



Defense Information Systems Agency  
**A Combat Support Agency**

**NETWORK SERVICES DIRECTORATE (NS)**  
**DISN & GSM PROGRAM MANAGEMENT OFFICE**  
**(NSP)**

**UNIFIED CAPABILITIES  
APPROVED PRODUCTS LIST  
(UC APL) PROCESS GUIDE**

Version 2.0  
December 2012

Defense Information Systems Agency  
DISN Program Office (NSP)  
[www.disa.mil/ucco](http://www.disa.mil/ucco)

## **EXECUTIVE SUMMARY**

This DISA Unified Capabilities Approved Products List Process Guide for Sponsors, Vendors, and Testing Facilities implements the requirement in Department of Defense Instruction (DoDI) 8100.04, Unified Capabilities, 9 December 2010, and CJCSI 6211.02D , Defense Information Systems Network (DISN) Responsibilities, 24 January 2012, that Director, Defense Information Systems Agency (DISA), establish, manage, maintain, and promulgate the DoD UC APL and the customer process guide describing steps that must be followed for a product to be listed on the DoD UC APL.

This UC APL Process Guide:

Updates and cancels the previous DoD UC APL Process Guide, Version 1.5, dated May 2010.

This guide is approved for public release and is available on the Internet from the DISA website at <http://www.disa.mil/ucco>

The instructions in this guide are effective immediately.

**SIGNATURE PAGE**

The undersigned agrees with the Unified Capabilities Approved Products List (UC APL) Process for products defined in this document.

**Approval:**

\_\_\_\_\_  
Jessie Showers  
Chief, DISN & GSM Program Management Office

\_\_\_\_\_  
Date

### REVISION HISTORY

This document will be reviewed and updated as needed. Critical and Substantive changes will be reflected in the revision history table.

Version	Date	Comments
2.0	Dec 2012	Baseline document.

## Table of Contents

SECTION 1. INTRODUCTION .....	1
1.1 Overview .....	1
1.2 PURPOSE .....	1
SECTION 2. ROLES AND RESPONSIBILITIES .....	1
2.1 Unified Capabilities Certification Office (UCCO) .....	1
2.2 Sponsors for UC APL Certification .....	1
2.3 Equipment Vendors .....	2
2.4 Testing Labs .....	3
2.5 Joint Interoperability Testing Command (JITC) .....	3
SECTION 3. STANDARD OPERATING PROCESS.....	4
3.1 UC APL Process Rules and Guiding Principles.....	4
3.2 Update / Changes to Current System Under Test (SUT) .....	9
3.3 Desktop Review (DTR) Process .....	10
3.4 UC APL Fast Track Process.....	11
APPENDIX A ACRONYMS .....	A-1
APPENDIX B REFERENCES .....	B-1
APPENDIX C DOCUMENTATION GUIDE .....	C-1
APPENDIX D MITIGATIONS, POA&MS AND COMMENTS GUIDANCE .....	D-1
APPENDIX E JITC FFS ROE.....	E-1
APPENDIX F 18 MONTH RULE .....	F-1
APPENDIX G UC APL PROCESS CHARTS.....	G-1

## 1 INTRODUCTION

### 1.1 Overview

The Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) Process is developed in accordance with DoD Instruction 8100.04. The UC APL Process is managed by Defense Information Systems Agency (DISA) – Network Services (NS) Unified Capabilities Certification Office (UCCO) under the DISN Program Office (NSP). The UC APL is to be the single approving authority for all Military Departments (MILDEPs) and DoD agencies in the acquisition of communications equipment that is to be connected to the Defense Information Systems Network (DISN) as defined by the Unified Capabilities Requirements (UCR). In accordance with CJCSI 6211.02D, DEFENSE INFORMATION SYSTEMS NETWORK (DISN) RESPONSIBILITIES, 24 January 2012, ENCLOSURE B. POLICY. Para 1.c. (4): “CC/S/As shall procure or operate UC products listed on the DOD UC Approved Products List (APL), as applicable, unless granted an exception to policy IAW DODI 8100.04.” The UC APL Process provides for an increased level of confidence through Information Assurance (IA) and Interoperability (IO) Certification.

### 1.2 Purpose

This document defines the process for getting UC products onto the UC APL and defines the roles and responsibilities for participants within the UC APL process.

## 2 ROLES AND RESPONSIBILITIES

### 2.1 Unified Capabilities Certification Office (UCCO)

The UCCO acts as the staff element for DISA NSP to manage the UC APL. The UCCO provides process guidance, coordination, information, and support to government sponsors and vendors throughout the entire process, from the registration phase to the attainment of DoD UC APL status. In addition, the UCCO manages the UC APL Removal List which consists of products that have been removed from the UC APL. In the DoD distributed testing environment the UCCO is the primary point of contact for scheduling and coordination of partnering test labs.

### 2.2 Sponsors for UC APL Product Certification

Main sponsor responsibilities for UC APL Certification are as follows:

- Assist DISA with developing requirements for the desired product and product features.
- Ensure acquisition of UC products aligns with DoD policy and direction.
- Attend the Initial Contact Meetings (ICM)
- Attend the IA and IO Out-Briefs to discuss test results and assist with vendor mitigation strategies (if applicable) and Plan of Actions and Milestones (POA&Ms) in accordance with the guidance provided in this process.
- Coordinate all testing activities and logistics with UCCO and vendors.
- Provide to the vendor the Security Technical Implementation Guides (STIGS) and Security Readiness Review (SRR) checklists that are Public Key Infrastructure (PKI)-restricted

- Coordinate with DoD test facility for funding (sponsor or vendor).
- Attend Test Discrepancy Report (TDR) Adjudication meetings.

### **2.3 Vendors**

Main vendor responsibilities for UC APL Certification are as follows:

- Download and review DoD UC APL Documentation Guide (Appendix C)
- Submit documentation in accordance with the UC APL Documentation Guide.
- Coordinate with DoD test facility for funding (See Appendix E)
- Apply applicable STIG requirements to the submitted product and submit results to UCCO as directed in Section 3.
- Ensure on-site engineering support is provided during all phases of UC APL testing assigned for the System Under Test (SUT).
- Attend the ICM and Out-Briefs to discuss test results.
- Provide Deployment Guidelines for SUT to UCCO.
- Coordinate all testing activities and logistics with UCCO, government sponsors and test facility.
- Assist testing centers in development of test plans and test procedures.
- Provide IA and IO Plan of Actions and Milestones (POA&Ms) within specified timeframes.
- Provide product and management descriptions which will serve as input to the Information Assurance Assessment Report (IAAR).

### **2.4 Testing Labs**

Main testing lab's responsibilities for the UC APL process are as follows:

- Attend UC APL scheduling meetings to provide IA and IO testing dates for products that have been assigned for testing.
- Assign an Action Officer (AO) to be the primary testing point of contact for a given tracking number.
- Coordinate with DISA NS on cost model (FFS or equipment CRADA) that will be applied to vendor product.
- Generate cost estimate and submit to vendor (or sponsor) if product falls under FFS cost model.
- Schedule and attend ICM and Out-Brief Meetings.
- Work with the product engineers onsite during setup and testing of SUTs.
- Disseminate ICM minutes, SAR Template, IA Findings Summary Report, IA Assessment Report (IAAR), and IO Certification Summary in the approved formats and timelines as specified in this document.
- Develop Test Discrepancy Reports (TDRs) for UC requirements that the SUT does not meet.
- Coordinate with JITC AO on TDRs.
- Attend TDR adjudication meetings.
- Develop Test Summary Report within specified guidelines.
- Provide JITC with Interoperability Test Certification recommendations.

- Provide JITC AO with DTR approval recommendation.
- Coordinate with JITC on DTR extension memorandum updates.
- Develop UC Implementation Guide based on their unique business models.
- Review IAAR reports for quality assurance prior to uploading into APLITS.

## 2.5 JITC

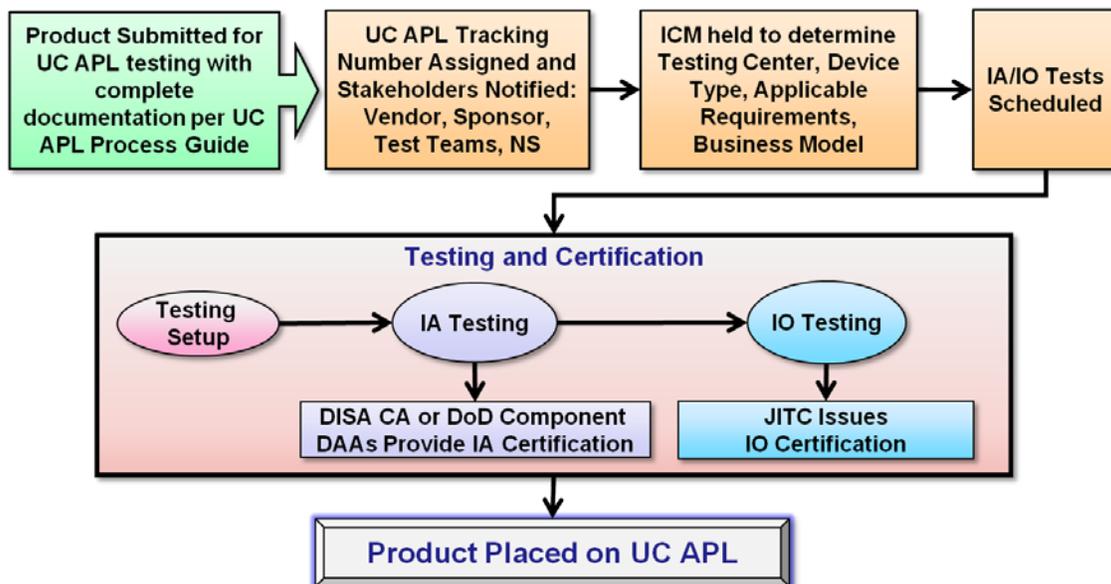
Above and beyond its test lab responsibilities, the JITC also has responsibilities for:

- Overall format and content of the UC test and certification documentation: test procedures, certification memorandum, etc.
- Development and staffing of the Interoperability Test Certification memorandum

## 3 STANDARD OPERATING PROCESS

The standard UC APL process, as identified in the DoDI 8100.04, is shown in **Figure 1**. This process reflects that both IA certification and IO certification are required for placement of products on the UC APL.

**Figure 1 Standard Process for UC APL Certification**



### 3.1 APL Process Rules and Guiding Principles

The following general rules apply to the standard APL process:

1. Vendor obtains government sponsorship.

*Note: Two government POCs are required to ensure sponsor availability for attending ICM and Out-Briefs.*

2. Vendor submits product for testing via APLITS <https://aplots.disa.mil>. In certain limited cases the Sponsor may submit products to the UCCO.

*Note: Product submittal will not be processed until UCCO receives the product documentation package. See Appendix C for additional documentation details (as applicable).*

The following items are to be submitted in the documentation package:

- A detailed diagram of the test environment. The diagram should include all components and their interfaces.
- A comprehensive product documentation set.
- A list of all system components with descriptions, the underlying operating system, all applicable applications and all applicable application version numbers. Interface and functional cards/modules (with quantities) in each chassis listed out in table format, if applicable
- Completed STIG Questionnaire, which is located at [http://www.disa.mil/Services/Network-Services/~media/Files/DISA/Services/UCCO/APL-Process/STIG\\_Questionnaire.pdf](http://www.disa.mil/Services/Network-Services/~media/Files/DISA/Services/UCCO/APL-Process/STIG_Questionnaire.pdf)
- Letter of Compliance (LoC). Vendor will submit LoC in accordance with UC product LoC template that addresses product requirements and IPv6.
  - Submit a signed LoC cover letter with the company logo and attachments which include the respective LoC requirements including IPv6 category compliance for the submitted product(s).
  - Include the requirements as an attachment and state compliance to the requirements.
  - Include the nomenclature(s) and respective software release(s) applicable to this submission.
- Submit the LoC in .pdf format.
- SF 328 Form Certificate Pertaining To Foreign Interests

*Note: Certain UC APL products must be NIAP validated. Please review the respective UCR section to see if your product must undergo NIAP validation. A product requiring NIAP validation that is not already NIAP validated upon entrance into an approved DoD Testing Laboratory will require a plan of action and milestones (POA&M) detailing that the product will obtain NIAP compliance within 180 days of the approving decision.*

The complete documentation package should be uploaded to APLITS at the time of submittal. Failure to do so will result in unnecessary delays to the process.

3. UCCO sends verification request to the sponsor to confirm sponsorship:
  - a. Is the government sponsor of the submitted product in accordance with DoDI 8100.04.

