DISA

Unified Capabilities

Approved Products List Process Guide for Sponsors, Vendors, and Testing Facilities

May 2011 Version 1.5

TABLE OF CONTENTS

SECTION **PAGE**

Unified Capabilities Approved Products List Process

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

Approval:

SHOWERS.JESSIE.L.JR.1119211235

Digitally signed by SHOWERS.JESSIE.L.JR.1119211235
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=SHOWERS.JESSIE.L.JR.1119211235
Date: 2011.05.20 12:18:51 -04'00'

Jessie L. Showers Jr., Chief, Capabilities Center
DISA, Network Services Directorate

20 May 2011
Date

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) 2 Division's Unified Capabilities Certification Office (UCCO). 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). The UC APL Process provides for an increased level of confidence through Information Assurance (IA) and Interoperability (IO) Certification.

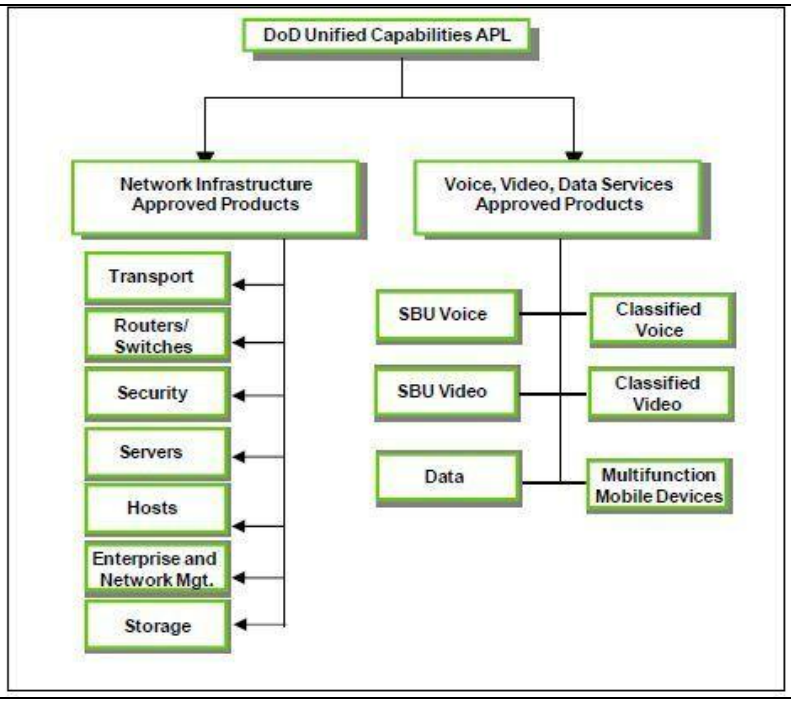
1.2 Purpose

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.

1.3 APL Structure

Figure 1.1 provides an overview of the structure of the UC APL in terms of services and network infrastructure. The various products for each category are found under the respective APL section.

Figure 1.1 Overview of UC APL Product Categories



Legend:

DoD	Department of Defense	SBU	Sensitive But Unclassified
APL	Approved Products List		

2 ROLES AND RESPONSIBILITIES

2.1 Unified Capabilities Certification Office (UCCO)

The UCCO acts as the staff element for DISA NS2 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. As the DoD moves towards a distributed testing environment, the UCCO will be 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 Appendix D.
- 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).

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.
- 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 such as Multifunction Soft Switches (MFSS) will be tested under an equipment Cooperative Research and Development Agreement (CRADA). Edge products such as Assured Service LANs (ASLANs) will be targeted for vendor Fee For Service (FFS). Generally, if an Edge product is sponsored by one of the Military Services, then it will be tested under the FFS cost model. 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 MFSS, Wide Area Network (WAN) SS's, DoD Secure Communications Devices (DSCDs), and any product that DISA NS determines to be part of the DISN core or essential to the DISA transition to end-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. The product will only be listed on the APL if IA and IO certifications are successful. Costs associated with each FFS product can be estimated by reviewing the document entitled "Estimated Test Timeframes for UCR Product Categories" at the URL, http://www.disa.mil/ucco/apl_process.html?panel=1#A_Services "

- 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 Solution Under Test (SUT).
- Attend the ICM and Out-Briefs to discuss test results and provide mitigation strategies and POA&M (if applicable).
- Provide Deployment Guidelines for SUT to UCCO.
- Coordinate all testing activities and logistics with UCCO and government sponsors.
- Assist testing centers in development of test plans and test procedures.

