

APL How to Guide for Vendors and Sponsors

The process from beginning to end encompasses a multitude of steps; the following depicts the normal process flow that can be expected when submitting for testing.

This document is meant to be a step-by-step guide that complements the UC APL Process Brief found here <http://disa.mil/ucco/index.html>

Preparation:

What to do first before you submit:

- **Verify that the product is not already on the DoD Unified Capabilities (UC) Approved (APL) (see <http://jitc.fhu.disa.mil/tssi/apl.html>), or that it is not already scheduled for testing at JITC (see <http://jitc.fhu.disa.mil/tssi/schedule.html>).**
- **Identify a DoD sponsor for the product. Ask them if they will sponsor your product.** Recommendation: Normally a senior enlisted, CWO, O3 through O5, GS12 through GS14 are our best options for sponsors – sometimes a GS11 or Junior Enlisted military personnel or lower might be hesitant to make decisions.
- **Prepare a topology diagram of the system to be tested (this must be provided later). Verify with the sponsor that your product meets their requirements.**

Please use the links below to assist you with becoming familiar with the process:
<http://disa.mil/ucco/index.html>

To see what products are currently scheduled, see:
<http://jitc.fhu.disa.mil/tssi/schedule.html>

To submit a product for testing, see:
http://www.disa.mil/ucco/apl_submission.html

To submit for retest, updates or adjustments, see:
http://www.disa.mil/ucco/apl_update.html

Process:

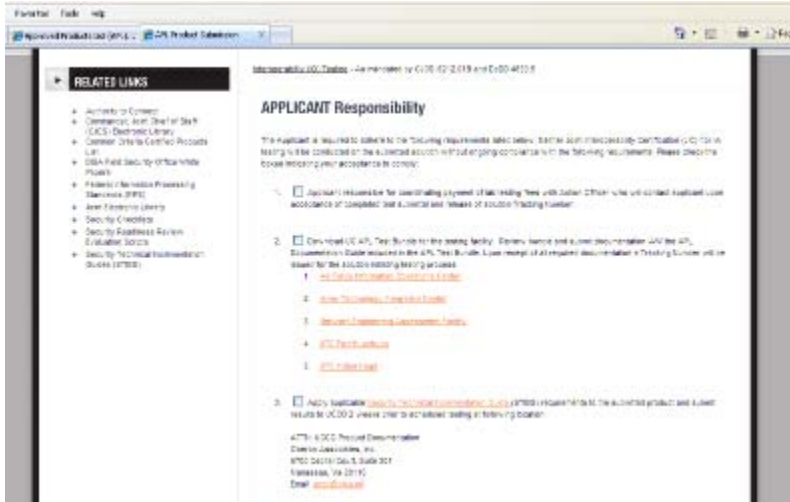
1. To begin the process start here. (<http://www.disa.mil/ucco/index.html>)
This is what you should see.