- b. Agrees to attend the ICM, Out-Brief, and TDR adjudication meetings.
- c. Agrees to the configuration submitted by the vendor.
4. Sponsor approves SUT configuration and verifies contact information.
5. UCCO issues Tracking Number (TN) for complete submissions. Assigned Test Lab AO coordinates scheduling of ICM. Attendees include: Vendor, Sponsor, applicable DoD Component Lab POCs, CA representative, JITC AO, and Subject Matter Experts (SME) on the UCR. The outcome of the ICM will be an APL Product-type, agreement on applicable UCR requirements, business model determination, SUT Configuration, IA/IO requirements, test location, products included by similarity (if applicable), and certification document deliverables. The ICM will also determine overall readiness to proceed with testing based on LoC compliance and 18-month rule POA&Ms. The Government may chose to delay or cancel testing based on non-compliance or unacceptable POA&Ms.
6. Assigned Test Lab AO will provide ICM minutes to all attendees and coordinate business model with vendor, sponsor, or DISA NS
7. Products with a complete business model will be placed on the next Scheduling Meeting agenda. Scheduling Meetings take place bi-weekly, however, updates to the schedule may be performed at any time.
8. Vendor is required to submit a complete Self-Assessment Report (SAR) to UCCO 10 business days prior to IA test start date. Conditions as follows:
  - A complete SAR is a representation of findings from all current STIGs applied to the SUT identified during the ICM with mitigation and POA&M statements for all findings.
  - An incomplete SAR will not be accepted.
  - A previous IA Findings Letter will not be accepted in place of SAR.
  - Failure to comply with the SAR requirement will result in a cancellation of the scheduled test dates and the TN in turn will be retired.
  - The IA Test Team will provide the SAR to the Vendor after the ICM.
  - SAR template to be used for IA testing will lock in on date of SAR suspense.
    - If the STIG checklists have been updated from the time the vendor was provided the SAR checklist template (after the ICM), the test lab AO will obtain an updated SAR template to include these updated STIGs. The input from the vendor's-submitted SAR will be transferred to the new, updated templates at the start of IA testing.

*Note: UCCO will send out an email reminder of the SAR due date. Vendors are to use the SAR template provided by the IA Test Team which will be sent in conjunction with the ICM minutes.*

9. UCCO has 3 business days to review the SAR for completeness and distribute to the Test Team.
10. IA Testing commences.
11. IA Testing completed per the Test Lab. If CAT 1 findings exist, the Vendor will submit for a Verification and Validation (V&V) test window. If IA V&V test fails to demonstrate CAT 1 correction, the TN will be retired. Vendor will then need to resubmit the product for testing after the findings have been corrected and / or mitigated.

*Note: V &V testing is carried out if the Vendor believes the problems discovered in testing can be resolved rapidly. If the Vendor is requesting V&V after testing is completed, then the Vendor must submit and be ready for V&V testing within 20 business days of the end of the original test window. If not, the TN will be retired and Vendor will then need to reinitiate the UC APL Process at a later date.*

12. IO Testing commences.
13. IA Test Team disseminates IA Findings Summary to the UCCO and Vendor within 10 business days of testing completion. Test events that result in multiple reports (i.e. ASLAN, Wireless, and LSC) will be granted an additional time as coordinated at the ICM.
14. Vendor has 10 business days from receiving the findings summary to turn in mitigations and IA POA&Ms for findings reported within the IA Findings Summary. Failure to update the IA Finding Summary with mitigations and POA&Ms by deadline will result in TN retirement and vendor will need to reinitiate the UC APL Process. See Appendix D for DISA Field Security Operations (FSO) guidance for the construct of proper Mitigations, POA&Ms and Comments.
15. IA Test Team schedules IA Out-Brief meeting to take place within 10 business days of receiving the IA Findings Mitigations from the Vendor. Required Attendees: Sponsor, Vendor, AOs (Lab and JITC, as applicable), IA Test Team, DISA CA or DoD Component DAA/CA representative and UCCO.

*Note: If during the Out-Brief the IA test team finds that a V&V is required, the Vendor will need to submit a V&V request to UCCO and be ready for V&V testing within 20 business days of the Out-Brief meeting. If not, the TN will be retired and Vendor will need to reinitiate the UC APL Process. A maximum of 2 V&Vs can be requested in one testing cycle before the solution will be retired.*

16. IA Test Team disseminates IA Out-Brief Meeting Minutes within 5 business days after conclusion of the meeting.
17. Vendor submits any action items listed in the IA Out-Brief Meeting Minutes and provides updated IA Findings Summary with mitigations and IA POA&Ms within 10 business days of receiving the minutes, unless an extension has been approved by the UCCO. Failure to submit action items and mitigations and IA POA&Ms by deadline will result in TN retirement and

vendor will need to reinitiate the UC APL Process.

18. IA Test Team submits final draft IA Assessment Report (IAAR) to UCCO within 10 business days of completed Out-Brief action items. Test events that result in multiple reports (i.e. ASLAN, Wireless, and LSC) will be granted an additional time as coordinated at the ICM.
19. UCCO has 3 business days to review the final draft IAAR for quality assurance.
20. UCCO requests Certifying Authority (CA) Certification Determination Recommendation Letter for IA Certification.
21. DISA CA or DoD Component DAA/CA has 15 business days to complete the CA Certification Determination Recommendation Letter and return to UCCO.

*Note: If the DISA CA or DoD Component DAA/CA issues a negative recommendation letter, UCCO will notify the vendor. UCCO allows 10 business days for the vendor to address and correct outstanding issues in the IA report. If the vendor fails to resubmit corrections to the UCCO within this timeframe, the TN is retired and the vendor must reinitiate the UC APL Process. If the vendor corrects the report, mitigates or resolves the findings and submits valid POA&Ms, UCCO will resubmit the report to DISA CA or DoD Component DAA/CA with a request for reconsideration of the certification recommendation.*

*Note: If an IAAR report is returned to the vendor or IA Test Team due to the need for corrections of discrepancies in the report (i.e. product description, diagrams, mitigation errors or missing POA&Ms), delays to the DAA/CA timeline can be expected.*

22. (Conditional step – as necessary) Per decision criteria, if the product is to go to the Defense IA/Security Accreditation Working Group (DSAWG), UCCO has 3 business days to prepare a read-ahead briefing for the SUT and DSAWG) for approval.

*Note: Decision Criteria: If the product type has already been reviewed by the DSAWG, or the technology is well known and understood, the product should not go to the DSAWG. However, if the product technology is first time seen, or has the potential to cause a community risk to the DoD enterprise, the product may go before the DSAWG for review as determined by the DISA CA and NSP.*

23. CA provides UCCO with an IA Certification Recommendation letter or the DAA/DSAWG provides an Authority to Operate (ATO)/Interim authority to operate (IATO).
24. UCCO provides the JITC Action Officer with the IA configuration approval documentation that is based on the CA recommendation letter, ATO/IATO and/or DSAWG approval.
25. In the product's lifecycle, if the Vendor's IA POA&Ms are not met, the product may be removed from the APL based on the guidelines in Appendix D of this document.

*Note: There are times throughout the life of a product where fixes will need to be implemented. Such fixes, especially the ones that close POA&Ms, will need to go through the DTR process. See the Section 3.3 for further details on DTR process.*

26. IO Test Team will coordinate Test Discrepancy Reports (TDRs) with JITC AO during IO test window.
27. Once IO Testing has been completed, the Test Team will provide the record of any open TDRs to the Vendor. The vendor will have 5 business days to provide a response (IO POA&Ms) to the open TDRs; responses should be made with input and concurrence of the Sponsor.

*Note: Responses should minimally include: a IO POA&M addressing whether the vendor plans on resolving the discrepancy, planned resolution timeline, and software / hardware implications if the currently defined system under test if not fixed (hardware/software).*

28. IO Outbrief will be held within 5 days of IO test completion to discuss completion of IO testing, POA&Ms and TDR adjudication schedule. Participants include, test team, sponsor, vendor, JITC AO, and UCCO. AO will provide comprehensive TDR Report and IO Test Summary.
29. If no IO POA&M is received within 5 business days, the TDR adjudication process will proceed without the information. Adjudication may result in TN retirement if the TDRs are deemed to be critical (non-placement on the UC APL).
30. Distributed Test Lab Action Officer (AO) will prepare open TDR synopsis in accordance with prescribed format and staff to the DISA NS Capabilities Center (NS2) IO Adjudication Board Chair for TDR adjudication.
31. Distributed Test Lab IO Team will coordinate the IO Certification Summary with the Action Officer. The Distributed Test Lab will staff the IO Certification Summary and recommendation to JITC within 10 business days after the IO Adjudication Board at which the IO TDRs are successfully adjudicated, or 10 business days after test completion if no IO TDRs are found. Test events that result in multiple reports (i.e. ASLAN, Wireless, and LSC) will be granted an additional time as coordinated at the ICM.
32. After the Distributed Test Lab submits the IO Certification Summary, JITC has up to 10 business days to staff and approve the IO Certification Letter. If JITC is the Lab that performed the IO testing, JITC will have up to 10 business days after the final IO Adjudication Board to draft and approved the IO Certification Letter. Test events that result in multiple reports (i.e. ASLAN, Wireless, and LSC) will be granted an additional time as coordinated at the ICM.

*Note: If the IO Adjudication Board determines that the IO test fails, and there is a Critical TDR, the TN will be retired. Vendor will need to reinitiate the UC APL Process. Any TDRs based on failure to meet UCR standards will be adjudicated for severity, and a way-ahead will be provided to the Vendor.*

33. Vendor submits the Deployment Guide which reflects the SUT, for review and approval by NSP prior to the issuance of UC APL Approval Memorandum.
34. UCCO has 3 business days to prepare the UC APL Approval Memorandum and submit to NSP for signature after receipt of the JITC signed IO Certification Letter. APL listing of the product is for no longer than 3 years.
35. UCCO sends UC APL Approval Memorandum to Configuration Control Board (CCB) members, Sponsors, and Vendors.
36. UCCO posts the product on UC APL website: <https://aplots.disa.mil>
37. From the date of the APL Approval memorandum, UCCO has 10 business days to compile the Information Assurance Assessment Package (IAAP).

*Note: Before an IAAR report is uploaded into APLITS the test team should review for quality assurance. The IAAR is stored in APLITS and available for distribution only to government civilian or uniformed military personnel.*

38. In the product's lifecycle, if the Vendor's IO POA&Ms are not met, the Vendor will be contacted to provide updated POA&Ms. The product will then be reviewed by the IO Adjudication Board and a recommendation will be made by the Board to either extend the POA&M, or proceed with a recommendation to remove the product from the APL. If the IO Adjudication Board recommends that the product be removed from the APL, the board will provide its recommendation to DoD CIO, NSP, and JITC for final determination.
39. Exceptions to the preceding processes will be coordinated with DISA NSP, CA and/or JITC as applicable.

*Note: Products that are already in production networks but not currently on the APL are expected to be submitted for the APL process.*

### **3.2 Update / Changes to current SUT**

Vendors are required to notify UCCO of any updates / changes to the SUT. These changes include, but are not limited to:

- Sponsor Point of Contact (POC)
- Vendor POC
- Software Release
- Product Model
- System configuration
- Test date request
- Verification and Validation request

*Note: Vendors are allowed 2 test deferral requests. If the Vendor is not available to test by the 2<sup>nd</sup> test deferral date, the TN will be retired and the Vendor will need to reinitiate the UC APL Process.*

*Note: It is understood that there are products that are on the APL and are already in production in the field. These products may require fixes to be implemented, such as*

*IAVMs, in order to meet DoD requirements. The implementation of IAVMs will not change the status of a product on the APL. UCCO must be notified via DTR so as to ensure that any documentation changes are addressed.*

The process to update a current SUT is as follows:

1. Vendor submits update / change request(s) via UCCO Website: <https://aplots.disa.mil> (See [APLITS User Guide](#) for instructions). For system configuration updates, a Visio drawing needs to be submitted to the UCCO.
2. UCCO distributes the update / change request(s) to Sponsor/Vendor/Test Team to review for accuracy.
3. If no objection by the Sponsor or Test Team, UCCO makes the update(s)/change(s).