2.4 Testing Labs

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

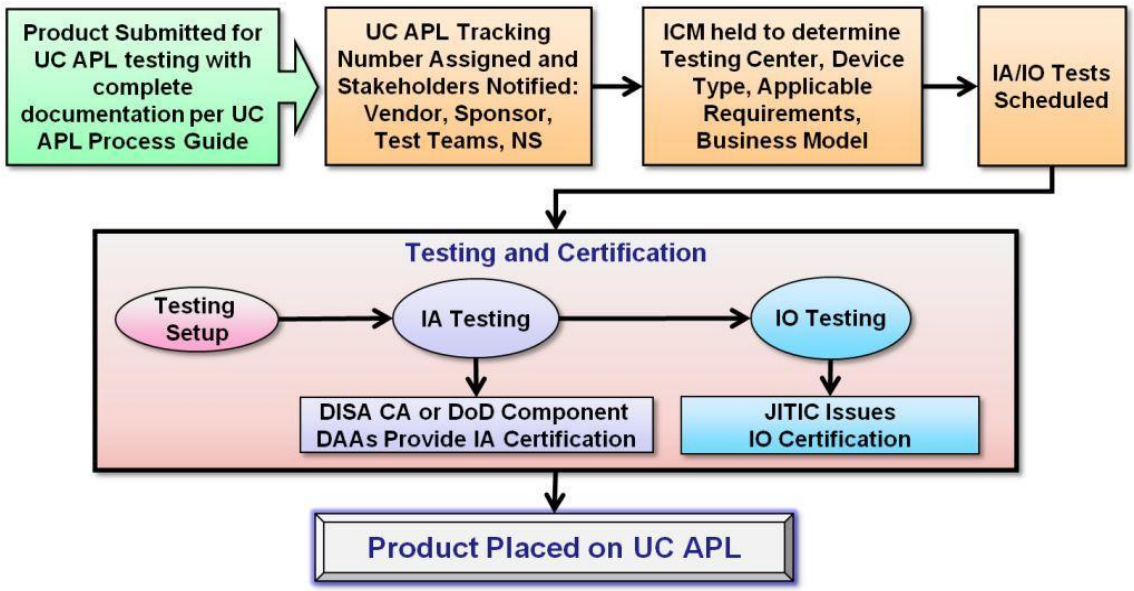
- Attend UC APL scheduling meetings to provide IA and IO testing dates for products that have been assigned for testing.
- Assign an Action Officer (AO) to be the primary testing point of contact for a given tracking number.
- Coordinate with DISA NS on cost model (FFS or equipment CRADA) that will be 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 meeting minutes, findings summary, IA Assessment Report (IAAR), and IO Certification Summary per the timeline guidance in this document and as circumstances allow.

3 STANDARD OPERATING PROCESS FOR UC APL C&A

The standard UC APL process, as identified in the UCR 2008, is shown in **Figure 2**. This process reflects that both IA certification and IO certification are required for placement of products on the UC APL.

Figure 3.1 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://aplits.disa.mil

Note: Product submittal will not be processed until UCCO receives the product documentation package. See Appendix C for a detailed Product Documentation package to include:

- A detailed diagram of the test environment.
- 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. Cards/modules in each chassis listed out in table format, if applicable
- Completed STIG Questionnaire, which is located at http://disa.mil/ucco/webfiles/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 for your appliance (i.e. L3 Switch, Simple Server, UC Host Work Station and etc…).
    - Include the requirements as an attachment and state compliance to the requirements relevant to your profile.
    - Include the nomenclature(s) and respective software release(s) applicable to this submission.
    - Submit the LoC in .pdf format.

Note: Please see Appendix C Section 2.4 for the IPv6 Rules of Engagement for the various products.

- SF 328 Form Certificate Pertaining To Foreign Interests (If Applicable)

Note: Certain UC APL products must be NIAP validated. Please review Section 5.4 (Information Assurance) of the UCR 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 certification decision.

The complete vendor 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 the sponsor:
    a. Is the government sponsor of the submitted product in accordance with DoDI 8100.04.
    b. Agrees to attend the ICM and Out-Brief.
    c. Agrees to the configuration submitted by the vendor.
4. Sponsor approves SUT configuration and verifies contact information.

    Note: Execution of Step 5 is currently in-progress and some solutions may follow the traditional path of the ICM taking place after the scheduling meeting for a certain amount of time.

5. UCCO issues Tracking Number (TN) for complete submissions. UCCO coordinates scheduling of Initial Contact Meeting (ICM). Attendees include: Vendor, Sponsor, applicable DoD Component Lab POCs, CA representative, JITC PoC, and Subject Matter Experts (SME). The outcome of the ICM will be an identified JITC AO, APL Product-type, business model determination, IA/IO requirements, and test location.
6. Assigned Test Lab AO will coordinate business model with vendor.
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.

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 be ready for V&V testing within 20 business days of the request. 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.
14. Vendor has 10 business days to turn in mitigations and POA&Ms for findings reported within the IA Findings Summary. Failure to submit 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 within 10 business days of receiving the IA Findings Mitigations from the Vendor. Required Attendees: Sponsor, Vendor, AO, 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 mitigations and 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 POA&Ms by deadline will result in TN retirement and vendor will need to reinitiate the UC APL Process.

Note: If the Out-Briefing results in no change in numbers of findings but only recommended changes in mitigations and POA&Ms, the Vendor will submit their revisions to NS2 for NS2 to incorporate into the draft IAAR. NS2 will submit the draft IAAR to UCCO and/or CA as the actions requires.

18. IA Test Team submits draft IA Assessment Report (IAAR) to UCCO within 10 business days of receiving vendor's mitigations and Out-Brief action items.
19. UCCO has 3 business days to review the 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 10 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. 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.

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.

