

APL General

Do I need an APLITS account to view the APL?

No, the APL is publicly accessible at <https://aplits.disa.mil/processAPList.do>

How do I acquire additional information about a solution on the APL?

Please contact the UCCO at disa.meade.ns.list.unified-capabilities-certification-office@mail.mil with the Tracking Number and description of the product you are requesting information for. Note that only government civilian and/or uniformed military personnel may receive the Information Assurance Assessment Package (IAAP).

Why can't I find the type of device I need?

The scope of the UC APL is determined by the Unified Capabilities Requirements (UCR) which can be found at <http://www.disa.mil/Network-Services/UCCO/Policies-and-Procedures>. Solutions which do not fall into an applicable category are not eligible for listing on the UC APL.

Where are software, programs, etc. listed on the UC APL for my military/government laptop?

These are not applicable categories for the UC APL. Please follow guidance by your local Certify Authority and / or Designated Accrediting Authority.

Where can I find a list of approved KVMs?

NIAP has a list of compliant KVM (Peripheral) Switches that are located at the NIAP page below: https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm Select "Peripheral Switch" and a list of compliant products will be displayed.

Where can I find a list of approved Red/Black Peripheral products?

http://disa.mil/services/network-services/video/~media/files/disa/services/dvs/red_black_peripherals.xls

Equipment not on the list maybe added through one of the following methods:

- 1) Successful evaluation by an NSA Certified Tempest Lab and providing Certification Letter to DVS
- 2) Evaluation by the DISA Certified Tempest Technical Authority (CTTA). Send equipment and completed Assessment Request Form to: DISA NS5- For shipping instructions, contact: dvsdap@disa.mil Commercial (703) 882-0839, DSN (312) 381-0839

What are the steps I need to follow for submitting a product for UC APL testing?

Please refer to the UC APL Process Guide at http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/APL-Process/UCAPL_Process.pdf

SPONSORSHIP

How do I know if a product has been removed from the UC APL? Products approved for use on the DoD networks are available at <https://aplits.disa.mil/processAPList.do>. If a product has expired and is no longer listed on the UC APL, a list of removed products can be viewed on the Approved Products List Removal page at <http://www.disa.mil/Network-Services/UCCO/APL-Removal-List>.

Can I purchase a product that has been removed from APL? No. Only products currently listed on the APL can be purchased in accordance with the DoDI 8100.3. Products that have been removed from the APL are eligible for obtaining an Authority to Connect (ATC).

<http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Approval>

Can I connect to the DSN prior to receiving approval to connect (ATC)? No. You must receive approval from the DSN Connection Approval Office prior to connecting to the DSN. You need to request connection approval by filling out the JIC submittal form.

Connection Approval Office: (301) 225-2900 | (301) 225-2901

DSN 312-375-2900 | DSN 312-375-2901

disa.meade.ns.mxb.ucao@mail.mil (NIPR)

disa.meade.ns.mxb.ucao@mail.smil.mil

Who can sponsor a product for testing? Any DoD Component user of the DISN with acquisition or management-level responsibilities of equipment can sponsor a product for testing.

If my product is already Interoperability certified, do I need a sponsor for Information Assurance Testing? Yes. Even if a product is currently Interoperability certified, effective on Jan. 16, 2004 with the signing of the DoDI 8100.3, any testing performed requires a test sponsor.

What role does the sponsor play in the testing process? The sponsor will be responsible for working with a vendor to get the test submittal application completed and submitted to the UCCO. The sponsor will also be involved in the testing process as far as being notified of any problems that occur during testing. In the case of a negative test report, it is the sponsor's decision whether or not an appeal is made up to the Military Communications-Electronics Board (MCEB) if the case is for Interoperability, or to the DISN Designated Approving Authority (DAA) in the case of Information Assurance.

Why do I need a sponsor for my product to be tested? The requirement for a sponsor was established for the first time in the DoDI 8100.3. With the signing of the DoDI, it became a violation of Department of Defense Policy for either Interoperability or Information Assurance testing to occur without the product having a government sponsor.

STIG COMPLIANCE

How do I know what STIGs to apply to my products? It is up to the vendor to work with the sponsor to examine all components of the solution desired to be tested, and compare against the list of available STIGs to see which apply and which do not. It is strongly advised that any applicable STIGs that are available for any components of your solution be applied prior to applying for testing. Non-compliance with available STIGs will result in increased vulnerabilities discovered and reported at the end of testing.

Where can I access the latest STIGs? The latest STIGs are available at

<http://iase.disa.mil/stigs/Pages/index.aspx>

What if applying every item of the STIG breaks my product? In the case of certain items within a STIG rendering a device inoperable try to pinpoint exactly which item of the STIG is causing the problem. You then have two choices; you can either try to make changes to your product so that it will work with that item in the STIG, or you can document a mitigation procedure for that item and submit to the IA test team with your product prior to testing. In the case of the latter, the vulnerability and mitigation will be reflected in the final report of the product.

AUXILIARY COMPONENTS

What is an auxiliary component? Some larger solutions submitted for testing rely on sub-devices to operate properly. For example, a VoIP solution submitted may require a network management server, firewall, etc., to be operational in a secure manner to complete certification. Any additional devices outside of the main solution need to be described in the auxiliary components section.

What if I have more than one auxiliary component? If there are multiple auxiliary components, please list the specifications for the additional ones in the General Information Section in box 9 d, Technical Specifications.

COMMON CRITERIA CERTIFICATION

What is common criteria certification? Common criteria certification is a standard that came into effect on July 1, 2002 with the passing of the NSTISSP #11. It mandated that departments and agencies within the Executive Branch, for use on National Security Systems, only acquire IA and IA-enabled information technology products that are certified as meeting common criteria security standards. In an effort to not repeat testing, for device types that common criteria certified devices exist such as firewalls and operating systems we prefer that common criteria certified devices are used. It is strongly recommended for a solution to use common criteria certified components when they are available. For more information, go to <http://iase.disa.mil/common>.

How do I know if a product is common criteria certified? The list of common criteria certified products go to <http://www.commoncriteriaportal.org/products.html> . For a list of products currently undergoing testing for common criteria certification, go to https://www.niap-ccevs.org/CCEVS_Products/in_eval.cfm.

FIPS

What is FIPS? FIPS stands for Federal Information Processing Standard. FIPS are the standards and guidelines for information processing developed by NIST and approved by the Secretary of Commerce as requirements for the federal government for information assurance and interoperability. For more information on FIPS please refer to <http://www.itl.nist.gov/fipspubs/index.htm>.

What does FIPS have to do with the testing of my product? If your product performs any type of encryption of data, it is required that the encryption method being used meet FIPS standards for both information assurance and interoperability testing. For more information on FIPS, go to <http://www.itl.nist.gov/fipspubs/by-num.htm>.