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

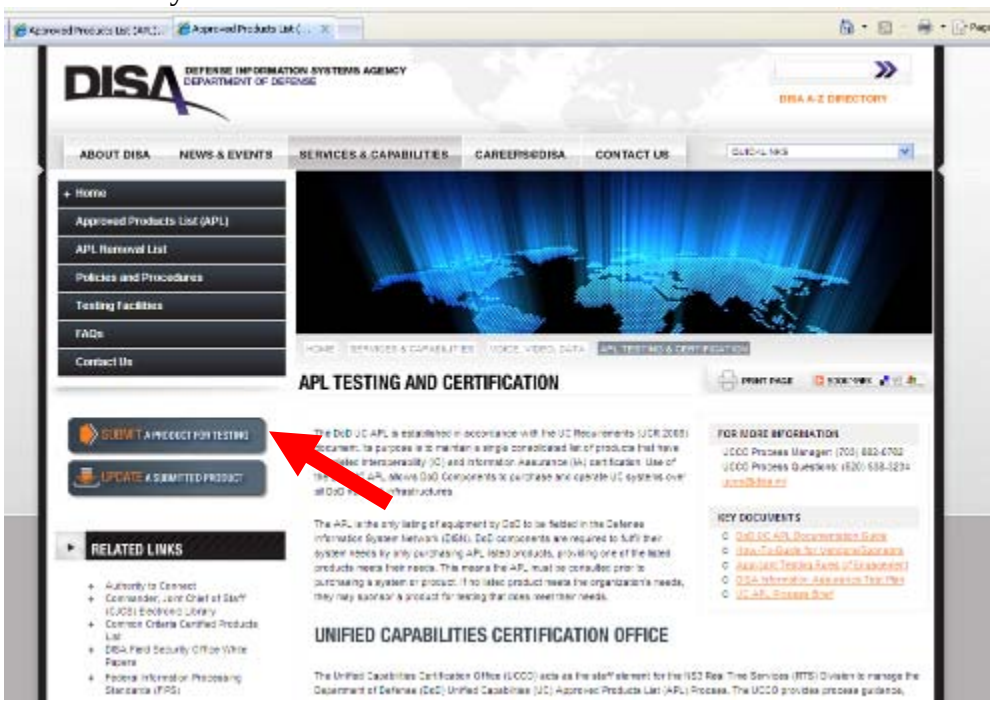
  To see what products are currently scheduled, see:
  http://jitc.fhu.disa.mil/tssi/schedule.html

  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

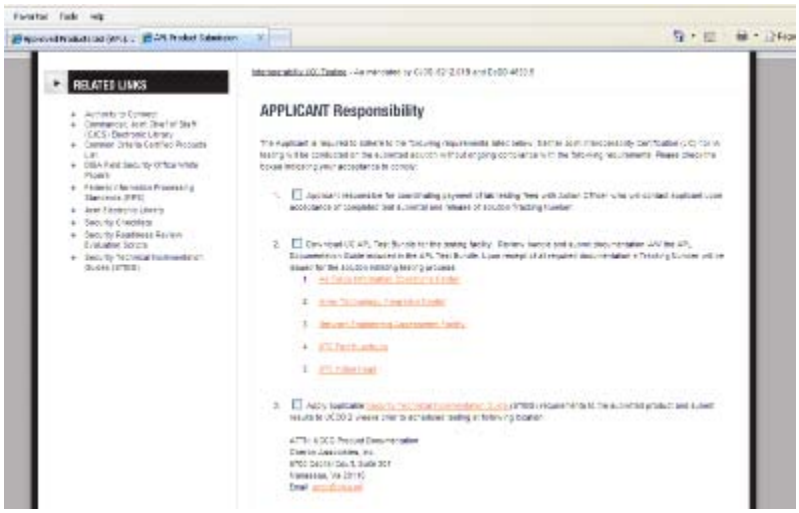
2. The most important section is "Applicant Responsibility". Ensure that you understand all the requirements, prior to submitting the "Applicant Responsibility" form.
    - Ensure that the appropriate UC APL Test Bundle has been downloaded from the web page representing the testing center your solution 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

    - Check the five boxes to indicate your acceptance to comply.

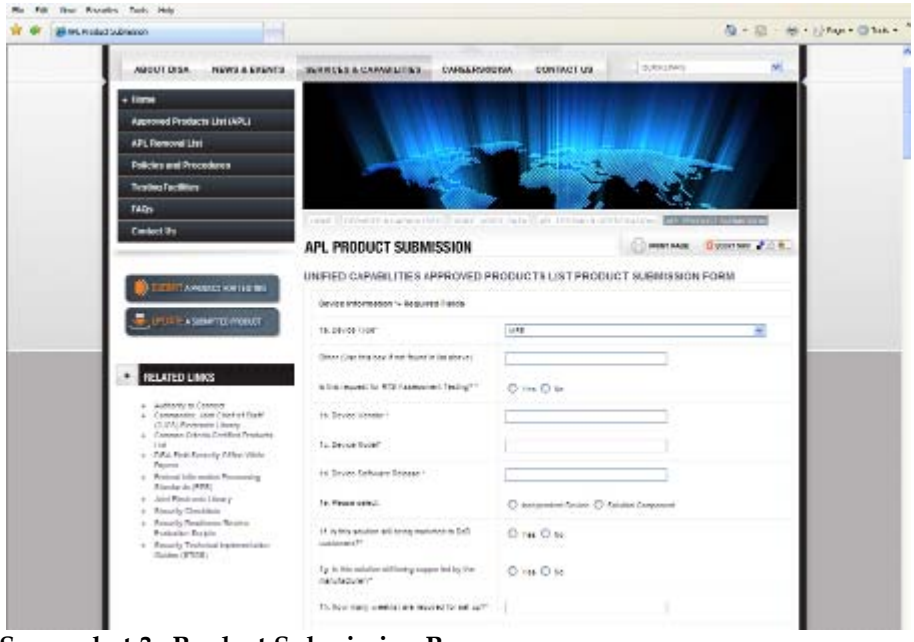
    - Type your email address in the "Email Address" field.