### **3.3 Desktop Review (DTR) Process**

For any changes and/or patch updates to a product that is already on the UC APL, and POA&M closures, a Desktop Review (DTR) application must be submitted to UCCO. DTR request will result in either: update to APL memo, minimal testing as the same TN, or new submission for testing resulting in new TN. Note. A DTR is for changes to existing APL approved software releases (i.e., within UC APL specified major software release), not new major software releases. New software releases will be submitted as new submissions. *Example: an update from version 7.2 to 7.3 would likely be considered a valid DTR, however, an update from version 7.2 to 8.1 would require a new submission.*

1. Vendor submits product for review via UCCO Website <https://aplots.disa.mil> (See [APLITS User Guide](#) for instructions) additionally, the vendor will submit a detailed description of the patch to be evaluated within 5 business days of the DTR request. If documentation package is not received within the 5 business day window, the DTR request will be cancelled.
2. UCCO validates DTR request against DTR criteria.
3. UCCO distributes DTR information and documentation to the original testing lab that accomplished IA and IO testing for review.
4. The testing lab designated AO coordinates IA/IO review. Testing lab AO will provide JITC AO with DTR recommendation within 5 business days. JITC AO will present to the UCCO one of the following recommendations:
  - a. No testing required and recommends that the IO and UC APL memo be updated.
  - b. Minimal testing is recommended. The lab will provide a short detailed description/justification for the recommendation.
  - c. New submission is recommended. The lab will provide a short detailed description/justification for the recommendation.
5. UCCO will forward the recommendation to NSP for review and coordination with Service Manager, if applicable. NSP has 3 business days to provide:

- a. Concurrence on the testing/update recommendation, or the testing recommendation is accepted.
- b. For items 4b and 4c if the IA posture is changed, UCCO will contact the original CA for the product and NSP. This could be the Service CA for products they sponsored or the DISA CA (FSO).
6. The Test Lab that conducted the original IA test shall update the IAAR with DTR information (in an approved DISA format)
7. JITC updates IO certification letter within 10 days of DTR approval or DTR test event, whichever is applicable. (Note: if the product was placed on the APL without a JITC certification (Fast Track), then JITC will coordinate with NSP to determine if a certification requires development. Development of a certification summary report / memorandum will result in additional time being allocated to complete the certification process.
8. Upon receipt of JITC updated IO certification letter, UCCO posts the updated product on the UC APL: <https://aplots.disa.mil> and updates the IAAP with the DTR information
9. If a change to the System Under Test (SUT) is made via the DTR process, an updated deployment guide will be provided by the Vendor.

### **3.4 UC APL Fast Track (FT) Process**

The FT process is intended to expedite new UC product types onto the UC APL, or to use existing artifacts (test results, LOCs, etc.) to aid in placing products onto the UC APL. The FT process is structured to deal with the fact that DoD sponsors may have a need for products for which they have reasonably well-established requirements, and in some cases, test results, yet these products do not appear in the UCR that is published on an annual basis. If the UC Steering Group (SG) agrees that new product categories and/or new products should be in the UCR, the DoD sponsors and vendors do not have to wait for the next UCR to get tested and placed on the APL. The APL testing can begin based on existing requirements that will be placed in the next version of the UCR. Products that are candidates for the FT process are as follows:

- Products that are within existing UCR product categories with well-established requirements, and in some cases, the existing requirements can be augmented by current UCR requirements.
- Products that have existing test results that can be reused to verify requirements against current UCR products or approved FT UC products.
- Products (current UCR products or approved FT products) which are currently fielded and successfully performing from both an Interoperability and Information Assurance perspective in operational networks.
- Products that should be added to the UCR per the UCSG.

Three categories of FT products are as follows:

- Products within Current UCR Product Categories. Products that were tested and/or certified before development of the product category or products that have existing requirements similar to those in the UCR that can be augmented with UCR requirements. These products' ability to demonstrate applicable UC requirements will be verified prior to placement on the APL with coordination of DISA NSP and JITC. An Interoperability Test Certification Memorandum and Certification Summary Report will be developed using the existing test results.
- Operationally Validated. Products (current UCR products or approved FT products) that are currently operating in DoD networks that have an Interim Authority to Operate (IATO) or ATO, are in compliance with appropriate STIGs, and are requesting APL status. Products may be end of life (i.e., APL Removal status) or active (i.e., normal APL status). Products submitted against the operationally validated APL placement shall have UC requirements verified prior to APL placement with coordination of DISA NSP and JITC based upon an LOC for UC Requirements and/or operational field artifacts (testing artifacts, reports, certifications, etc). An Interoperability Test Certification Memorandum and Certification Summary Report will be developed using the specified artifacts.
- New UCR Product Categories. Products that have existing DoD (non-UCR) requirements that can be used in the next version of the UCR and have been approved for the UCR by the UC Steering Group.

#### Submitting a product for UC APL Fast Track Consideration

The rules for submitting a product in Section 3.1 of this document regarding sponsorship and product documentation apply for FT products. For products which are being presented as a new UCR Product Category, that category should be specified at the time of submission in APLITS. If there are existing test results or certifications available they should be included in the APLITS product documentation submission. Once the documentation set is complete, a meeting will be scheduled with the Vendor, Sponsors, UCCO, JITC, Distributed Lab (if applicable) and NS Engineering team to evaluate product maturity, features affecting Assured Service, and suitability for UC APL testing. The UCSG will be used to provide guidance and issue resolution as necessary. UCCO will disseminate the results of the meeting and related discussions and clarify the way forward to all parties.

APPENDIX A  
ACRONYMS

<b>Acronym</b>	<b>Definition</b>
<b>APL</b>	Approved Products List
<b>ATO</b>	Authorization to Operate
<b>CA</b>	Certifying Authority
<b>C &amp; A</b>	Certification and Accreditation
<b>CCB</b>	Configuration Control Board
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>CJCSI</b>	Chairman Joint Chiefs of Staff Instructions
<b>DAA</b>	Designated Accrediting Authority
<b>DATO</b>	Denial of Authorization to Operate
<b>DISA</b>	Defense Information Systems Agency
<b>DISN</b>	Defense Information System Network
<b>DoD</b>	Department of Defense
<b>DoDI</b>	Department of Defense Department Instruction
<b>DSAWG</b>	Defense IA/Security Accreditation Working Group
<b>DSN</b>	Defense Switched Network
<b>DTR</b>	Desk Top Review
<b>FFS</b>	Fee For Service
<b>FSO</b>	Field Security Operations
<b>IATO</b>	Interim Authorization to Operate
<b>ICM</b>	Initial Contact Meeting
<b>IA</b>	Information Assurance
<b>IAAP</b>	Information Assurance Assessment Package
<b>IAAR</b>	Information Assurance Assessment Report
<b>IO</b>	Interoperability
<b>IP</b>	Internet Protocol
<b>JIC</b>	Joint Interoperability Certification
<b>JITC</b>	Joint Interoperability Test Command
<b>JS</b>	Joint Staff
<b>MILDEP</b>	Military Department
<b>NIAP</b>	National Information Assurance Partnership

<b>Acronym</b>	<b>Definition</b>
<b>NII</b>	Networks and Information Integration
<b>NIPRNet</b>	Unclassified Internet Protocol Router Network
<b>NS</b>	(DISA) Network Services (Directorate)
<b>OSD</b>	Office of Secretary of Defense
<b>OSS</b>	(DISA NS) Operational Support Systems (Division)
<b>POC</b>	Point of Contact
<b>RTS</b>	Real Time Services
<b>SAR</b>	Self Assessment Report
<b>STIG</b>	Security Technical Implementation Guide (STIG)
<b>SUT</b>	System Under Test
<b>TDR</b>	Test Discrepancy Report
<b>TN</b>	Tracking Number
<b>UC</b>	Unified Capabilities
<b>UCCO</b>	Unified Capabilities Certification Office
<b>UCR</b>	Unified Capabilities Requirements
<b>USD</b>	Under Secretary of Defense
<b>V&amp;V</b>	Verification and Validation

APPENDIX B  
REFERENCES

- Department of Defense (DoD) Unified Capabilities Requirements (UCR) 2008 Change 3, December 2010
- Chairman of the Joint Chiefs of Staff Instruction 6212.01E, “Interoperability And Supportability Of Information Technology and National Security Systems,” 15 December 2008
- CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities, 24 January 2012
- CJCSI 6215.01C, “Policy for DoD Voice Networks with Real Time Services (RTS),” 9 November 2007
- DoDI 8100.04 “DoD Unified Capabilities”, 9 December 2010
- DoDD 8500.1E, “Information Assurance (IA),” 24 October 2002
- DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
- DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007

## APPENDIX C

### UC APL DOCUMENTATION GUIDE

#### 1 INTRODUCTION

The following document outlines the minimum requirements for acceptable documentation intended for submittal to the Unified Capabilities Certification Office (UCCO) in support of the Unified Capabilities Approved Products List (UC APL) testing. Anyone attempting to submit a product for UC APL testing will be expected to provide the following at the time of submittal:

#### PRE-TRACKING NUMBER DOCUMENTATION

- 1) A detailed diagram of the test environment,
- 2) A comprehensive product documentation set,
- 3) A list of all system components with descriptions, the underlying operating system, all applicable applications, and all applicable version numbers, and
- 4) Completed Security Technical Implementation Guide (STIG) Questionnaire.

All applicants attempting to complete a submittal must provide these documents to the UCCO in order to receive a tracking number and start processing of the submittal for testing. This document is meant to assist solution vendors and sponsors in the development of the above identified solution documents.

The UCCO will confirm receipt of documentation when the above requirements have been satisfied.

All documentation should be submitted to the UCCO using APLITS <https://aplots.disa.mil> :

*Table C2.1 – Documentation Checklist*

Diagram	<input type="checkbox"/>
System description	<input type="checkbox"/>
STIG Questionnaire	<input type="checkbox"/>
Letter of Compliance	<input type="checkbox"/>
SF-328 Form	<input type="checkbox"/>
SAR ( <i>provided after the ICM</i> )	<input type="checkbox"/>

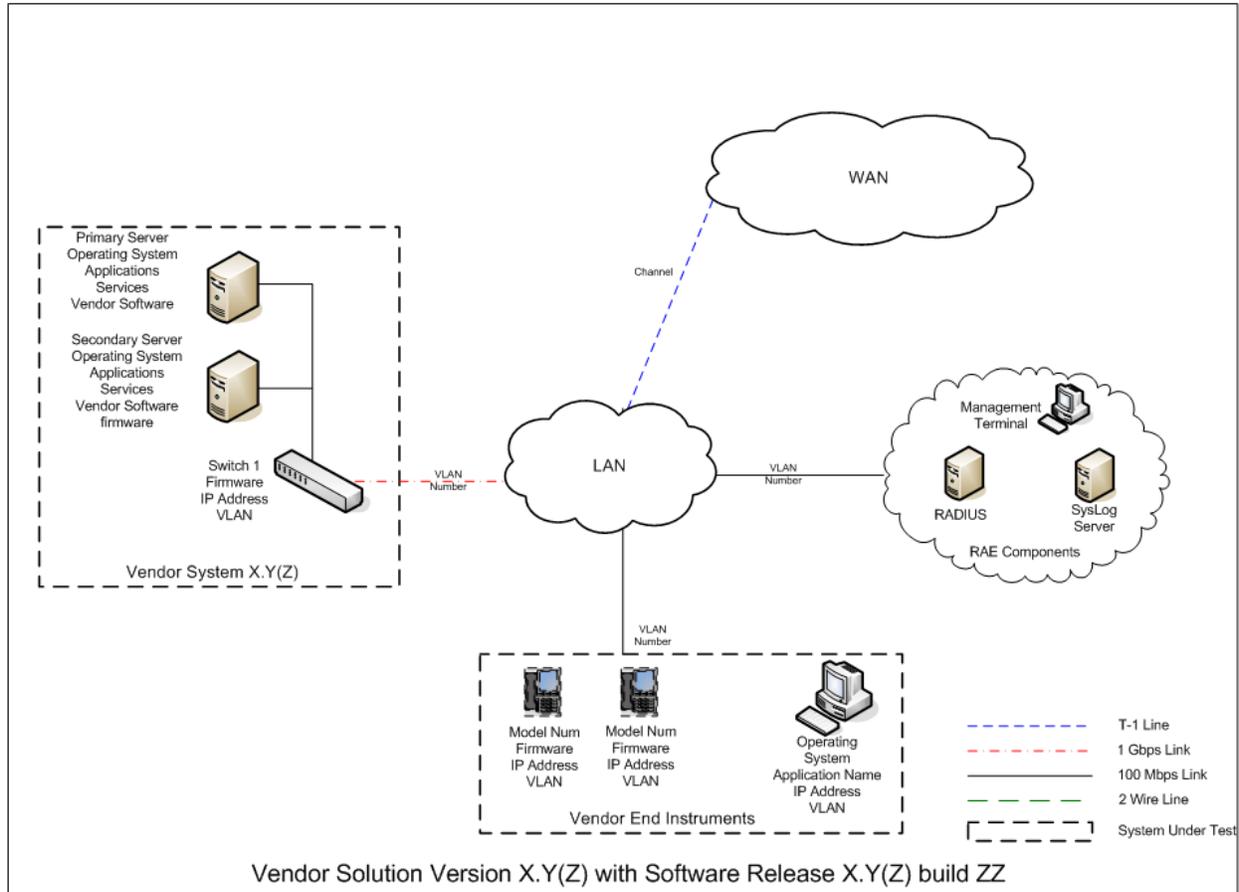
**E-mail:** [disa.meade.ns.list.unified-capabilities-certification-office@mail.mil](mailto:disa.meade.ns.list.unified-capabilities-certification-office@mail.mil)

**Phone: UCCO Process Questions :** (520) 538-3234 or (703) 365-8801 x3434

#### 2 SOLUTION DOCUMENTATION

##### 2.1 SYSTEM DIAGRAM

The detailed diagram of the test environment must be in Visio format. Please note the Visio version (i.e., 2000 Technical, 2002 Standard or 2003 Professional, etc.) when submitting the system diagram. See Figure C2.2 as an example of an acceptable solution diagram.