23. UCCO receives either product Authority to Operate (ATO)/Interim authority to operate (IATO), product IA Certification Recommendation from CA, or DSAWG approval.
24. UCCO provides JITC AO IA configuration approval (ATO/IATO, CA or DSAWG approval).
25. IO Test Team will coordinate Test Discrepancy Reports (TDRs) with JITC AO during IO test window.
26. IO Test Team will liaise with vendor to get a POA&M for open TDRs remaining at the completion of IO testing.
27. Open TDRs at the completion of testing and vendor submitted POA&Ms will be coordinated with JITC AO for review and validation.
28. DoD Test Lab AO will prepare open TDR synopsis in accordance with prescribed format and staff to DISA NS2 for adjudication. Open TDRs submitted must have a vendor POA&M addressing proposed fix.
29. IO Test Team will coordinate IO Certification Summary with Action Officer. Test facility will staff IO Certification Summary and recommendation to JITC within 10 business days after IO TDRs are successfully adjudicated.

30. JITC has up to 10 business days to staff IO certification and accompanying IO Certification summary. Test events that result in multiple reports (i.e. ASLAN, Wireless, LSC) will be granted an additional two business days.

Note: If IO test fails, the TN will be retired. Vendor will need to reinitiate the UC APL Process. Any Technical Deficiency Reports (TDR) based on failure to meet UCR standards will be adjudicated for severity, and a way-ahead will be provided to the Vendor.

31. Vendor submits the Deployment Guide which reflects the SUT, for review and approval by the NS2 Information Assurance Manager (IAM), prior to the issuance of UC APL Approval Memorandum.
32. UCCO has 3 business days to prepare the UC APL Approval Memorandum and submit to NS2 for signature after receipt of the JITC signed IO Certification Letter. APL listing of the product is for 3 years.
33. UCCO sends UC APL Approval Memorandum to Configuration Control Board (CCB) members, Sponsors, and Vendors.
34. UCCO posts the product on UC APL website: https://aplits.disa.mil
35. From the date of the APL Approval memorandum, UCCO has 10 business days to compile the Information Assurance Assessment Package (IAAP).

Note: The IAAP is stored in APLITS and available for distribution only to government civilian or uniformed military personnel.

36. Exceptions to the above process will be coordinated with DISA NS2 and JITC.

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

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

- Verification and Validation request

The process to update a current SUT is as follows:

1. Vendor submits update / change request(s) via UCCO Website: http://www.disa.mil/ucco/apl_update.html. 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 Guide

For any changes and/or patch updates to a product that is already on the UC APL, including POA&M closure, 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, not new software release. New software release will be submitted as new submissions.

1. Vendor submits product for review via UCCO Website http://www.disa.mil/ucco/apl_update.html. 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 within 5 business days. 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 NS2 for review and coordination with Service Manager, if applicable. NS2 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, the original CA for the product will be contacted in parallel with NS2. This could be the Service CA for products they sponsored or the DISA CA (FSO).
6. JITC updates IO certification letter.
7. Upon receipt of JITC updated IO certification letter, UCCO posts the updated product on the UC APL: https://aplits.disa.mil and updates the IAAP with the DTR information

3.4 UC APL Fast Track (FT) Process

The FT process is intended to expedite products onto the APL. The FT process is structured to deal with the fact that DoD sponsors 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 by Joint Interoperability Test Command (JITC) 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.

- 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., retired APL status) or active (i.e., normal APL status).

- 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**

Acronym	Definition
APL	Approved Products List
CA	Certifying Authority
C & A	Certification and Accreditation
CCB	Configuration Control Board
CRADA	Cooperative Research and Development Agreement
CJCSI	Chairman Joint Chiefs of Staff Instructions
DAA	Designated Accrediting Authority
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DoDI	Department of Defense Department Instruction
DSAWG	Defense IA/Security Accreditation Working Group
DSN	Defense Switched Network
DTR	Desk Top Review
FFS	Fee For Service
FSO	Field Security Operations
ICM	Initial Contact Meeting
IA	Information Assurance
IAAP	Information Assurance Assessment Package
IAAR	Information Assurance Assessment Report
IO	Interoperability
IP	Internet Protocol
JIC	Joint Interoperability Certification
JITC	Joint Interoperability Test Command
JS	Joint Staff
MILDEP	Military Department
NII	Networks and Information Integration
NIPRNet	Unclassified Internet Protocol Router Network
NS	(DISA) Network Services (Directorate)
OSD	Office of Secretary of Defense

Acronym	Definition
OSS	(DISA NS) Operational Support Systems (Division)
POC	Point of Contact
RTS	Real Time Services
SAR	Self Assessment Report
STIG	Security Technical Implementation Guide (STIG)
SUT	System Under Test
TN	Tracking Number
UC	Unified Capabilities
UCCO	Unified Capabilities Certification Office
UCR	Unified Capabilities Requirements
USD	Under Secretary of Defense
V&V	Verification and Validation

Appendix B **References**

- Department of Defense (DoD) Unified Capabilities Requirements (UCR) 2008 Change 2, 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 6211.02C, "DISN: Policy and Responsibilities," 9 July 2008
- 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://aplits.disa.mil :

Table C2.1 – Documentation Checklist

Diagram	☐
System description	☐
STIG Questionnaire	☐
IPv6 Letter of Compliance (if applicable)	☐
SF-328 Form (if applicable)	☐
SAR (if applicable)	☐

E-mail: ucco@disa.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.