    - Click the "I Agree" button.



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.

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.

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

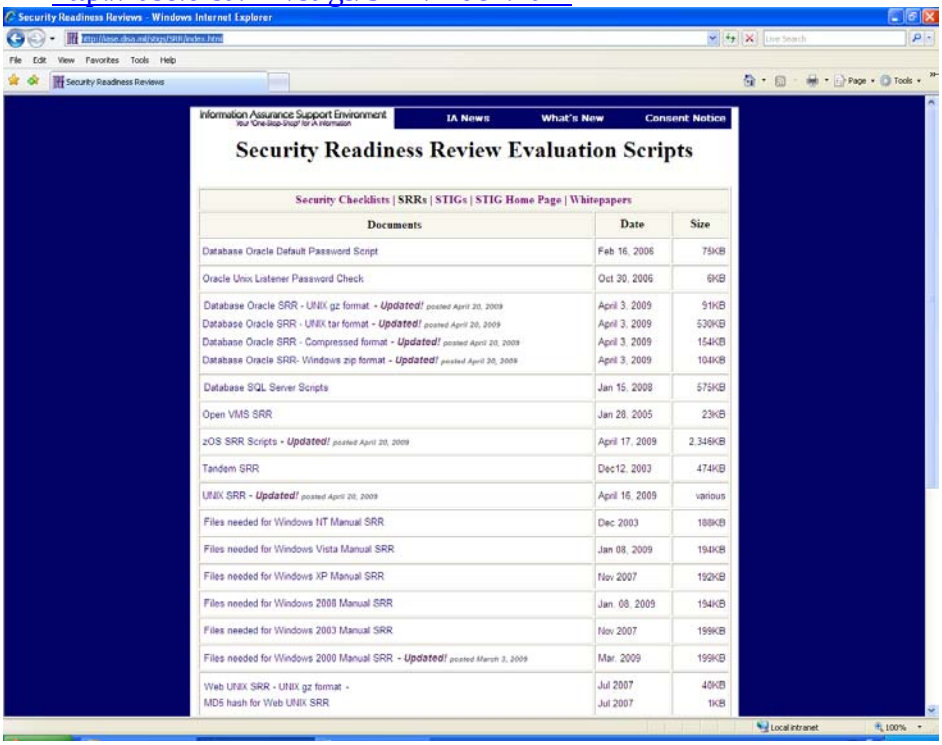
Additional Resources:

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

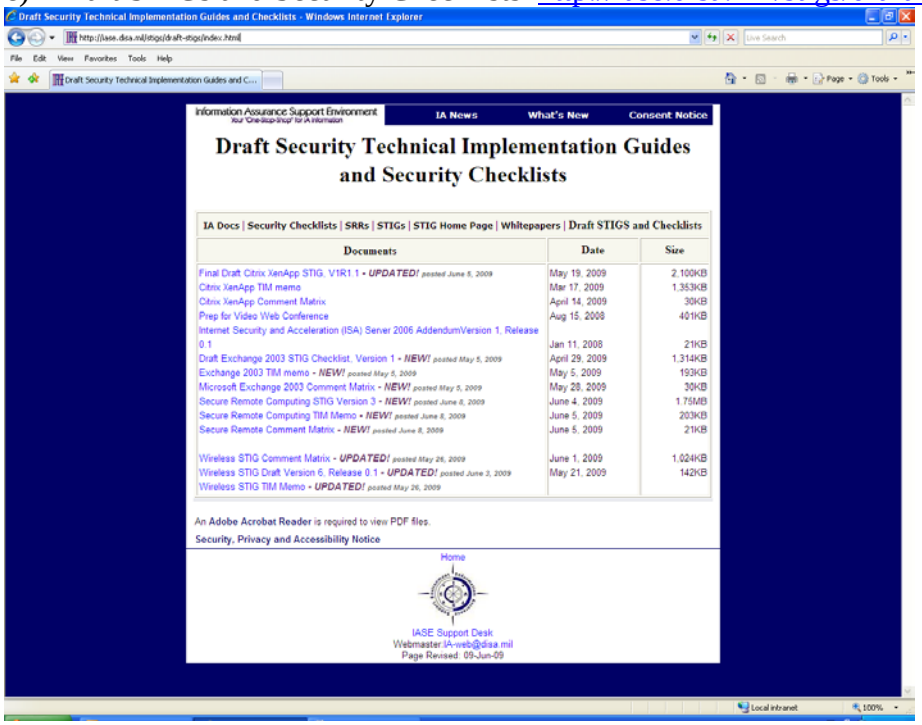
b) Security Checklists http://iase.disa.mil/stigs/checklist/index.html

c) Security Readiness Review Evaluation Scripts (SRRs)
http://iase.disa.mil/stigs/SRR/index.html



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

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



f) Common Control Identifier http://iase.disa.mil/cci/index.html