*Figure C2.2 – Sample Diagram for Submission*

The items identified within the heavy solid lines are items within the test boundary. Use this example diagram to show a functional item that falls outside the test boundary. Note the Operating Systems (OSs), applications, databases, web servers, Internet Protocol (IP) addresses, etc. applicable to the solution. Creation of a legend is required. All acronyms used will be defined in the drawing and in the documentation upon first use.

## 2.2 SYSTEM DESCRIPTION

Provide a brief description regarding the functionality and purpose of the entire solution. This is usually approximately a paragraph. It gives the reader a clear understanding of what type of solution it is, i.e., (Session Controller), Network Element, etc. Please spell out acronyms if they are used.

## SOLUTION COMPONENTS

All solution components that will be involved in the testing of the solution need to be clearly identified in the solution's product documentation. If there are components needed to provide proof of functionality for the System under Test (SUT), but not targeted for Information Assurance (IA) and Interoperability (IO) certification, these components need to be clearly identified and remain outside the test boundary. The test boundary should be clearly identified

within the diagram using lines around the components of the SUT. The only solution components that are represented in the diagram as part of the SUT should be those components desired by the government sponsor of the solution. No optional solution components that are available for purchase not requested by the government sponsor should be included in the SUT diagram submitted to the UCCO.

SUT	Release	Function	Sub-Component	Description
Vendor Family Series XYZ				
Box 100Series 100-1 100-2	OS 2.3	Routing	N/A	Provides ....
100 Manager		Syslog/Admin	100M-Xmodule	
Notes and Legends as necessary				

*Table C2.3 Sample Solution Component Table*

## COMPONENT DESCRIPTION

Provide a brief description of each component in the solution noting its function. Ensure marketing language is removed from the component descriptions and hardware/software versions are accurate.

Use the following format as an example:

**Component #1** Component description, primary and secondary functions, unique hardware features, (i.e., failover, active or passive), without marketing language. Also indicate whether or not the system is the primary or the subordinate in the SUT.

- 1) Hardware. The model, not the host name,
- 2) OS. This includes versions and any Service Pack (SPs),
- 3) Application. Custom vendor software version 4.2, Microsoft Structured Query Language (SQL) 2000 SP4, McAfee Enterprise 8.0.0i.
- 4) Firmware, and
- 5) IP address (If known)
- 6) Rack Space and Power Requirements

**Component #2** Component description, primary and secondary functions, unique hardware features, (i.e., failover, active or passive), without marketing hype. Also indicate whether or not the system is the primary or the subordinate in the SUT.

- 1) Hardware. The Model, not the host name (i.e., Vendor Chassis):
  - a. Card 1- Card 1's description,
  - b. Card 2- Card 2's description, and
  - c. Additional components as needed,

- 2) OS. This includes versions and any SPs,
- 3) Application. Custom vendor software Version 4.2, SQL 2000 SP4, McAfee Enterprise 8.0.0i,
- 4) Firmware,
- 5) IP address.
- 6) Rack Space and Power Requirements

## **SOLUTION OS**

As shown in Figure C2.2 Sample Diagram, the specific OSs of all components within the certification boundary of the SUT, including patch level and service pack details, need to be clearly identified and labeled on the provided diagram. The specific OS identified in the diagram needs to be identical to the system intended to be deployed by the government sponsor of the solution.

*Note: It is very important that the vendor and sponsor of any solution discuss and agree upon the OSs of each component of the solution prior to submitting their documentation to the UCCO.*

## **SOLUTION APPLICATIONS**

As shown in Figure C2.2 Sample Diagram, the specific application details of any non-standard applications (i.e., Microsoft Office Suite) running on any of the components within the certification boundary of the SUT, including software release or version details, need to be clearly identified and labeled. The specific application information system identified in the diagram needs to be the exact same as what is intended for deployment by the government sponsor of the solution.

*Note: It is very important that the vendor and sponsor of any solution discuss and agree upon the details of the applications desired for each component of the solution components prior to submitting their documentation to the UCCO.*

## **SOLUTION CONNECTIONS**

As shown in Figure C2.2 Sample Diagram, the specific details of all connection types supported by the SUT that are desired to be covered within the certified configuration of the solution must be clearly detailed and labeled in the diagram submitted to the UCCO. The only solution connections that are represented in the diagram as part of the SUT should be those components desired by the government sponsor of the solution. No optional solution connection types that are available but not requested or needed by the government sponsor should be included in the SUT diagram submitted to the UCCO.

*Note: It is very important that the vendor and sponsor of any solution discuss and agree upon the details of the connection types necessary to support the configuration of the solution intended for actual deployment by the sponsor prior to submitting their documentation to the UCCO.*

## SOLUTION MANAGEMENT/ADMINISTRATION

Most solutions have a number of different options available to manage the solution. The main options fall under the following categories:

- 1) Local Management Only:
  - a. Management directly connected to the terminal, and
  - b. Management directly connected to an administrative Personal Computer (PC)/laptop.
- 2) Emergency Management. Major configuration and setup operations for the solution are performed by the manufacturer prior to shipping the product to the installation site. No further administrative access to the device is needed except during emergency maintenance of the device.
- 3) Remote Management:
  - a. In-Band Management. Management done via Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Network Management Protocol (SNMP),
  - b. Out-of-Band (OOB) Management. Management via modem. If a modem is intended to be used, it is required that an approved UC APL secure modem is used in the solution or the modem must be included in the SUT and subject to full IA testing.

If the SUT intends to be certified using either Option #1 or #2 as the method for management, it needs to be noted in the diagram. If the solution intends to support Option #3, remote management, the port, protocol, and version being used by the system to support remote management needs to be included in the diagram.

*Note: It is very important that the vendor and sponsor of any solution discuss and agree upon the method of management that will be used to support the administrative functions of the solution intended for actual deployment by the sponsor prior to submitting the documentation.*

Provide details of any file sharing done by the SUT, components of the SUT involved, method used for file sharing, and ports and protocols involved.

### 2.3 DISN UC APL STIG QUESTIONNAIRE

[http://www.disa.mil/Services/Voice-Video-and-Data-Services/~media/Files/DISA/Services/UCCO/APL-Process/STIG\\_Questionnaire.pdf](http://www.disa.mil/Services/Voice-Video-and-Data-Services/~media/Files/DISA/Services/UCCO/APL-Process/STIG_Questionnaire.pdf)

The STIG Questionnaire has been developed to help vendors analyze their solutions and determine which Department of Defense (DoD) STIGs are applicable based on the break out of all the components, software applications, general environment configuration, protocols and management methods used by the solution.

### 2.4 UNIFIED CAPABILITIES LETTERS OF COMPLIANCE (LOC) RULES OF ENGAGEMENT (ROE)

- 1) Detailed requirements for UC products and/or functions are provided or referenced in the UC Requirements Documentation.

- 2) Submit a signed Letter of Compliance (LoC) cover letter with company logo with attachments which include the respective category for your appliance  
<http://www.disa.mil/Services/Network-Services/UCCO/Policies-and-Procedures>
  - a. Include the IPv6 general requirements as an attachment and state compliance to the requirements relevant to your profile.
  - b. Include the nomenclature(s) and respective software release(s) applicable to this submission.
  - c. Submit the compliance letter in .pdf format, on company letterhead, and with a Vice President level authority signature.
- 3) In accordance with the UCR, systems are required to have IPv6 capability for testing.

## 2.5 SF-328 FORM CERTIFICATE PERTAINING TO FOREIGN INTERESTS

All companies submitting for UC APL testing must submit an up-to-date Standard Form 328 (SF328) with their product documentation. Instructions for filling out the SF328 can be found at [http://www.dss.mil/documents/foci/sf328\\_instructions.pdf](http://www.dss.mil/documents/foci/sf328_instructions.pdf) the SF328 itself can be found at <http://www.dss.mil/documents/foci/sf328.pdf>

## 3 POST TRACKING NUMBER DOCUMENTATION

- 1) Self-Assessment Report (SAR)
- 2) Deployment Guide.

All applicants attempting to complete APL certification must first agree to provide these two documents to the UCCO in order to receive final APL approval. This document is meant to assist solution vendors and sponsors in the development of the above two identified solution documents and to reduce the amount of time by all parties involved in achieving acceptable product documentation packages.

### 3.1 Self Assessment Report (SAR)

- Vendors may use the STIG Questionnaire to generate a list of applicable STIG Checklists to complete. The full list of applicable STIGs will be validated during the ICM and provided to the vendor in the appropriate SAR Template format by the Action Officer with the ICM minutes.
- The SAR template is also located at <http://www.disa.mil/Services/Voice-Video-and-Data-Services/UCCO> under Key Document and Requirements. This document is to be used as a guide only; the most recent and applicable SAR Template will be provided by the Action Officer. *All SARs must be in Excel format using the provided template.*
- SAR checklists to be used for IA testing will lock in on date of SAR suspense.
  - If the STIG checklists have been updated from the time the vendor was provided the SAR checklist template (after the ICM), the test lab AO will obtain an updated SAR template to include these updated STIGs. The input from the vendor's-

submitted SAR will be transferred to the new, updated templates at the start of IA testing.

- The following minimum requirements necessary to be considered a complete Self-Assessment:
  - Shows the status of all STIGs identified in the SAR Template (open, closed, N/A, etc.),
  - Has completed mitigations for each Open finding. If a status is marked N/A please include a short comment detailing why it is considered N/A., and
  - If the Self-Assessment is for a retest, provide additional requirements to show resolution of all items identified during the previous solution outbrief.
  - For all STIGs that have automated scripts available, the results from applying those to all components of the solution showing all status (i.e., open, closed, Not Applicable [N/A], etc.) need to be included in the Self-Assessment package. The majority of the automated scripts generate multiple files for different uses, with one containing all the consolidated findings. If that document is available from the automated script, then it is sufficient instead of sending all the raw output data from the scripts. Other acceptable options are pulling all the vulnerability data from the raw output of the scripts and consolidating into either a Microsoft Excel, Microsoft Word, etc.
- The SAR is due to the UCCO two weeks prior to scheduled APL testing (i.e., Setup). The UCCO highly encourages Self-Assessment Reports be submitted as soon as possible to avoid delays or confusion regarding test preparation.

If additional information or more detail is required, please contact the UCCO.

### **3.2 DEPLOYMENT GUIDE**

Prior to final APL approval, the vendor is required to submit to the UCCO a vendor-developed Deployment Guide. The purpose of this document is to collect, document and make available to the DoD community all configuration changes made during testing to the solution by the vendor in order to pass IA and IO. The Deployment Guide will provide enough detail to allow a customer to take an out of the box solution and reconstruct the final configuration of the solution as tested and approval.

The following evaluation factors should be considered by the vendor/sponsor when developing the document:

- Is the DG titled to reflect that it is the Military Unique Deployment Guide?
- Does the DG include the Vendor's Logo?
- Is the DG dated? Is the date of the DG after the Final IA Outbrief?

- Is there version numbering, Document Change Control History page, information for who to submit recommendations for comments/changes, and a page numbering scheme?
- Does the DG include the Conditions of Fielding as reflected in the IAAR?
- Does the DG include any clarifying or necessary screen shots?
- Does the DG include any clarifying or necessary device configuration files?
- Does the DG include any clarifying or necessary reference tables to specific portions of a solution's Users' Guide that provides information on addressing a specific issue?
- Does the DG include clarifying or necessary Vendor configuration details/release notes/tweaks implemented during testing?

The Deployment Guide can be submitted to the UCCO at any point after testing is successfully completed for early feedback and guidance on format and information.

## APPENDIX D

### MITIGATIONS, POA&MS AND COMMENTS GUIDANCE

#### 1 INTRODUCTION

This Appendix is designed to provide guidance on developing IA mitigations and Plan of Action and Milestones (POA&M) for both IA and IO.

##### Background

In accordance with the DODI 8100.4 Instruction, DoD Unified Capabilities (UC), dated December 9, 2010, ENCLOSURE 3, Paragraph 4, “UC products acquired by the DoD Components, and connected or planned for connection to DoD networks, shall be both interoperability and IA certified pursuant to the UCR or an approved information support plan that includes UC products.” Paragraph 4.3 states: “The UC APL is the single authoritative source for certified UC products intended for use on DoD networks. The DoD Components are required to acquire or operate only UC products listed on the UC APL, unless, and until, a waiver is approved.

##### **IA POA&M Policy**

The DoD Components shall issue a new or update an existing accreditation decision when UC products are installed, pursuant to DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” dated November 28, 2007”. As a result, all vendors, who wish to have their product listed on the Approved Product List APL, must comply with the DoDI 8510.01 instruction, DoD Information Assurance Certification and Accreditation Process (DIACAP), dated November 28, 2007 and obtain an Authorization to Operate (ATO).