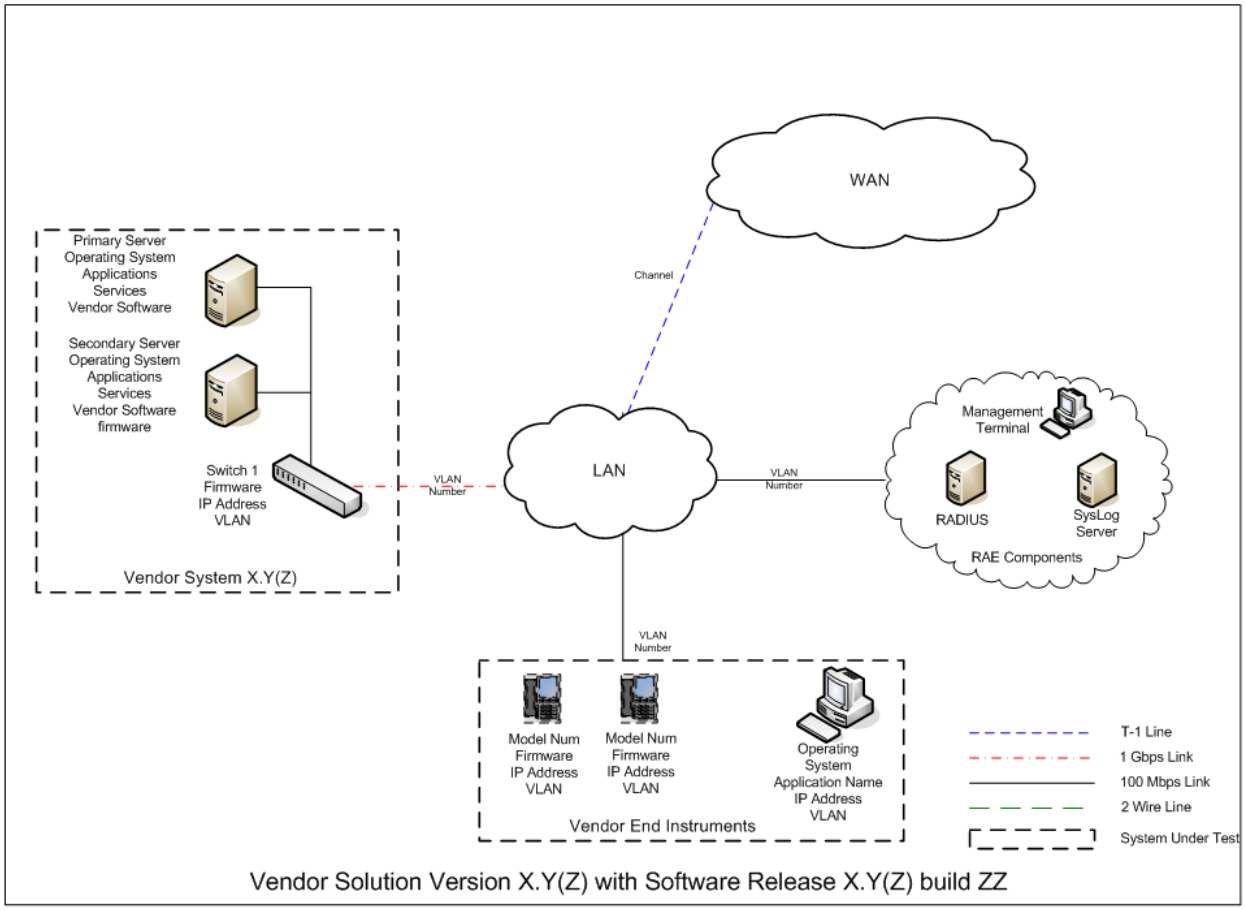


Figure C2.2 – Sample Diagram for Submission

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., Private Branch Exchange (PBX), 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.

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).

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, and
5) IP address.

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://disa.mil/ucco/webfiles/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 (UC) IPv6 RULES OF ENGAGEMENT (ROE)

1) Detailed IPv6 requirements for UC products and/or functions are provided in section 5.3.5-1 of UCR 2008 Change 2. Table 2.10 provides a high level listing of UC product or function, UCR IPv6 profile category, and UCR IPv6 requirements to be considered IPv6 capable.

2) Refer to Table 5.3.5-1 from UCR 2008 Change 2 to determine the applicable IPv6 Profile Category for your specific appliance or product.

