required, then IAW with DoD/USAF Policy listed above, you may have to sponsor the product through the process before it can be utilized.

There are currently six APLs in use: UC APL, Cryptographic Module Validation Program, Common Criteria Evaluation & Validation Scheme, Federal Identity Credential, Access Management, HAIPE and TEMPEST. The APL used depends on the requirements associated with the products being purchased (crypto, TEMPEST, etc.)

1.1 DoD UC APL

1.1.2 Purpose

The DoD Unified Capabilities (UC) APL is established in accordance with the UC Requirements (UCR 2013) document. Its purpose is to maintain a single consolidated list of products that have completed Interoperability (IO) and Information Assurance (IA) certification. Use of the DoD UC APL allows DoD Components to purchase and operate UC systems over all DoD network infrastructures.

Per DoDI 8100.04, all networks that support Unified Communications (UC) shall use certified products from the DoD UC APL, which may be found at: http://disa.mil/ucco. However, not all Products support UC, therefore not all products are required to come from the APL (i.e. Hosts, Servers). Check the UCR 2013 to see what products support UC before making the APL a requirement. Some examples of the types of hardware that are required are: routers, switchers, repeaters, wireless LAN equipment, firewalls, VPN concentrators, encryptors, IA tools, and data storage controllers.

If your Product is required to come from the UC APL (i.e. there is a category) but none of those products meet your requirement then the requesting unit may sponsor (per DoDI 8100.3) to have that product tested and added to the APL or seek an APL waiver. Further guidance can be found in the UCR or contacting the UCCO help desk via email at UCCO@DISA.MIL.

1.1.3 Types of Products required to come from the UC APL

Category: Network Infrastructure

- Transport – AGS Device, OTS, FNE, DNE, Access Aggregation Function M13 Device
- Enterprise Network Management – Element Management System, Operational Support Systems
- Routers/Switches – Aggregation Router, Provider Edge Router, Customer Edge Router, Access IP Switch, Distribution IP Switch, Core IP Switch, Wireless LAN Equipment
- Storage – Data Storage Controller
- Security – EBC, Data Firewall, VPN Concentrator, IPS, HAIPE, Link Encryptors, Integrated Security Solution, IA Tools, Network Access Control

Category: Voice, Video and Data Services

- Classified Voice – LSC, Dual Signaling Softswitch, AS-SIP End Instruments
- Classified Video – LSC, Dual Signaling Softswitch, AS-SIP End Instruments, Multi-signaling MCU
- Multi-Function Mobile Devices – Multifunction Mobile Devices are a new top-level product that will include product subcategories such as smartphones. This product category will primarily consist of COTS products with added IA requirements. The aspects of the smartphone, which are related to UC WoIP functions are genetically defined as the "UC Smartphone Application". The requirements for non-UC WoIP-related aspects of the smartphone (such as e-mail or web-browsing) are generally defined by DISA Field Service Office STIGs. Classified Multi Media Device, SBU Multi Media Device NOTE: According to AFI 33-112 all commodity devices (i.e. Multi-Function Mobile Devices) must be purchased from the Information Commodity Council (ITCC).

1.1.4 APL Information

A list of products can be viewed at: https://aplits.disa.mil/processAPList.do

1.2 Cryptographic Module Validation Program

1.2.1 Purpose

The CMVP is a joint effort between NIST and the Communication Security Establishment Canada (CSEC) that validates cryptographic modules to FIPS 140-2. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. *If the agency specifies that the information or data be cryptographically protected*, then FIPS 140-2 is applicable. In essence, if cryptography is required, then it must be validated.

1.2.2 Authority

FIPS 140-2
Federal Information Security Management Act (FISMA) 2002
Committee on National Security Systems Policy (CNSSP) 15
Homeland Security Presidential Directive (HSPD) 12

1.2.3 Waivers

With the passage of FISMA 2002, there is no statutory provision to allow for agencies to waive FIPS compliance.

1.2.4 Types of Products required to come from the Cryptographic Module Program

Include, but not limited to:

- Cryptographic Software
- Telecommunication Devices
- Land Mobile Radios
- Routers/Switches
- VPN Devices
- Firewalls
- Disk Encryption
- Flash Drives

1.2.5 APL Information

A list of products can be viewed at: http://csrc.nist.gov/groups/STM/cmvp/validation.html

1.3 Common Criteria Evaluation & Validation Scheme

1.3.1 Purpose

The CCEVS is a products conformance to international standards developed under the National Information Assurance Partnership which is a joint effort established by NIST and the NSA. These standards are applicable for products not using cryptographic modules, or in other words, not CMVP applicable.

1.3.2 Authority

Committee on National Security Systems Policy (CNNSP) 11
Committee on National Security Systems Policy (CNSSP) 15

1.3.3 Waivers

Waivers were previously allowed under NSTISSP 11 but under CNSSP 11, they are not currently allowed and policy is still being determined.