Under the DIACAP process, Section 4.1 states that “The Department of Defense shall certify and accredit Information Systems (ISs) through an enterprise process for identifying, implementing, and managing Information Assurance (IA) capabilities and services. IA capabilities and services are expressed as IA controls as defined in DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” dated February 6, 2003.” These IA controls are tested as part of the IA testing phase of the UCCO APL process and the results of the testing are documented in an Information Assurance Assessment Report (IAAR) and a DIACAP Scorecard.

The DoDI 8510.01 instruction provides specific guidance regarding the issuance of ATOs with regards to IA findings and mitigations. Paragraph 6.3.3.1.4.1 states: “CAT I weaknesses shall be corrected before an ATO is granted.” As a result, each CAT I finding will be resolved by the vendor. Paragraph 6.3.3.1.4.2 states: “CAT II weaknesses shall be corrected or satisfactorily mitigated before an ATO can be granted.”

Furthermore, Paragraph 6.3.3.2.6.1.3 states: “A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or

satisfactorily mitigated within 180 day of the accreditation decision.” As a result, all CAT II findings must be either resolved or satisfactorily mitigated to an acceptable level of risk.

The clear evidence required by this statement is a POA&M. DoDI 8510.01 instruction Paragraph Enclosure 3.4 reinforces this requirement by stating: “An IT Security POA&M is required for any accreditation decision that required the corrective action and is also used to document Non Compliant (NC) or Non-Applicable (NA) IA controls that have been accepted by the responsible DAA.”

Finally, Paragraph 6.3.3.1.4.3 states, “CAT III weaknesses will not prevent an ATO from being granted if the DAA accepts the risk associated with the weaknesses.” It should be noted that CAT III findings will require a Mitigation and a POA&M also. For further information on POA&Ms see Enclosure 3 of the DoDI 8510.01 instruction. It should be noted that even though mitigations to lower the level of risk enable an ATO to be approved, vendors are still required to fix the product and the CAT II findings remain open until the finding is fixed.

### IA POA&M Format

The following two examples of mitigations and POA&Ms are provided to assist in the development of IAAR reports. It is requested that the following format be used and the mitigations, POA&Ms and comments be provided in blue.

**VULID/STIGID:** VMS ID: V0013727/PDI: WA000-WWA026

**Requirement:** The httpd.conf StartServers directive is not set properly.

**Finding:** The httpd.conf StartServers directive is set to 16. It should be set between 10 and 15.

**Vulnerability:** These requirements are set to mitigate the effects of several types of DOS attacks.

**Components Affected Components Affected (2):** Vendor Network Controller A, Vendor Network Controller B.

**Mitigated by RAE:** NO

**Vendor Mitigation:** In this area, please specify what controls will be implemented to lessen the risk, (i.e. placing the product behind a firewall, restricting by IP address, running the application on a CAC enabled workstation, placing the product in a secured area, password change procedures will be documented in the Deployment Guide). Also, include any additional Condition of Fielding in this area which will lessen the risk.

Preface the controls with: “This finding will be mitigated by ...”

**Vendor POA&M:** In this area, please specify what the fix is, when the fix will be implemented by and how the fix resolves the finding. The date specified must be within 180 days of the date that the product is placed on the APL. Please specify the date in the format MM/DD/YYYY. (i.e. If the fix was to change the products configuration file, the POA&M would stat: “The fix is to change the product configuration file to include the directive ..... which implements ..... by MM/DD/YYYY.”)

(Note: If the finding cannot be fixed, because of such reasons as technology limitations or your product requires a third party product, then you must request the DAA to accept the risk. To do so, please specify: “The vendor requests the DAA to accept the risk because .... (please state why you are making the request, (i.e. a fix to the product cannot be implemented because there is not enough storage or it will break the product in the following manner .....). Not specifying a date, or saying that the fix is estimated to be implemented by or is scheduled for sometime in Quarter Number or stating a specific date cannot be provided at this time is unacceptable and will delay the product’s addition to the APL.

**Vendor Comment:** In this section, please provide any additional information about the product that will help in a recommendation determination. Such things as: how the product will be deployed in the field or how it will be administered, or if only administrators are allowed to use the application are considered good information. Copying a STIG section in this area is not acceptable or specifying that the vendor does not consider the finding a finding is not acceptable.

For findings that are mitigated by Required Ancillary Equipment (RAE), it is acceptable to change the above “Mitigated by RAE” statement from NO to YES and a description of the mitigation utilizing the RAE be provided in the Vendor Mitigation section. If a follow-on product change is to be made, please describe what the change will be in the Vendor Comment section and under the Vendor POA&M provide the date the product will be changed. Below is an example.

a) **VULID/STIGID:** VMS ID: V0006173/PDI: APP6140

**Requirement:** Log files are not retained for at least one year.

**Finding:** The product does not have any means of notifying the user when the logs are full. However, this is mitigated through the use of an external SYSLOG server.

**Vulnerability:** Log files should be maintained so that if any questionable event should occur on the network, the situation could be reconstructed to determine exactly what happened. Keeping Log files for a period of one year provides a sufficient amount of time to determine if anything occurred that requires evaluation.

**Components Affected (2):** Vendor Network Controller A, Vendor Network Controller B

**Mitigated by RAE:** Yes, as proven by the use of an external SYSLOG server.

**Vendor Comment:** The vendor believes that this requirement will be better handled through the use of RAE and will continue to

require an external SYSLOG server. This will be included as a condition of fielding.

Finally, all UCR, IPV4, and IPV6 findings are to be treated the same as STIG findings when attaching Category levels, with HIGH being treated as a CAT I, Medium as a CAT II, and Low as a CAT III. Mitigation/POA&Ms should concur with STIG mitigation requirements. Finally, all Open Ports Table findings should be addressed with a mitigation and POA&M.

## IA POA&Ms Rules of Engagement

- Vendor provides quarterly updates, and updates to coincide with scheduled finding POA&M completions.
- CA and DAA approve APL listing with expectation to close POA&Ms
- UCCO will send notifications of the POA&M expiration date and provide guidance for successful closure:

Options to successfully close this POA&M include:

- 1) Verification from government or military personnel responsible for overseeing the installation of the solution with the approved POA&M closed (Preferred)
- 2) Desktop Review of the fix to the solution by the Test Centers resulting in no additional testing
- 3) Desktop Review of the fix resulting in required Verification and Validation testing necessary to update the solutions certification.

- If one of the 3 options is met prior to the expiration date, the POA&M will be closed out and the product will remain on the APL.
- If by the expiration date none of the options to close the POA&Ms have been met then the following will be applied at NS Leadership's discretion:
  - Vendor either does not respond or responds negatively to the NS POA&M notification – Results in **Removal from APL**
  - Vendor responds that the POA&M conditions have been met but is currently in process to identify the best option to satisfactorily prove to NS– Results in **Remaining on APL** with the expectation of an expeditious resolution. Timeline to be granted at NS leadership discretion.
  - Vendor responds that the fix is still in progress and requests additional time for the POA&M. – Results in **Possible Removal from APL** based on NS leadership decision.

## IO POA&Ms Rules of Engagement

- Once IO Testing has been completed the Test Team will provide record of any open TDRs to the Vendor. The vendor will have 10 business days to provide a response (IO POA&Ms) to the open TDRs; responses should be made with input and concurrence of the Sponsor. *Responses should minimally include: an IO POA&M addressing whether the vendor plans on resolving the discrepancy, planned resolution timeline, and software / hardware implications the currently defined system under test if not fixed (hardware/software).*
- If no IO POA&M is received within 10 business days, the TDR adjudication process will proceed without the information. This may result in TN retirement if deficiencies are deemed to be critical (non-placement on the UC APL).
- DoD Test Lab AO will prepare open TDR synopsis in accordance with prescribed format and staff to DISA NS2 for adjudication.
- TDRs will be adjudicated by and NS-led adjudication team. Participants for adjudication should include NS representation, JITC, and sponsor.
- All adjudications with an outcome that would preclude certification (i.e. critical) will be reviewed by DoD CIO, DISA NSP, DISA NS2, and JITC. Final adjudication decision will be provided to the vendor, test facility, and JITC for appropriate action.
- Post APL active status: any vendor IO POA&Ms that are not met will result in review of the APL validity. DISA NS2 and JITC will review and provide DoD CIO a recommendation as to whether the product should remain on the active APL or be placed on the APL Removal List.

### **Waivers and Test Discrepancy Reports (TDRs) for DoD UC Interoperability (IO) Requirements**

1. The following policy applies to all DoD Components, sponsors, and/or fielding authorities seeking to field UC products that do not meet ALL DoD UCR 'required' IO requirements for the respective UC product:
  - a. DoD Components shall only acquire UC products that have been placed on the APL.
  - b. To be placed on the APL, a UC product must have Information Assurance (IA) approval and have no remaining critical IO deficiencies for not having met the respective UC product 'required' IO requirements.
  - c. Waivers to UC product IO requirements may be granted to accommodate the introduction of new or emerging technology, pilot programs, or to accommodate critical operational requirements for specific limited fielding when validated by the DoD Component concerned, coordinated with, and recommended by the DISA (NSP), and approved by DoD CIO.
  - d. Only the DoD CIO, in coordination with DISA (NS) and DISA (JITC), may revise or waive requirements contained in the UCR.

- e. Waivers to UC requirements shall not normally be granted for a period exceeding 1 year. Only in exceptional circumstances, and with DoD CIO approval, shall extensions of waivers be granted. Vendors who do not implement corrective actions/mitigations to resolve waived requirements within the waived period (e.g., 1 year), are subject to having the product removed from the APL. DISA UCCO shall maintain the status of granted waivers.
2. To certify and place products on the UC APL without meeting all applicable UCR product IO functional requirements, performance objectives, and technical specifications, the following process shall be adhered to:
- a. DISA (JITC) or the DoD Component Test Lab shall analyze interoperability test results with all parties concerned and develop test discrepancy reports (TDRs) that detail the UC IO requirement deficiency. At the completion of testing, the DoD Component Lab or JITC shall submit open TDRs accompanied by a vendor's Plan of Actions and Milestones (POA&M) for adjudication to DISA (NS2) TDR Adjudication Panel.
  - b. The TDR Adjudication Panel shall make the TDR severity recommendation (critical to certification, minor with POA&M, or requirement change required).
  - c. TDR adjudication recommendations that would result in a UC product not being certified will be vetted and approved by DoD CIO, DISA (NSP), and DISA (JITC).
  - d. UC products that have critical TDRs will not be certified or placed on the APL unless the UC requirement has been waived by the DoD CIO.
3. If a DoD Component/sponsoring agency/fielding authority desires to field the UC product with the critical deficiencies identified during Test and Evaluation (T&E), then the DoD Component/sponsoring agency/fielding authority shall submit a UCR Waiver Request to DISA (NSP).
4. DISA (NSP) shall review the results of T&E, operational impact assessment, and DoD Component UCR Waiver Request; and provide a recommendation on the waiver to DoD CIO.
5. DoD CIO shall review the DISA (NSP) waiver recommendation, DISA (JITC) certification recommendation, and make the final waiver decision leading to DISA (JITC) certification.

## APPENDIX E

## JITC FEE FOR SERVICE RULES OF ENGAGEMENT

After DISA and Sponsor acceptance of the completed submittal and assignment of the solution tracking number (TN), an Initial Contact Meeting (ICM) will be scheduled to discuss the scope of testing and the cost model that applies to this vendor solution; either DISA NS2 funding or Fee For Service (FFS). Vendor products used within the DISN core network will be tested under an equipment Cooperative Research and Development Agreement (CRADA). Edge products will be targeted for vendor Fee For Service (FFS). Generally, if an Edge product is sponsored by DISA, then it will be tested under the NS2 funding cost model. Products will only be listed on the APL if IA and IO certifications are successful. The equipment CRADA and FFS cost models are defined as follows:

- **Equipment CRADA:** The government and vendor agree through a legal document that the cost of the Approved Product List (APL) testing (Information Assurance and Interoperability) will be paid for with the vendor equipment that is left at the government test facility. That is, the government is exchanging the cost of their test labor for vendor equipment. The government will support equipment CRADAs for any product determined to be part of the DISN core or essential to the DISA transition to end-to-end IP connectivity for all DoD users.
- **FFS (Cost CRADA):** The vendor or the sponsor agree through a legal document to pay the government for the cost of APL testing with a check (refer to DoD Component Lab practices) or Military Interdepartmental Purchase Request (MIPR) for all labor, installation, travel, de-installation (if applicable), and Other Direct Costs (ODCs) that are incurred in support of APL testing. Payment for testing does not guarantee listing on the APL. Costs associated with each FFS product can be estimated by reviewing the document entitled “Estimated Test Timeframes for UCR Product Categories” at <http://www.disa.mil/ucco> ”

Vendor applicant will be informed of the Cost Model that applies to their product by the government Action Officer at the Initial Contact Meeting. When the Cost Model is FFS, the following process will be supported:

- 1) Government will generate a cost CRADA that will contain similar language provided in the Equipment (No-Cost) CRADA, a cost breakdown, and a listing of vendor equipment.
- 2) The following estimated cost information will be included in the cost breakdown as a minimum:
  - a. Government Services and Other Direct Costs (ODC)\*
  - b. Contractor Test Labor costs\*\*
- 3) The government will submit the cost CRADA to vendor for signature within 3 weeks of the ICM. The government does not require the vendor to have signed the cost CRADA prior to scheduling, however the cost CRADA must be signed by both parties and funding received at

least 4 weeks prior to the scheduled start of test. Otherwise, the government will have to remove the vendor product from the test schedule and reschedule after funding is received.