Table 5.3.5-1. IPv6 Requirements for UCR 2008 Change 2 Products

UCR 2008 CHANGE 2 PRODUCT	UCR 2008 CHANGE 2 IPv6 REQUIREMENTS [1, 2, 3, 4]
SBU IP Based UC Product	
Multifunction Softswitch (MFSS)	The MFSS/ CCA application in conjunction with the VVoIP EI and MG[5] must be IPv6-capable. (Note: "IPv6-capable is defined in Section 5.3.5.3.2) Other applications within this APL product have a conditional requirement to be IPv6-capable if the IP packets remain internal to the product. Use guidance in UCR 2008 Change 2 Table 5.3.5-4 for NA/SS.
WAN Softswitch (WAN SS)	Must be IPv6-capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Local Session Controller (LSC)	The LSC/CCA application in conjunction with the VVoIP EI and MG[5] must be IPv6-capable. Other applications in the APL product have a conditional requirement to be IPv6-capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Customer Edge Router (CER)	Must be IPv6-capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-5 for Routers.
AS-SIP End Instrument (AEI)	The EI in conjunction with the CCA application must be IPv6-capable. This requirement is applicable for EIs manufactured after January 2009. Softphones and soft videophones have a conditional requirement for IPv6. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Secure End Instrument (SEI)	Same as AEI, above.
XMPP Server/Client	Conditional requirement for IPv6. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
AS-SIP TDM gateway (AS-SIP TDM GW)	If the AS-SIP TDM GW has an IP interface, the AS-SIP TDM GW must be IPv6 capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
AS-SIP IP Gateway (AS-SIP IP GW)	Must be IPv6-capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
LAN Product	
LAN Access Switch	Must be IPv6-capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-6 Part 1 for LAN Access Switch.
LAN Distribution Switch	Must be IPv6-capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-6 Part 2 for L3 Switches
LAN Core Switch	Must be IPv6-capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-6 Part 3 for L3 Switches (Edge Routers).
Wireless LAN Product	
Wireless LAN Access Switch (WLAS)	Must be IPv6-capable Use guidance in UCR 2008 Change 2, Table 5.3.5-6 Part 1 for LAN Access Switch.
Wireless LAN Access Bridge (WAB)	Must be IPv6-capable Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Wireless End Instrument (WEI)	Must be IPv6-capable. Same as AEI, above.
Peripheral Product	
Customer Premise Equipment (CPE)	With exception of EIs, the CPE have a conditional requirement for IPv6 capability. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Video Teleconferencing Unit (VTU) hardware only	If the VTU has an IP interface, the VTU must be IPv6-capable. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.

UCR 2008 CHANGE 2 PRODUCT	UCR 2008 CHANGE 2 IPv6 REQUIREMENTS [1, 2, 3, 4]
Integrated Access Switch (IAS)	Conditional requirement for IPv6. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
H.323 Gateway (GW)	Conditional requirement for H.323 IPv6. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
H.323 Gatekeeper (GK)	Conditional requirement for H.323 IPv6. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
Multi Signaling Multipoint Control Unit (MSMCU)	MSMCU must be IPv6-capable. MSMCU is considered a DISN core asset. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
DoD Secure Communications Device (DSCD)	Same as SEI, above except for those DSCD supported by a VoIP switch per Note 4 below
Conference Bridge (CB) external	Conditional requirement for IPv6. CB is considered a MILDEP level asset where the traffic stayed internal to the MILDEP. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
UC External Adjunct Devices	UC External Adjunct Devices that are not covered under CPE (such as an Lightweight Directory Access Protocol (LDAP) server, local directory services server) are to be covered under DoD IPv6 Profile for Net App or Simple Server. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
Network Monitoring for IPv6 data/voice networks	Must be IPv6 capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Instant Messaging, Chat, and Presence/Awareness Features	Conditional requirement for IPv6. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
RTS (Lightweight Directory Access Protocol—LDAP) Routing Database Server	Must be IPv6-capable. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
Network Infrastructure Products	
Multiservice Provisioning Platform (MSPP)	If the MSPP has an IP interface, the MSPP must be IPv6 capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Optical Cross Connect (ODXC)	If the ODXC has an IP interface, the ODXC must be IPv6 capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Provider Router/Provider Edge Router (P/PE Router)	If the P/PE Router has an IP interface, the P/PE Router must be IPv6 capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-5 for Router.
DISN Optical Transport Switch (OTS)	If the OTS has an IP interface, the OTS must be IPv6 capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Tactical UC Product	
Deployable Network Element (D-NE)	Must be IPv6-capable. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
Deployable LAN Products (DLAN)	Must be IPv6-capable. Use guidance from LAN Products, above,
Deployed Tactical Radio (DTR)	Must be IPv6-capable. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
Deployable Cellular Voice Exchange (DCVX)	Must be IPv6-capable. Use guidance in UCR 2008 Change 2,Table 5.3.5-4 for NA/SS.
Multifunction Mobile Devices	
Smartphone	Conditional requirement for IPv6. Use guidance in UCR 2008 Change 2,Table 5.3.5-3 for EI.
Security Devices (SDs)	
High Assurance IP Encryptor (HAIPE)	Must be IPv6 capable. Use guidance in DOD IPv6 Profile version 5.0 Appendix C for IA Devices.

UCR 2008 CHANGE 2 PRODUCT	UCR 2008 CHANGE 2 IPv6 REQUIREMENTS [1, 2, 3, 4]
Link Encryptor Family (LEF)	Must be IPv6 capable. Use guidance in DOD IPv6 Profile version 5.0 Appendix C for IA Devices.
Edge Boundary Controller (EBC)	Must be IPv6 capable. Use guidance in UCR 2008 Change 2,Table 5.3.5-7 for EBC.
Firewall (FW)	Must be IPv6 capable. Use guidance in DOD IPv6 Profile version 5.0 Appendix C for IA Devices.
Intrusion Protection System (IPS) and Intrusion Detection System (IDS)	Must be IPv6 capable and must be capable of inspecting IPv4 and IPv6 packets simultaneously and those packets contained within tunnels that are not encrypted (GRE, IPSec AH, IP in IP, etc.) or shall support the capability to alarm if tunneled packets are detected that could not be inspected further. Use guidance in DOD IPv6 Profile version 5.0 Appendix C for IA Devices.
Virtual Private Network Concentrator (VPN)	Must be IPv6 capable. Use guidance in DOD IPv6 Profile version 5.0 Appendix C for IA Devices.
Network Access Control (NAC)	Must be IPv6 capable. Use guidance in DOD IPv6 Profile version 5.0 Appendix C for IA Devices.
Integrated Security Solution (ISS)	Must be IPv6-capable. Use guidance in DOD IPv6 Profile version 5.0 Appendix C for IA Devices.
Storage Devices	
Storage Devices	Conditional requirement for IPv6. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Network Elements	
Assured Services Network Element (AS-NE)	Must be IPv6 capable. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
DSN Fixed Network Element (F-NE)	Conditional requirement for IPv6. Use guidance in UCR 2008 Change 2, Table 5.3.5-4 for NA/SS.
Classified Products	
Classified Local Session Controller (LSC)	Same as LSC, above.
Classified Core Router	Same as LAN Core Router above.
Classified Distribution Switch	Same as LAN Distribution Switch above.
Classified Access Switch	Same as LAN Access Switch above
Classified Edge Boundary Controller (EBC)	Same as EBC, above.
Classified Customer Edge Router (CER)	Same as CER, above.
Legacy Systems	
MFS/Tandem Switch, EO Switch, SMEO, DVX, PBX1 and PBX2.	IPv6 ROE for legacy systems are spelled out in the Interim IPv6 ROE for UCR 2008 Change 2, Change 1 at the UCCO web site http://www.disa.mil/ucco/apl_process.html.

