# Frequently Asked Questions

## Sponsorship

**• "Who can sponsor a product for testing?"**

*Answer: Any DoD Component user of the DSN with acquisition or management level responsibilities of DSN equipment can sponsor a product for testing at JITC.*

**• "If my product is already Interoperability Certified do I need a sponsor for Information Assurance Testing?"**

*Answer: Yes. Even if a product is currently Interoperability certified, effective on January 16, 2004 with the signing of the DODI 8100.3 any testing performed at JITC requires a test sponsor.*

**• "What role does the sponsor play in the testing process?"**

*Answer: 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?"**

*Answer: 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 at JITC without the product having a government sponsor.*

## STIG Compliance

**• "How do I know what STIGs to apply to my products?"**

*Answer: 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 STIG's to see which apply and which do not. It is strongly advised that any applicable STIG's that are available for any components of your solution be applied prior to applying for testing. Non-compliance with available STIG's will result in increased vulnerabilities discovered and reported at the end of testing.*

**• “Where can I get the latest STIGs from?”**

*Answer: The latest STIG's are available from a .mil or .gov source at the following link: http://iase.disa.mil/stigs/stig/index.html*

**• “How can I get the STIG's if I'm not a .mil or .gov?”**

*Answer: Vendors that are attempting to get the STIG's from a non .mil or .gov source should either work through their sponsors to get the desired documents or contact the FSO Support Desk at DSN 570-9264, commercial (717) 267-9264 or email to fso_spt@ritchie.disa.mil*

**• “How can I get the Security Readiness Review (SRR) scripts to test my product for STIG compliance?”**

*Answer: The latest SRR Scripts are available from a .mil or .gov source at the following link: http://guides.ritchie.disa.mil*

*Vendors attempting to get the SRR scripts from a non .mil or .gov source should either work through their sponsors to get the desired documents or contact the FSO Support Desk at DSN 570-9264, commercial (717) 267-9264 or email fso_spt@ritchie.disa.mil . Please note that the SRR scripts are unlicensed tools developed by the Field Security Office (FSO) and use of these on products are completely at users own risk.*

**• “What STIG's have SRR scripts?”**

*Answer: SRR Scripts are available for all Operating Systems that have STIG's. Also, all databases that have STIG's also have SRR Scripts. There is a SRR available for webservers using IIS as well.*

**• “What if applying every item of the STIG breaks my product?”**

*Answer: In the case of certain items within a STIG rendering a device inoperable try to pin point exactly which item of the STIG is causing the problem. Then have two choices, can either try to make changes to your product so that it will work with that item in the STIG or 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?”**

*Answer: 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?"**

*Answer: 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?"**

*Answer: 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 please refer to the following link: http://niap.nist.gov/cc-scheme/*

**• "What is EAL?"**

*Answer: EAL is the rating system that is used within Common Criteria certification. Products are certified as different EAL levels depending on the robustness of the devices security. For more information please refer to the following link: http://niap.nist.gov/cc-scheme/*

**• "How do I know if a product is Common Criteria certified?"**

*Answer: The list of Common Criteria certified products can be found at the following link: http://niap.nist.gov/cc-scheme/vpl_type.html*

*For a list of products currently undergoing testing for Common Criteria certification please view the following link: http://niap.nist.gov/cc-scheme/in_evaluation.html*

## FIPS

**• "What is FIPS?"**

*Answer: 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 the following link: http://www.itl.nist.gov/fipspubs/index.htm*

**• "What does FIPS have to do with the testing of my product?"**

*Answer: 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 please refer to the following link: http://www.itl.nist.gov/fipspubs/index.htm*

## APL

**• "How do I know if a product is on the Approved Product List (APL) or has been removed ?"**

*Answer: Products approved for use on the DoD networks are available at the following site: http://jitc.fhu.disa.mil/apl/*

*A list of those products that have been removed is available at http://www.disa.mil/gs/dsn/jic/apl_removal.html*

**• "Can I purchase a product that has been removed from APL ?"**

*Answer: No. Only products currently on the APL can be purchased IAW DoDI 8100.3. Products that have been removed from the APL are eligible for obtaining an Authority to Connect (ATC).*

• ***Can I connect to the DSN prior to receiving approval to connect (ATC)?***

*Answer: No. You must received approval from the DSN Unified Capabilities Connection Office prior to connecting to the DSN. You need to request connection approval by using the following URL: http://www.disa.mil/gs/dsn/jic/atcsubmittal.html*