4) Concurrent with the cost CRADA development, the government will send the vendor a formal detailed cost estimate letter with the details of where to send check, type check required, and government agency check should be made out to.

5) If testing is completed early or if vendor chooses to terminate test early due to large number of findings that precludes product listing on the APL, the remaining test funds on task will either be returned to vendor or left on task for future test activities after coordination with vendor.

Note, that the maximum length of time funding can remain on task is one year from the time of receipt of funds.

6) During testing, JITC testers will work with the vendor to resolve findings at vendor's request, but if testing is not completed at the end of the test window, then all testing will stop until additional funds are received from the vendor based on an amended cost CRADA.

7) Vendor complaints on test process, test delays, test personnel, have to be submitted in writing and the government will determine if additional test time is justifiable at no expense to the vendor.

8) Products that are on an active equipment (No-cost) CRADA will not be subject to FFS during the life of the CRADA. Therefore, testing of software or hardware updates will be in accordance with the rules of No-cost CRADA items through the life of the CRADA. The government however, can terminate No-cost CRADAs in accordance with the terms of the CRADA prior to its expiration date and retain ownership of all hardware and software. Additional testing of items on terminated No-Cost CRADA will occur through a FFS agreement.

\*Government labor is estimated to be approximately 15% of contractor costs.

\*\*Contractor labor is based on estimated test timeframe. Test timeframe for each product category in the UCR can be found at following URL, <http://www.disa.mil/Services/Voice-Video-and-Data-Services/UCCO/Policies-and-Procedures?panel=1> APL products test timeframes. Each product category has a maximum, intermediate, and minimum test window, one of which will be chosen by AO depending on product maturity. To assist vendor in estimating testing cost, the nominal cost for one-man week can be estimated as \$3000.

## APPENDIX F

### 18 MONTH RULE

When a UCR requirement addition, change, or deletion occurs and the UCR is signed, one of five dispositions will apply on the 1st day of a product interoperability test window as follows:

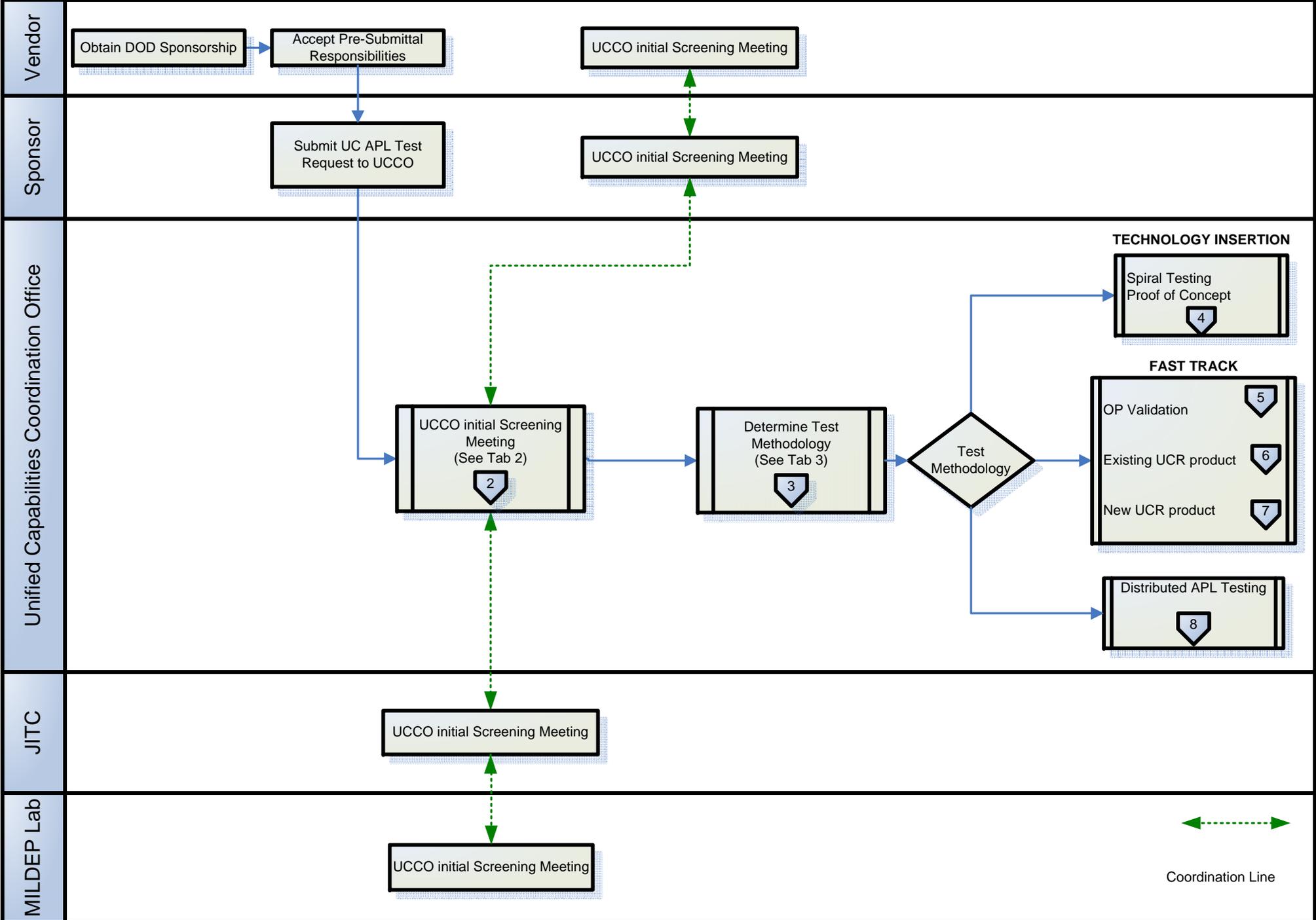
- 1) If the requirement has been lessened, vendor compliance is immediate.
- 2) If warning of the requirement change has been given before approval and the vendors notified via the UCCO web page, the requirement compliance may be immediate.
- 3) If the requirement addresses a Critical or Major IA risk, compliance is immediate.
- 4) If the requirement is necessary for multivendor interoperability, compliance is immediate.
- 5) All other requirements will become applicable 18 months after the UCR publication (see note below for 18 months occurring within test window).

If the UCR does not clarify whether a new requirement is immediate or 18 months, the requirement is considered an 18 month requirement. Requirement modifications occurring between UCR versions will be posted to the UCCO UCR section web link to which it applies. Only Critical or Major IA risk requirement changes between UCR versions will apply to products and will be deemed immediate. Requirement changes that are not Critical or Major IA risks may occur between UCR versions, but will not become effective until the next signed version of the UCR unless specifically noted (see disposition 2). Coordination of the requirements that will apply to a product test window to achieve APL status will occur at the Initial Contact Meeting (ICM) and will be based on the scheduled/projected day for the start of testing. If a UCR version is published during an interoperability test window, the requirements that apply to a product will be determined at the ICM and will be limited to Critical or Major IA requirements. If an interoperability test window encompasses the 18 month anniversary of a UCR publication, JITC and NS2 will determine which requirements will result in an informational TDR and require a vendor PoA&M to close the TDR prior to listing on the APL and the vendor will be notified at the ICM (i.e., the vendor does not have to meet the requirement, but must commit to meeting the requirement at a future date).

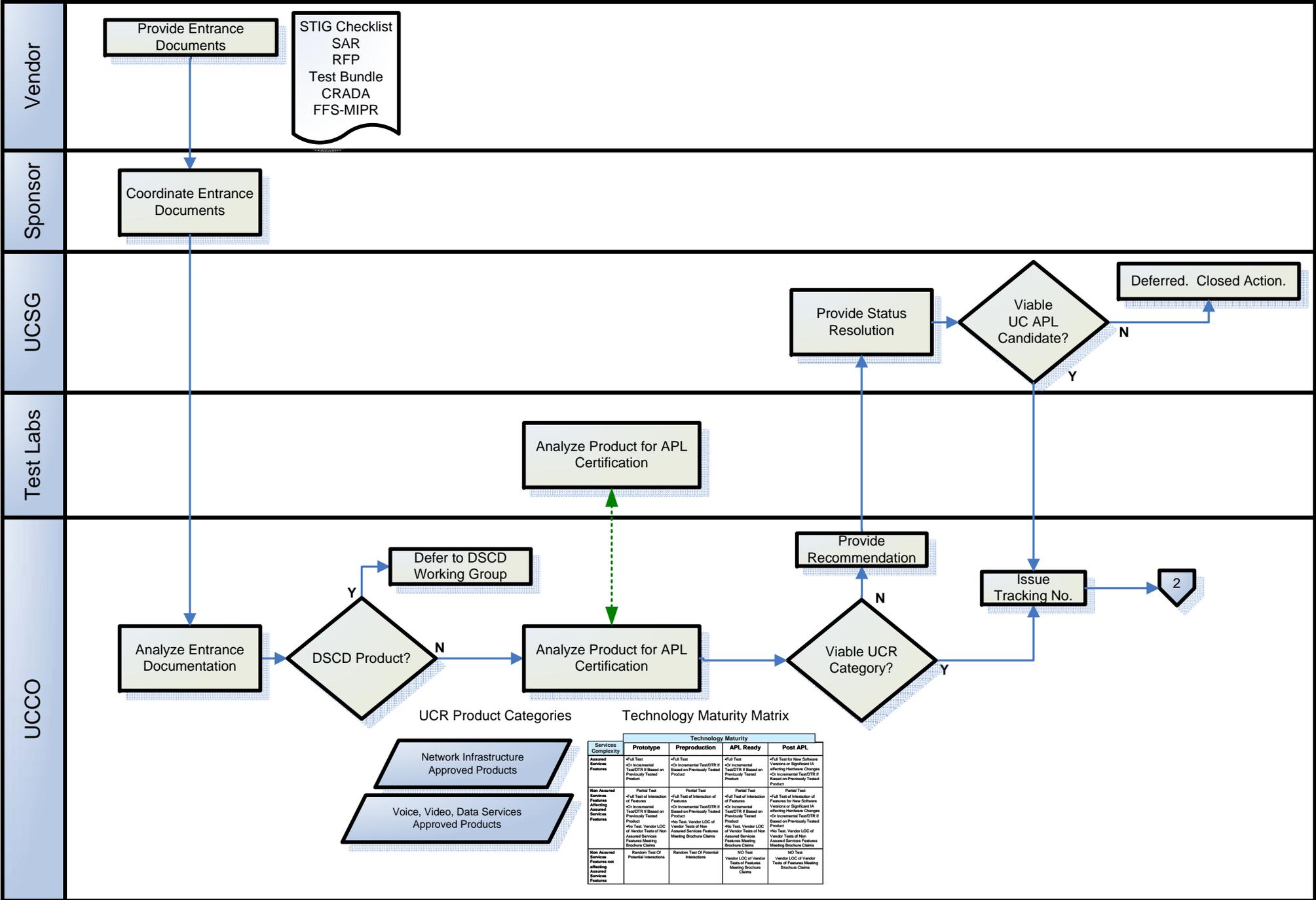
## **APPENDIX G**

The following Appendix is comprised of the UC APL Process Charts. These are provided for reference only and any questions as to interpretation and implementation should be directed to DISA NSP