UCR 2008 CHANGE 2 PRODUCT	UCR 2008 CHANGE 2 IPv6 REQUIREMENTS [1, 2, 3, 4]

1 The terms "Conditional requirement for IPv6" and "Other applications within the APL product have a conditional requirement to be IPv6-capable" effectively mean that the IPv6-capable features for the indicated UCR IPv6 application is optional and not required for listing on the UC APL.

2. For each product, guidance is provided for (1) mandatory or conditional IPv6-capable and (2) if the IPv6 requirements from UCR 2008 Change 2, or from DOD IPv6 Profile Version 5.0 are to be used.

3. While there is a requirement to manage IPv6 networks, the NM may be done using IPv4. Thus, NM is not included in this list.

4. For the cases where components are within the UC products and the IP packets remain internal to the System Under Test (SUT) without using the DISN WAN, (i.e. the external interface for the SUT for signaling traffic and bearer traffic are TDM/serial and IP is only used for external network management) the internal interfaces for the SUT are not required to be IPv6 and the product would not have to support IPv6 at this time. These components provide services as described in Section 5.3.2.24 *Requirements for Supporting AS-SIP-Based Ethernet Interfaces for Voicemail, Unified Messaging Systems, and Automated Receiving Devices.* The resulting UC product can only be fielded within a B/P/C/S boundary.

   This guidance would apply for both generic AS-SIP End Instruments (EIs) and proprietary protocol EIs. The EIs are required to be IPv6-capable regardless of placement within the SUT as indicated in this table, except for IP based DoD Secure Communication Devices (DSCD) supported by a VoIP capable switch that connects to the DISN TDM backbone for voice/data services. The UC APL listing shall reflect conditions under which the product was certified.

5. The MG is only required to be IPv6-capable if it has an external IP interface to the SUT. In these cases, the resulting product can only be fielded within a B/P/C/S boundary. The UC APL certification shall reflect conditions under which the product was certified.

3) If your appliance or product requires IPv6 compliance, submit a signed (Letter of Compliance (LoC) cover letter with company logo with attachments which include the respective IPv6 category for your appliance (i.e. L3 Switch, Simple Server, UC Host Work Station and etc…). http://disa.mil/ucco/webfiles/apl_process/IPv6_Template.xls

   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 IPv6 compliance letter in .pdf format.

4) In accordance with the UCR 2008 Change 2, systems are required to have IPv6 capability for testing. Products that have been placed on the DoD UC APL as a result of vendor commitments, via LoC, to be IPv6 capable will be removed from the UC APL if the vendor does not deliver on the commitment within 12 months of the LoC.

2.5 SF-328 FORM CERTIFICATE PERTAINING TO FOREIGN INTERESTS

Product in the following categories will need to submit a SF-328 Form prior to listing on the UC APL :

- Security Devices
- Multifunction Mobile Devices
- Wireless Equipment
- Enterprise Network Management

Please contact the UCCO (ucco@disa.mil) for a copy of the form

3 POST TRACKING NUMBER DOCUMENTATION

1) Self-Assessment Report (SAR), and

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 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/ucco/apl_process.html 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.*
- 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. 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.

Information provided as part of an acceptable vendor Deployment Guide should fall under one of the following categories of deployment information:

- Screen shots,
- Device configuration files,
- Conditions of Fielding, Mitigations and POA&Ms,
- Reference table to specific portions of a solution's User Guide that provides information on addressing a specific issue, and
- Vendor configuration details/release notes 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

Introduction

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

Background

All vendors, who wish to have their product(s) listed on the Approved Product List (APL), must comply with DoDI 8510.01 instruction, DoD Information Assurance Certification and Accreditation Process (DIACAP), dated November 28, 2007.

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.

Guidance

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 days 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 Enclosure 3 paragraph E3.4 reinforces this requirement by stating: "An IT Security POA&M is required for any accreditation decision that requires corrective action and is also used to document Non-Compliant (NC) and Not-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 POA & M also. For further information on POA&Ms see Enclosure 3 of DoDI 8510.01.