Screenshot 1: Submitting a Product for APL Testing

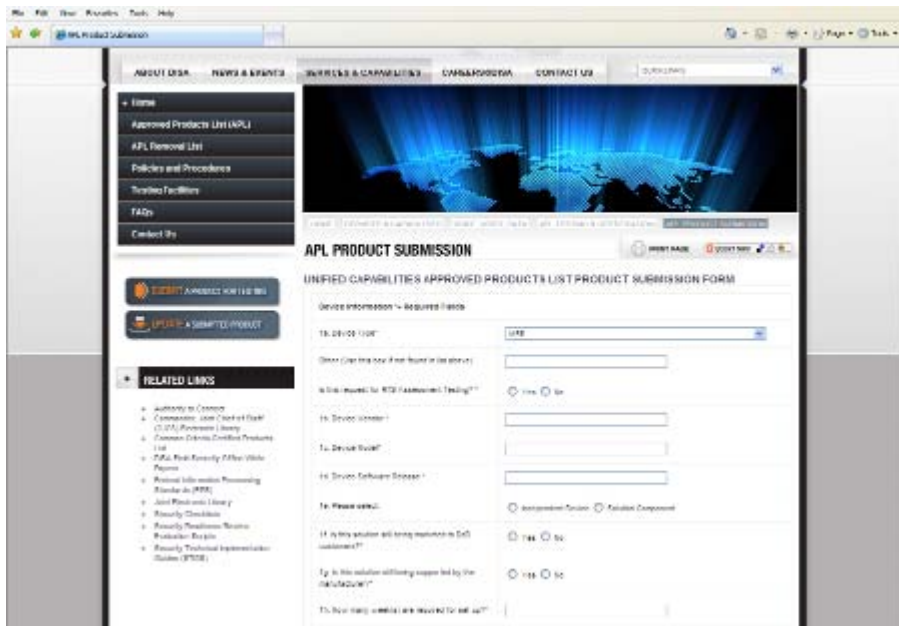
2. The most important section is “Applicant Responsibility”. Ensure that you understand all the requirements, prior to submitting the “Applicant Responsibility” form.
 - o Ensure that the appropriate UC APL Test Bundle has been downloaded from the web page representing the testing center your solution will go to.
 - a) Air Force Information Operations Center (AFIOC)
http://www.disa.mil/ucco/testing_facilities/afioc.html
 - b) Army Technology Integration Center (TIC)
http://www.disa.mil/ucco/testing_facilities/tic.html
 - c) Network Engineering Assessment Facility (NEAF)
http://www.disa.mil/ucco/testing_facilities/neaf.html
 - d) JITC Fort Huachuca
http://www.disa.mil/ucco/testing_facilities/jitc_hua.html
 - e) JITC Indian Head
http://www.disa.mil/ucco/testing_facilities/jitc_indian.html
 - o Check the five boxes to indicate your acceptance to comply.
 - o Type your email address in the “Email Address” field.
 - o Click the “I Agree” button.

APL How To Guide For Vendors / Sponsors



Screenshot 2: Applicant Responsibility

3. After submitting the “Applicant Responsibility” Form the user will be directed to the “APL Product Submission” Page. Here you will be asked a series of questions about your product. Fill in all the applicable questions. Required items are indicated with an “*”. When you have filled out the form in its entirety click the “Submit Test Form” Button. If you need assistance while filling out the form click on the hyperlinks labeled “Frequently Asked Questions”.



Screenshot 3: Product Submission Page

** Once you click “Submit Test Form” if any required blocks remain blank you will receive an error message indicating which blocks were missed. If your submittal is successful you will be redirected to a screen indicating that your form has been received and details as to what comes next in the APL submission process.

APL How To Guide For Vendors / Sponsors

4. Scrutinize the STIG questionnaire. This will assist you in your preparation for testing. [For Examples of the STIG web pages click here](#) The specific STIGS that will need to be applied to your solution will be identified at the Initial Contact Meeting (ICM).
5. Start your Self Assessment Report (**SAR**) process. You will need to provide this after submission. *A template for completing the SAR can be found in the APL Test Bundle you downloaded in step 2.*
6. Provide requested documents when contacted by the Unified Capabilities Certification Office (**UCCO**) by email. The email will have “Request for Documentation” as a subject line.
7. The sponsor will then receive an email requesting that they verify;
 - They are indeed the sponsor
 - The proposed solution diagram is a true representation of how the product will be deployed into their network/infrastructure (boundaries).
8. The sponsor will then verify themselves as such and verify all items on your proposal.
9. An Initial Contact Meeting (**ICM**) is conducted. The Information Assurance Test Team will contact sponsor and vendor with time and date of ICM. During the ICM, the following will be identified:
 - All applicable STIGs will be identified
 - Corporative Research and Development Agreement (**CRADA**)/Fee arrangements
 - Scheduled Information Assurance (**IA**) and Interoperability (**IO**) Test Dates
 - Tentatively schedule Outbrief date
 - Describe the System Under Test (**SUT**) configuration
 - Any action items to be completed by the vendor and/or sponsor

The ICM can be canceled if the sponsor and/or alternate sponsor is not available for the scheduled conference call. After 3 unsuccessful attempts to hold the ICM, the product/solution will be retired.
10. SAR mitigation strategy and all outstanding action items (identified during the ICM) are due to the UCCO **NLT** 2 weeks prior to scheduled test date. Prior to SAR due date the UCCO will send out warning notices to the vendor and sponsor indicating the SAR has not been received. When submitting for Real Time Service (RTS) the SAR is due at the time of submission.
11. The UCCO will send a request to sponsor on whether to proceed with test or not. This is determined from the results of documentation provided but is the ultimately the sponsor’s decision to move forward with testing.
12. Two weeks prior to beginning IA testing, a vendor engineer will arrive at the testing facility for equipment setup. The engineer will remain at the testing facility throughout IA and IO.