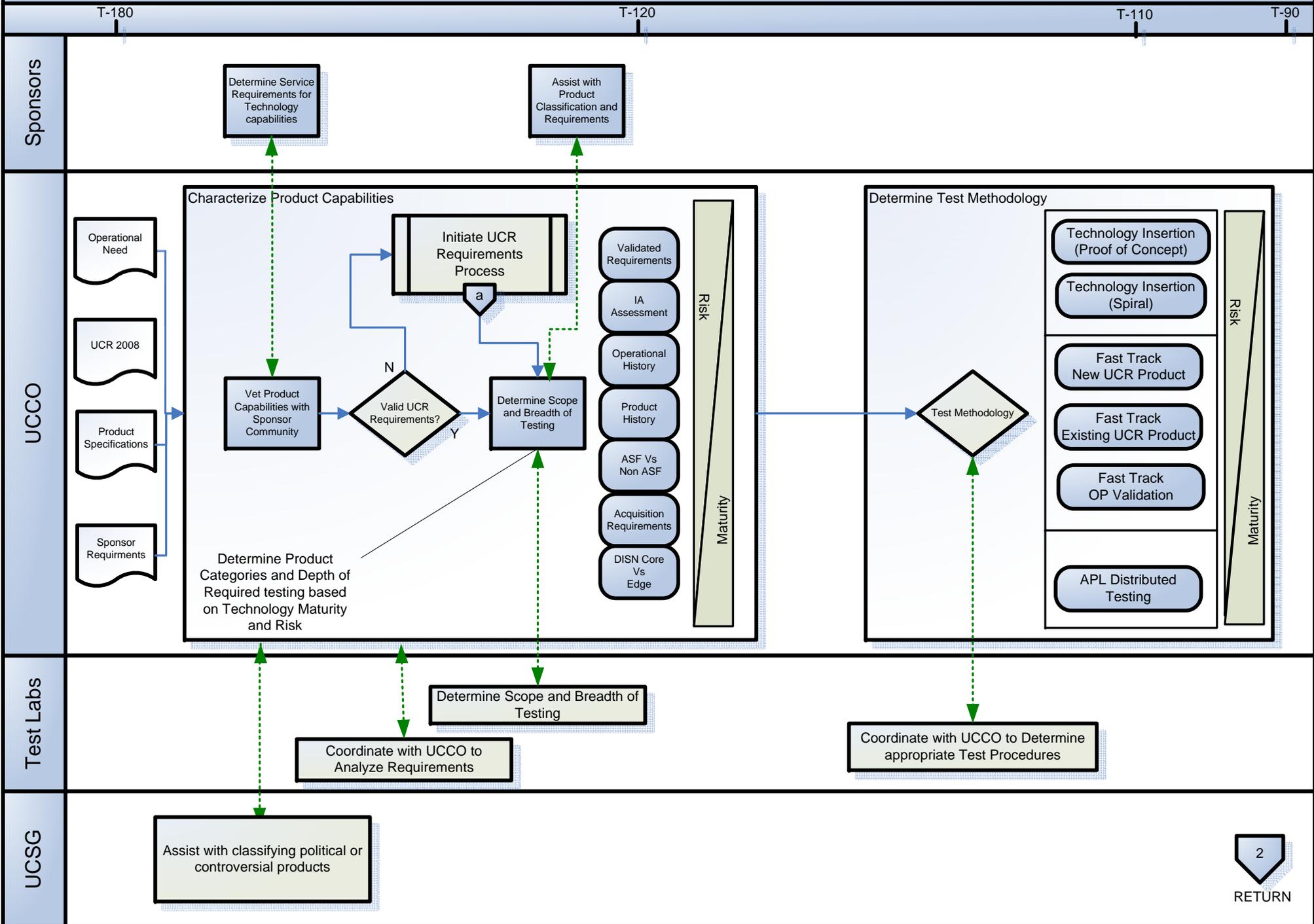
# UC APL Certification and Testing



# (Tab 2) UCCO Initial Screening Meeting

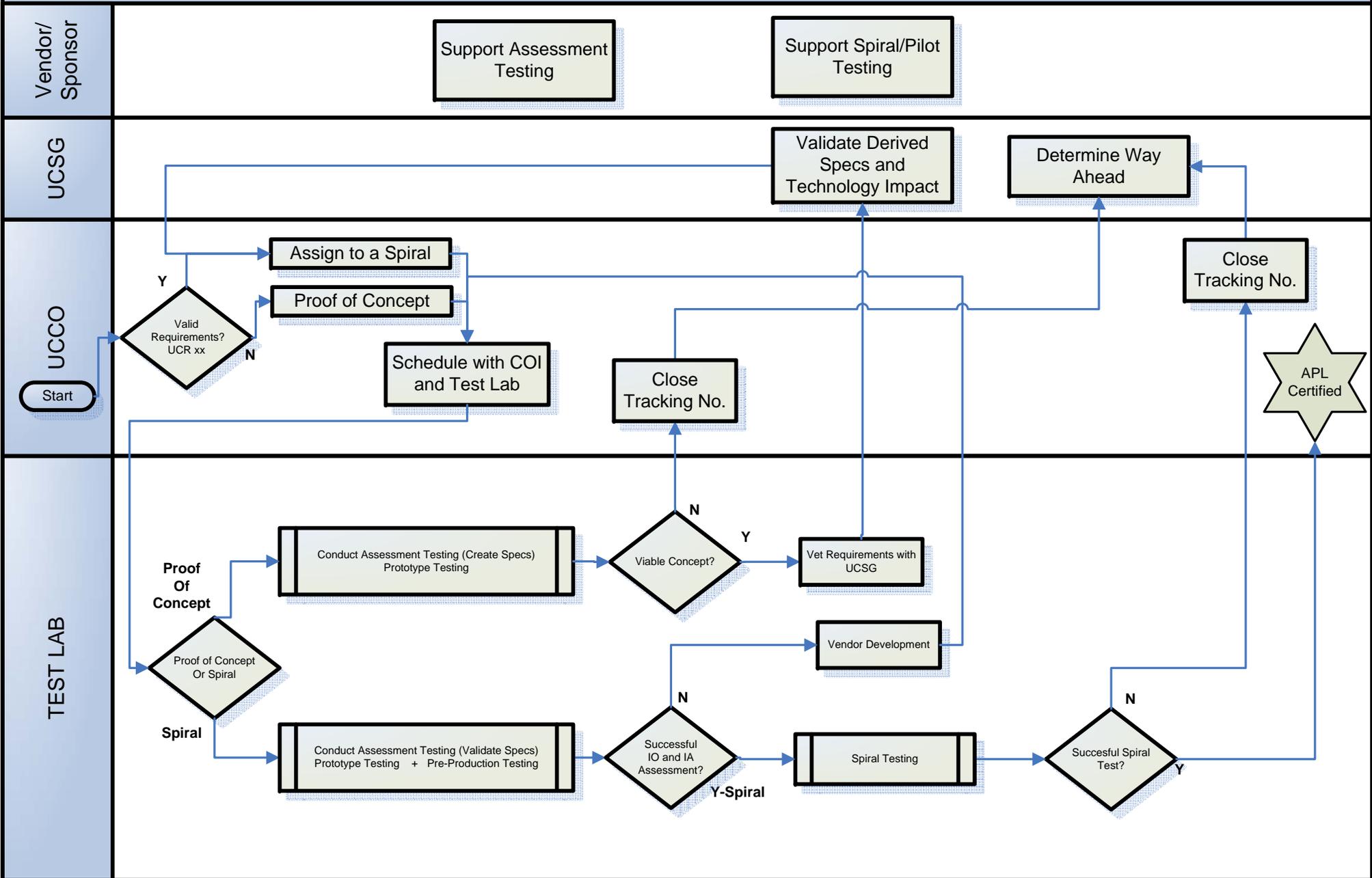


# (Tab 3) Determine Test Methodology



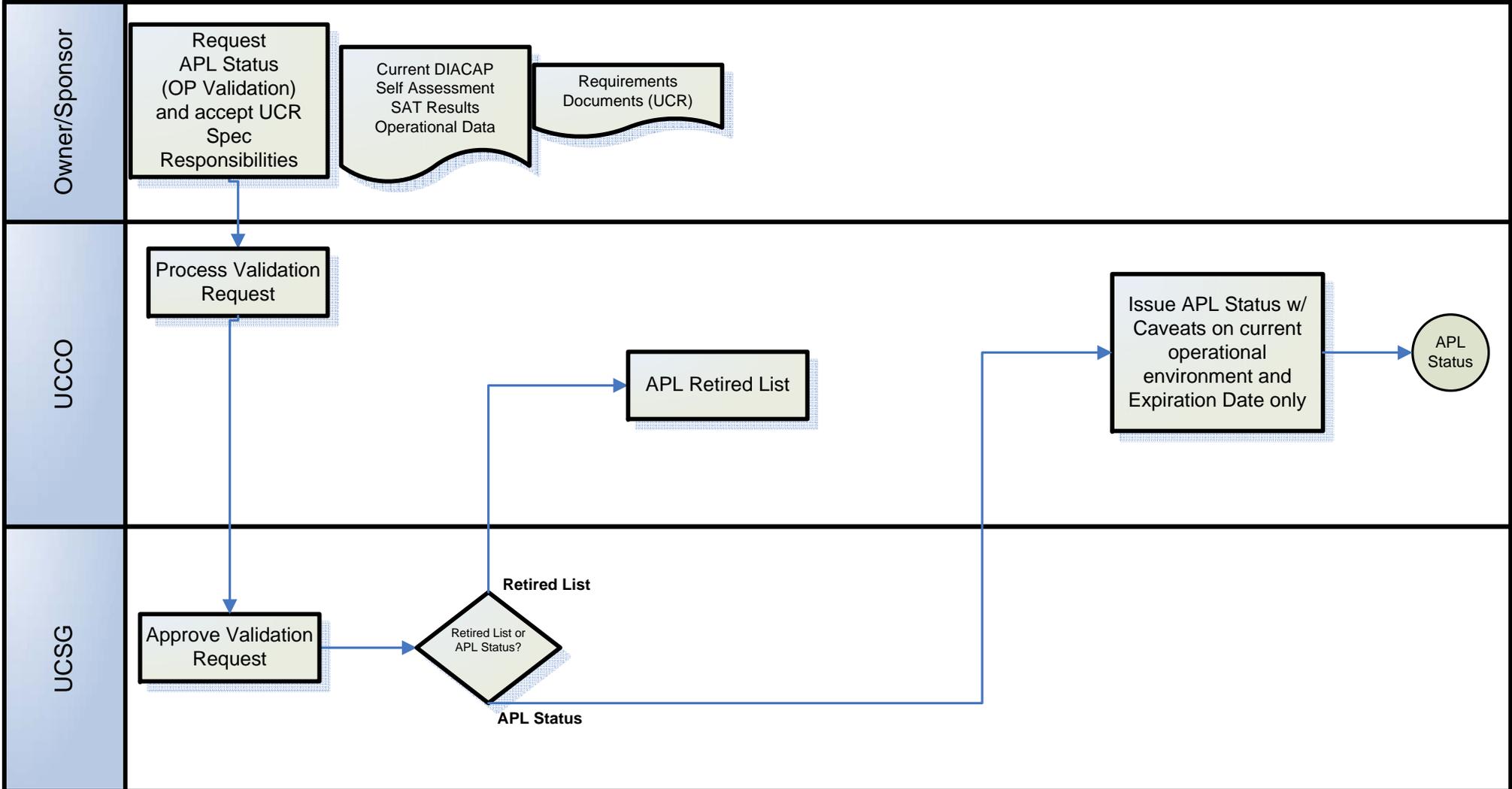
Tab 4 – Technology Insertion - Low Maturity and High Risk Products/Systems