Examples:

Appendix D - Mitigations, POA&Ms, Comments and Format

The following three 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 (2): Vendor Network Controller A, Vendor Network Controller B.
Mitigated by RAE: NO
Vendor Mitigation: This finding will be mitigated by implementing a modification to the httpd.conf StartServers directive. The value will be changed to 12.
Vendor POA&M: The vendor will implement the modification by MM/DD/YYYY.
Vendor Comment: As a condition of fielding, the vendor WLAN controllers should be deployed in a secured room/closet with access limited to only authorized, administrative staff. Also, network access to the controllers should be limited to specific administrative IP address/VLANS. A SYSLOG server should be configured to log all access to the controller and commands issued against the controller. This is documented in the Vendor Deployment Guide.

Note: In the above example, the mitigation is to change to httpd.conf StartServers directive and set the value to 12 which is within the recommended guidelines. The POA&M provides a date that the change will be implemented and is in a MM/DD/YYYY format.

VULID/STIGID: VMS ID: V0014671/PDI: NET0813
Requirement: The Information Assurance Officer (IAO) will ensure all received and sent messages between Network Time Protocol (NTP) peers are authenticated.
Finding: The vendor does not currently support authenticated messages between NTP peers.
Vulnerability: Since NTP is used to ensure accurate log file timestamp information, NTP could pose a security risk if a malicious user were able to falsify NTP information. Implementing the Secure Hash Algorithm (SHA)-1 or PKI between NTP peers can mitigate this risk. Where SHA-1 or PKI cannot be deployed, use Message Digest 5 (MD5) or Data Encryption Standard - Cipher Block Chaining (DES-CBC). When authentication is enforced, there is a greater level of assurance that NTP updates are from a trusted source.
Components Affected (2): Vendor Network Controller A, Vendor Network Controller B.

Mitigated by RAE: NO
Vendor Mitigation: The vendor will address this requirement through the implementation of NTP peer authentication. By adding this functionality, all peers will be authenticated and thereby mitigating the potential vulnerability of a peer or another controller from providing false NTP information.
Vendor POA&M: The vendor will implement this feature by MM/DD/YYYY.
Vendor Comment: As a condition of fielding, a firewall policy should be applied to the configured network ports to limit NTP traffic to a specified server while denying all other NTP communication. This is documented in the Vendor Deployment Guide.

Note: In the above example, the mitigation is to add NTP peer authentication to the vendor's product. The POA&M states that the vendor will implement the feature by MM/DD/YY.

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. Following is an example.

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, IPV, 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.

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 90/60/30 day-out 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.

Appendix E – JITC Fee For Service Rules of Engagement

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.

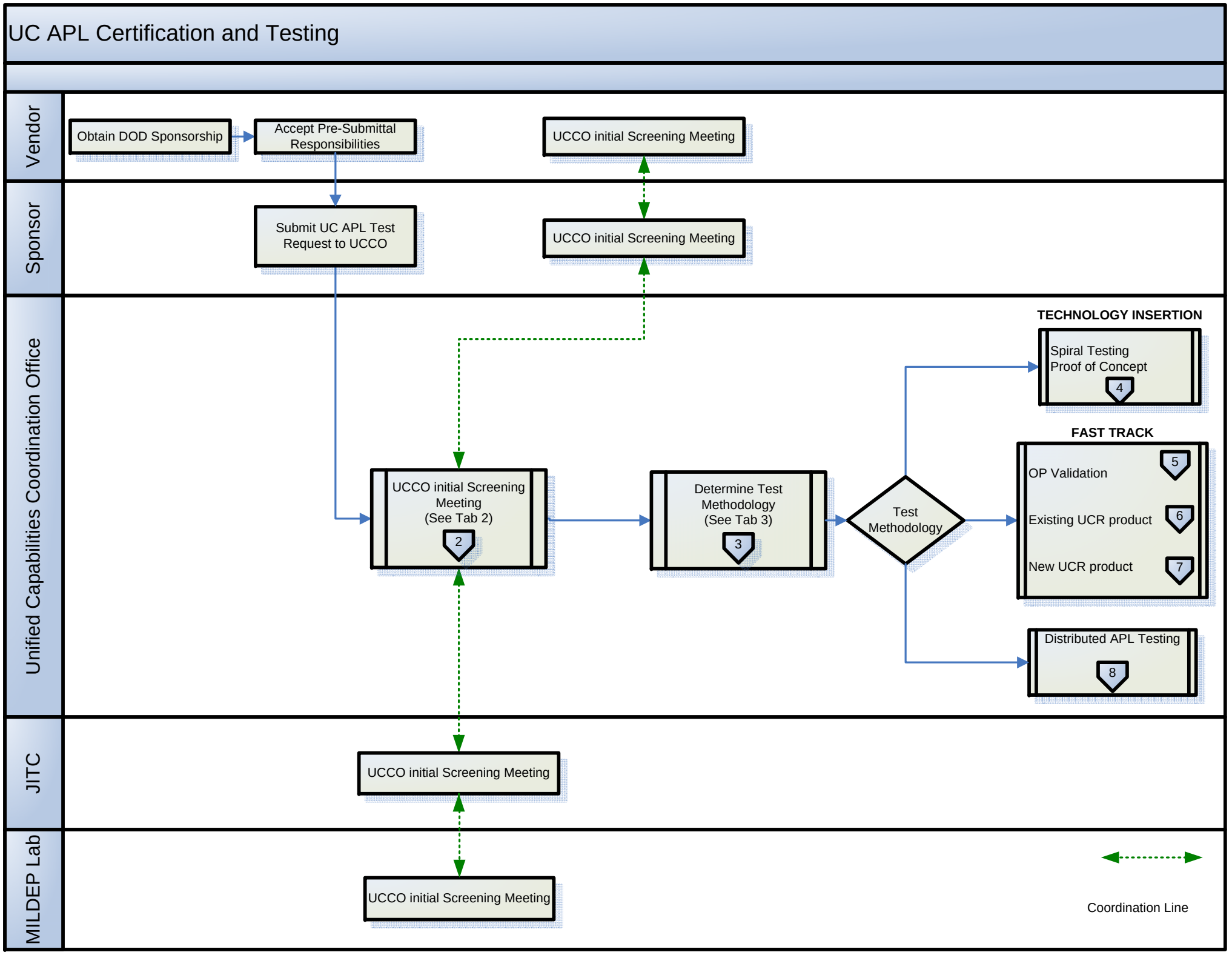
*Government labor is estimated to be approximately 15% of contractor costs.