APL How To Guide For Vendors / Sponsors

Any anomalies discovered during testing, the engineer is **highly encouraged** to fix on-site (**FOS**) all issues if possible, otherwise testing is cancelled.

13. IA Testing is performed consisting of:
 - Phase I: STIG Testing
 - Phase II: IP Penetration and Telephony Testing (only if required)
14. After IA testing is complete, an Out Brief is conducted to discuss/clarify mitigations and any outstanding action items.
15. UCCO makes official CA Recommendation Request to FSO.
16. The solution is briefed to the DSAWG board to either approve or disapprove connection to DISN.
17. IO Testing is performed (**only if IA testing is completed successfully**)
18. Your solution is recommended to be presented to Joint Staff (**JS**) (**only if IO testing is completed successfully**).
19. Official posting on the DoD UC APL will begin once your solution/product has achieved both IA, IO certification and the UCCO have received the vendor's configuration guide (CG). The CG details tweaks made during IA testing which is needed for out-of-box setup procedures to be used in the field at installation time.
20. More information may be obtained by reviewing the "UC APL Process Brief".
<http://disa.mil/ucco/index.html>

If you have a question or would like additional clarification, please feel free to contact UCCO at your convenience.

UCCO Process Manager
DSN: (312) 381-0762
COM: (703) 882-0762

UCCO Process Questions:
DSN: (312) 879-3234
COM: (520) 538-3234

E-Mail: UCCO@disa.mil

Additional Resources:

Download the STIGs and other applicable documentation and save them on your workstation. Below are links and screen shots for required documentation.

a) Security Technical Implementation Guides (STIGs)

<http://iase.disa.mil/stigs/stig/index.html>



b) Security Checklists <http://iase.disa.mil/stigs/checklist/index.html>



APL How To Guide For Vendors / Sponsors

c) Security Readiness Review Evaluation Scripts (SRRs)

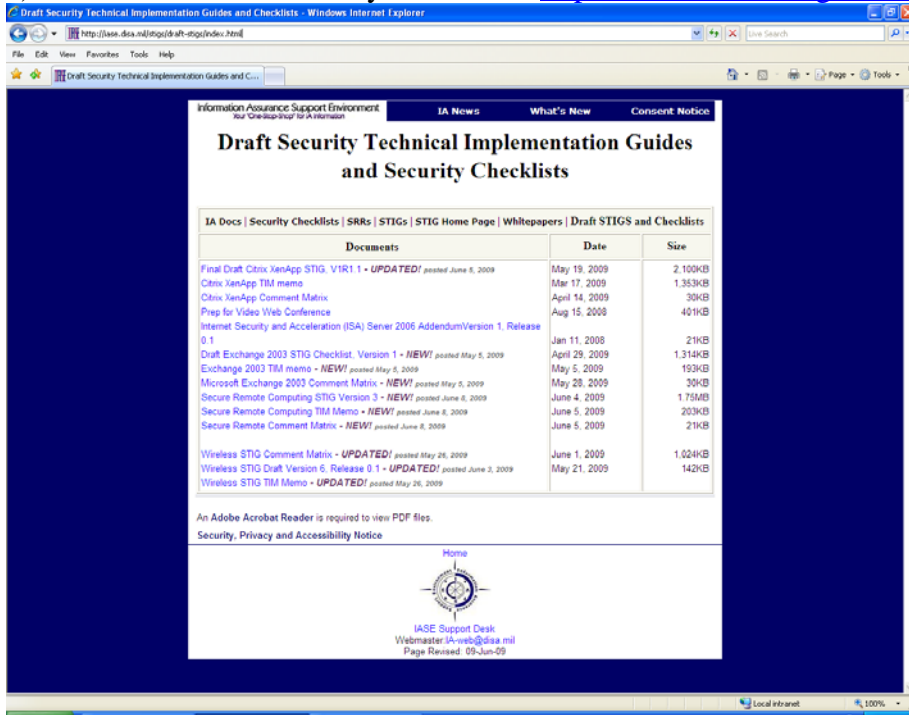
<http://iase.disa.mil/stigs/SRR/index.html>