1.3.4 Types of Products required to come from the Common Criteria Evaluation & Validation Scheme

Include, but are not limited to:

- VPN Gateways
- Enterprise Security Identity and Credential Management
- Servers
- Routers/Switches
- Database Management Systems (DBMS)
- Software
- Printers/Copiers
- Face/Palm Recognition Devices

1.3.5 APL Information

A list of products can be viewed at: https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm?&CFID=18276275&CFTOKEN=991e1edd298b35b7-3B35A089-E934-81AE-59FDD1F1C26A8D63

In addition, CCEVS also recognizes the certifications granted by other partners, therefore, the Common Criteria Portal can also be used: http://www.commoncriteriaportal.org/products/

1.4 Federal Identity, Credential and Access Management (FICAM)

1.4.1 Purpose

The FICAM testing program (formerly the NIST Personal Identity Verification Program) provides a comprehensive evaluation capability to support the selection and procurement of qualified products and services for the implementation of a federated and interoperable Identity, Credential & Access Management (ICAM) segment architecture. The objectives of the FICAM testing program are to provide compliance, consistency and alignment of commercially available products and services with the requirements and functional needs of government ICAM implementers as required by FIPS 201.

1.4.2 Authority

FIPS 201
Homeland Security Presidential Directive (HSPD) 12

1.4.3 Waivers

With the passage of FISMA 2002, there is no statutory provision to allow for agencies to waive FIPS compliance.

1.4.4 Types of Products required to come from the Federal Identity, Credential and Access Management (FICAM)

Include, but are not limited to:

- VPN Gateways
- Enterprise Security Identity and Credential Management
- Servers
- Routers/Switches
- Database Management Systems (DBMS)
- Software
- Printers/Copiers
- Face/Palm Recognition Devices
- Access Control Systems

1.4.5 APL Information

A list of products can be viewed at: http://www.idmanagement.gov/approved-products-list-apl

1.5 TEMPEST

1.5.1 Purpose

TEMPEST is a code word for emissions security and is not an acronym. TEMPEST centers around compromising emanations which are unintentional intelligence-bearing signals that, if intercepted, can disclose transmitted information. Systems that process classified information must use TEMPEST certified products which include monitors, keyboards, PCs and servers.

1.5.2 Authority

CNSS 300 National Policy on Control of Compromising Emanations (FOU)
DoD Directive C-5200.19 (FOUO)
NSTISSAM TEMPEST 2-95 (FOUO)

1.5.3 Waivers

DISA will allow for **some exceptions for VTC switching** from unclassified to classified under guidance provided at the following URL: http://www.disa.mil/Services/Network-Services/Video/DVS-G/Becoming-a-Customer. No other TEMPEST waivers are acceptable.

1.5.4 Types of Products required to come from the TEMPEST

Include, but are not limited to:

- Monitors
- Printers/Scanners/Fax
- Servers
- Switches

1.5.5 APL Information

A list of products can be viewed at: http://www.nsa.gov/applications/ia/tempest/index.cfm

1.6 High Assurance Internet Protocol Encryptor (HAIPE)

1.6.1 Purpose

A HAIPE device complies with the NSA’s HAIPE cryptography suite and can encrypt multicast data with a “preplaced key”. It provides a secure gateway that allows two enclaves to exchange data over an untrusted network. It is capable of protecting up to Top Secret transmissions. Any product with a HAIPE certification has undergone testing by the NSA.

1.6.2 Authority

Committee on National Security Systems Policy (CNNSP) 19
UC Framework 2013

1.6.3 Waivers

There is no waiver for this requirement, however, authorizing officials are granted leeway in working with vendors to ensure HAIPE-IS is met. Contact the NSA HAIPE program at haipe_po@nsa.gov.

1.6.4 Types of Products required to come from the HAIPE APL

Include, but are not limited to:

- Radios
- Various network encryption devices

1.6.5 APL Information

Most HAIPE products are available on the UC APL, however, if the product is absent from the UC APL, but the product has been issued a HAIPE-IS certificate from the NSA, a waiver can be sought for the product. Due to security reasons, the NSA will not publicly release an all-inclusive list.

2. Software purchases

IAW DFARS 208.7402 departments and agencies shall fulfill requirements for commercial software and related services, such as software maintenance, in accordance with the DoD Enterprise Software Initiative (ESI) (see website at <http://www.esi.mil/>) and in accordance with acquisition procedures at PGI 208.7403. In the event that the software required is not available to the customer through a DoD ESI source, the customer shall be authorized to obtain the software through this contract.

3. Technical Assistance

E-mail NETCENTS-2 CS at netcents@us.af.mil**,** if you have specific questions. Please ensure “NetCentric Products” is noted in the subject line for review and appropriate distribution.