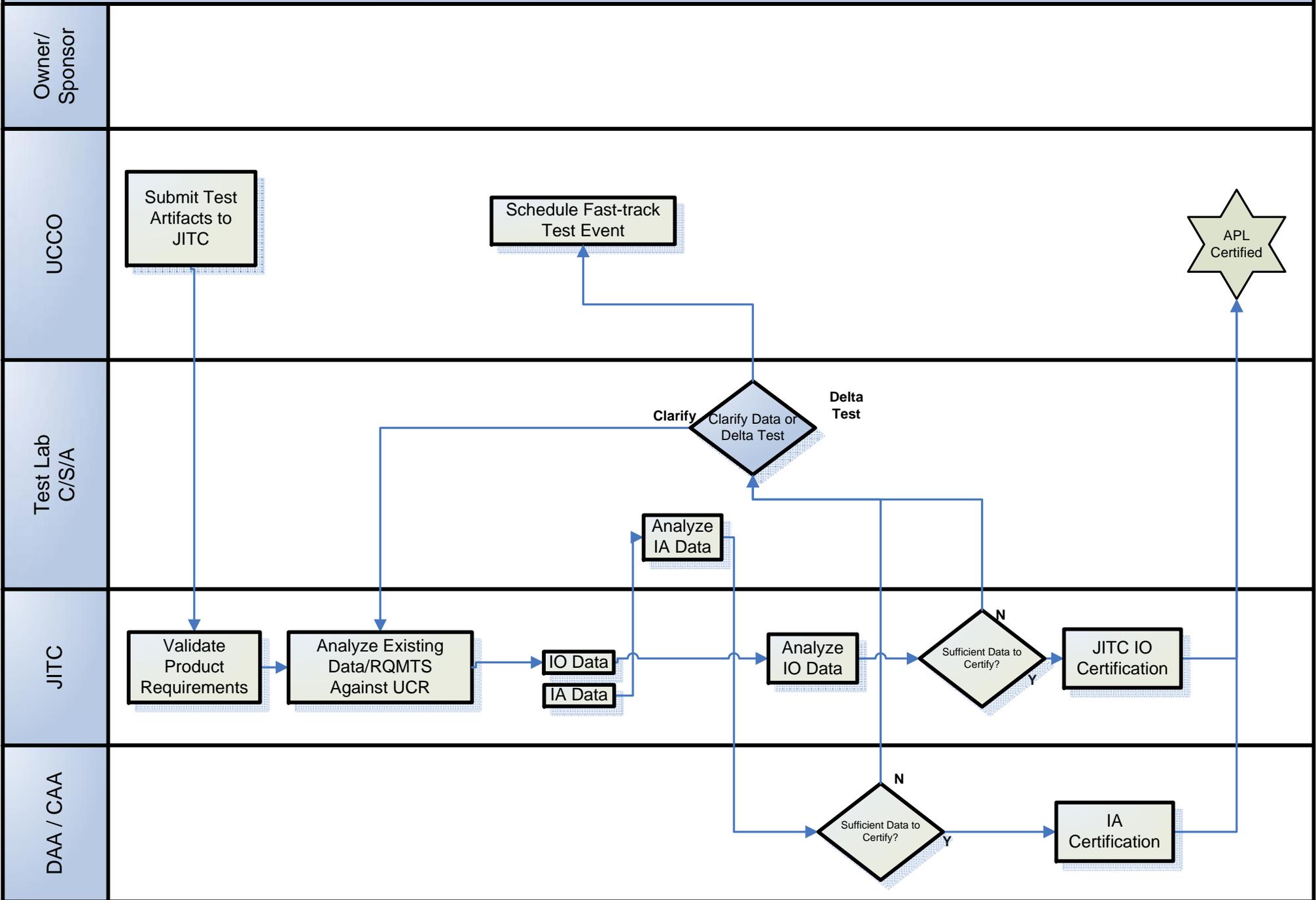
RETURN

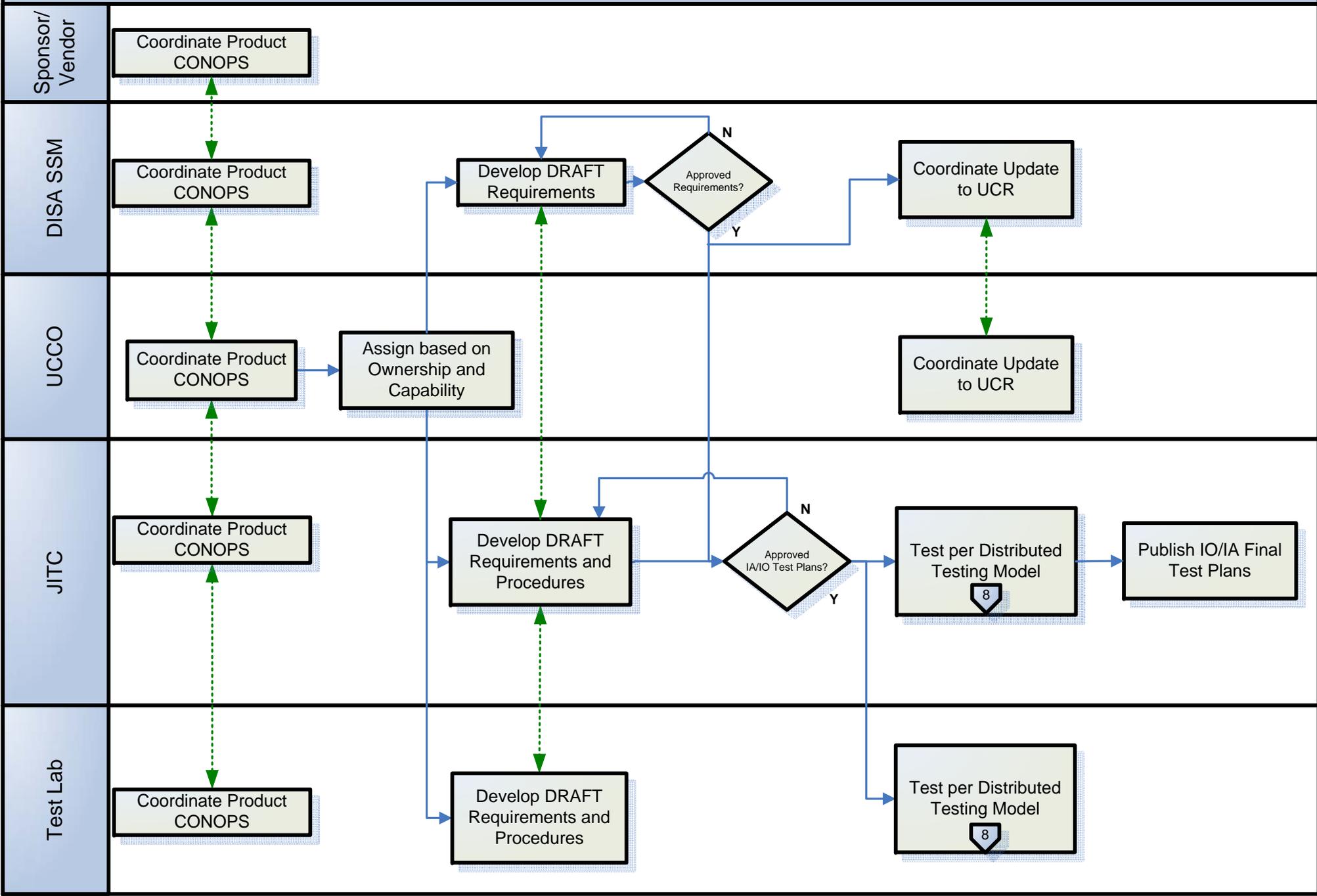


Tab 5 – Fast Track - Operational Validation (Product currently in operation)

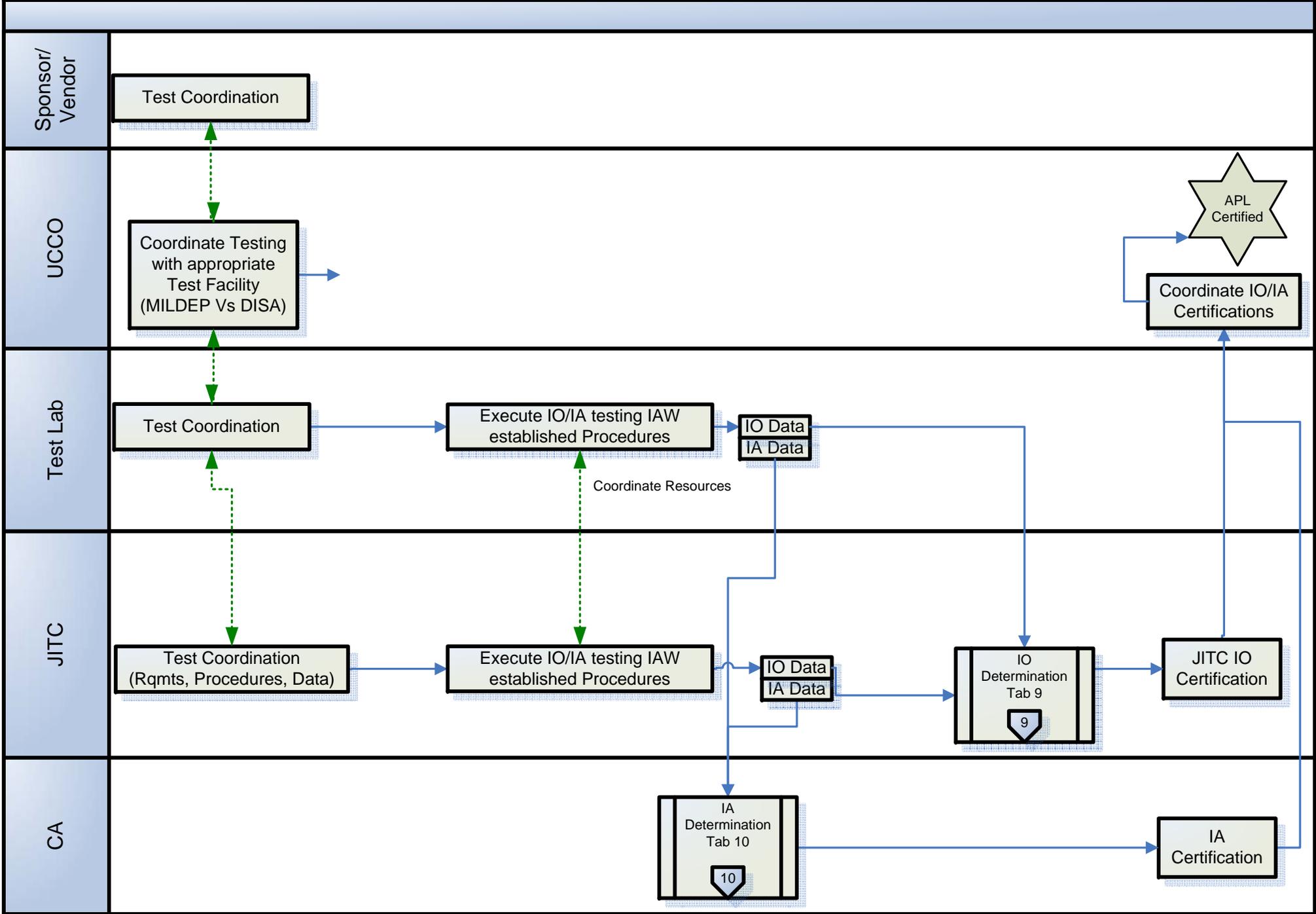
Operational Waivers Approved by UCSG



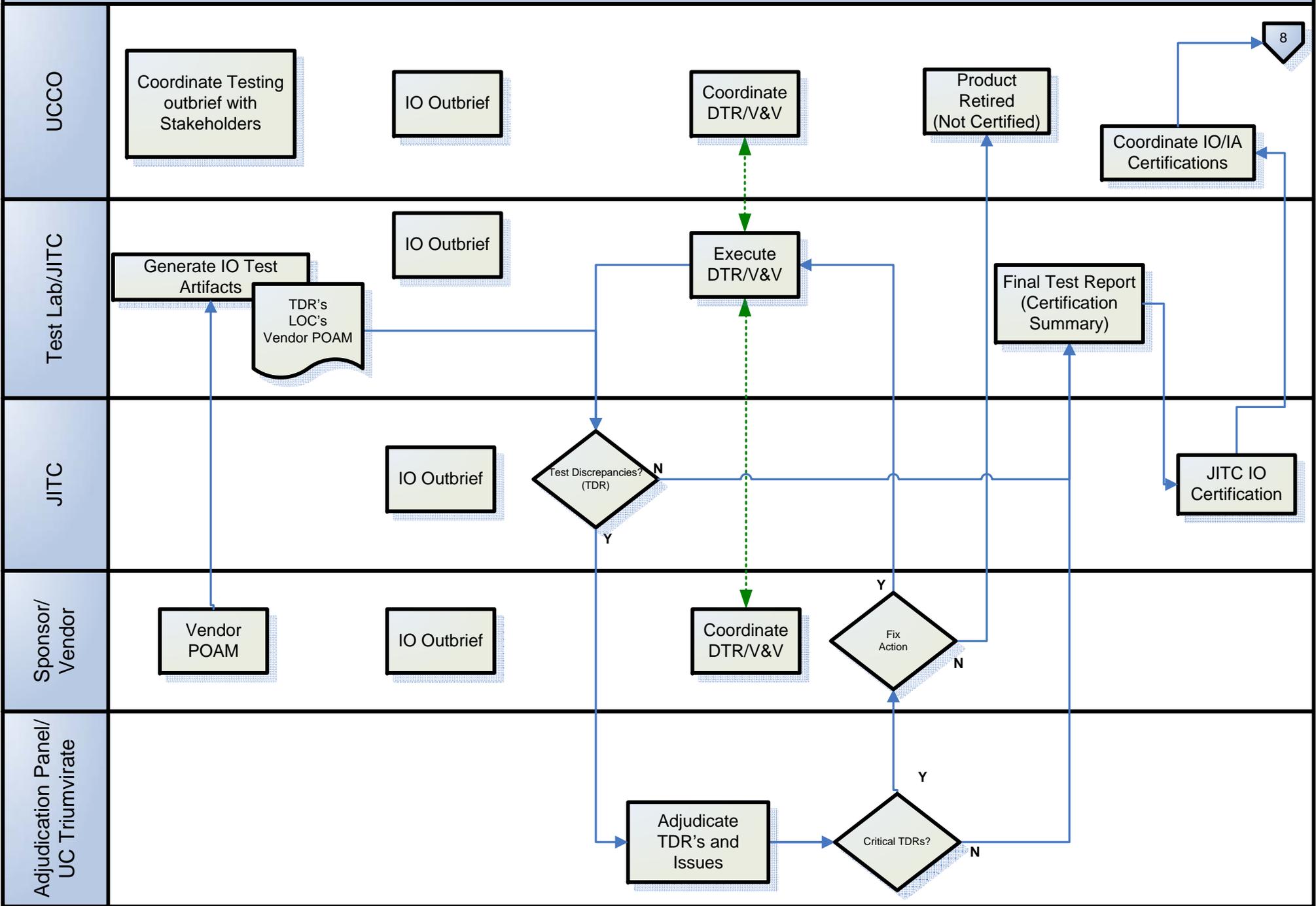




Tab 8 – APL Distributed Testing



Tab 9 – IO Determination



Tab 10 – IA Determination