Documents	Date	Size
Database Oracle Default Password Script	Feb 16, 2006	75KB
Oracle Unix Listener Password Check	Oct 30, 2005	6KB
Database Oracle SRR - UNIX gz format - <i>Updated!</i> posted April 20, 2009	April 3, 2009	51KB
Database Oracle SRR - UNIX tar format - <i>Updated!</i> posted April 20, 2009	April 3, 2009	530KB
Database Oracle SRR - Compressed format - <i>Updated!</i> posted April 20, 2009	April 3, 2009	154KB
Database Oracle SRR - Windows zip format - <i>Updated!</i> posted April 20, 2009	April 3, 2009	104KB
Database SQL Server Scripts	Jan 15, 2008	575KB
Open VMS SRR	Jan 28, 2005	23KB
zOS SRR Scripts - <i>Updated!</i> posted April 20, 2009	April 17, 2009	2,346KB
Tandem SRR	Dec 12, 2003	474KB
UNIX SRR - <i>Updated!</i> posted April 20, 2009	April 16, 2009	various
Files needed for Windows IT Manual SRR	Dec 2003	188KB
Files needed for Windows Vista Manual SRR	Jan 08, 2009	194KB
Files needed for Windows XP Manual SRR	Nov 2007	192KB
Files needed for Windows 2008 Manual SRR	Jan 08, 2009	194KB
Files needed for Windows 2003 Manual SRR	Nov 2007	199KB
Files needed for Windows 2000 Manual SRR - <i>Updated!</i> posted March 3, 2009	Mar 2009	199KB
Web UNIX SRR - UNIX gz format -	Jul 2007	40KB
MDS hash for Web UNIX SRR	Jul 2007	1KB

d) DISA FSO White Papers <http://iase.disa.mil/stigs/whitepaper/index.html>

Documents	Date	Size
Web Server Content Access Control White Paper Version 1 (posted Sept 22, 2006)	Mar 25, 2005	482KB
Windows Messenger Whitepaper	Feb 16, 2005	1,193KB
Security Review Methodology	Jan 15, 2005	294KB
Unencrypted File Transfer Protocol (FTP) and Telnet	Aug 30, 2004	183KB
Microsoft Windows XP Service Pack 2 Default Security Features	Aug 2, 2004	77KB
White Paper on Residual Risk in DoD Accreditation	Jun 1, 2004	64KB
Determining the Appropriate Evaluation Assurance Level for COTS IA and IA-Enabled Products	Mar 15, 2004	170KB
IEEE 802.1x Port-Based Network Access Control in the DoD Environment Primer	Sep 4, 2003	62KB
Article on Microsoft NT De-Support		22KB
Sudo White Paper Report	April 19, 2004	257KB
Storage Area Networks (SAN) Security Analysis	Sep 5, 2003	291KB
OpenSSH for Solaris	Aug 26, 2003	263KB
OpenSSH for Windows	Dec 30, 2002	352KB
VMware Workstation 3.2 for Windows White Paper	Aug 4, 2003	137KB
White Paper - WEBSPECT	Nov 1, 2002	41KB
Bantu White Paper	Dec 13, 2002	395KB
Grease Networks	Dec 2, 2002	201KB
Openet Ace	Dec 2, 2002	174KB
Default Password Policy	Apr 18, 2003	151KB

e) Draft STIGs and Security Checklists <http://iase.disa.mil/stigs/draft-stigs/index.html>



f) Common Control Identifier <http://iase.disa.mil/cc/index.html>