Appendix E – JITC Fee For Service Rules of Engagement

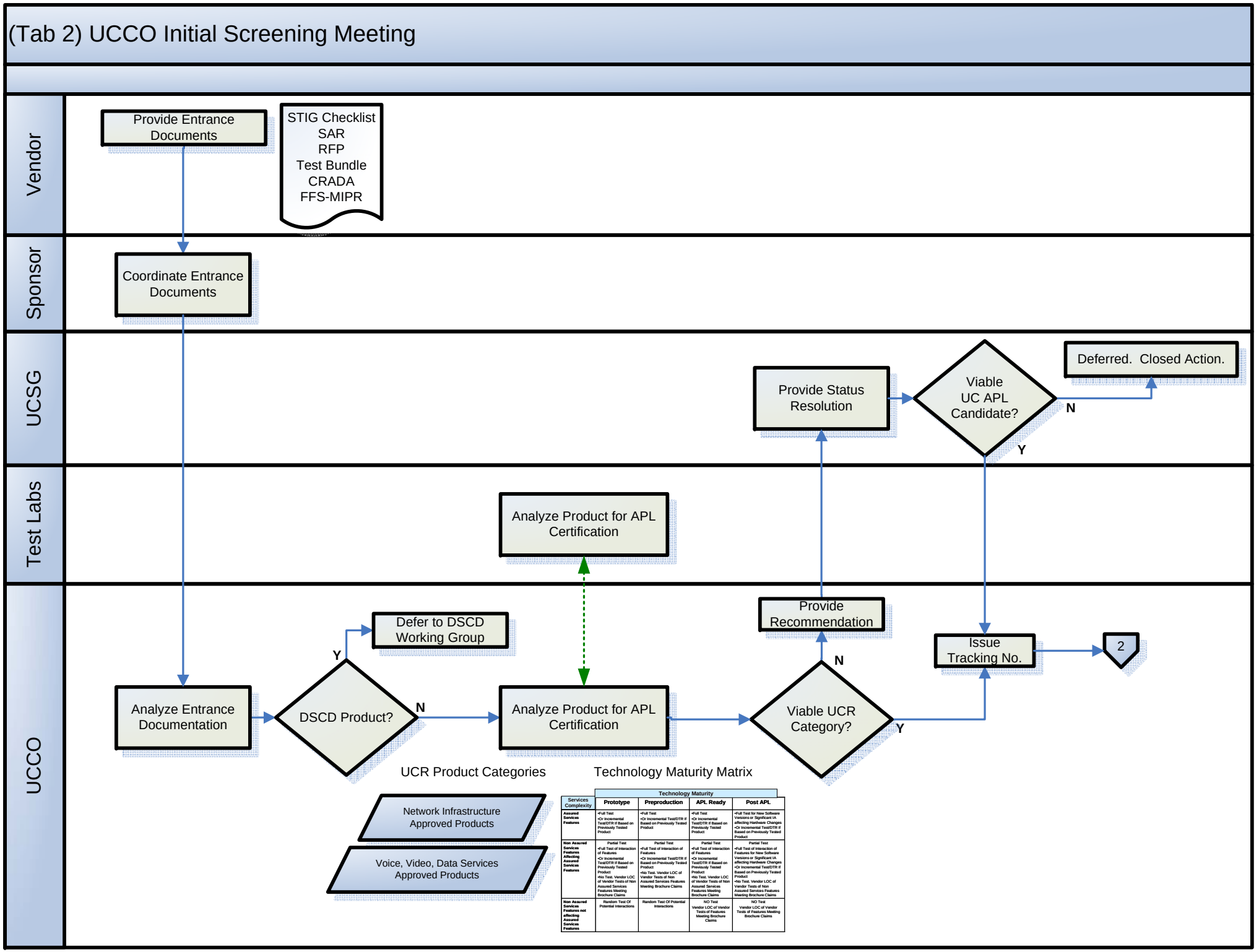
**Contractor labor is based on estimated test timeframe. Test timeframe for each product category in the UCR can be found at following URL, http://www.disa.mil/ucco/apl_process.html, APL products test timeframes. Each product category has a maximum, intermediate, and minimum test window, one of which 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 – UC APL Process Charts

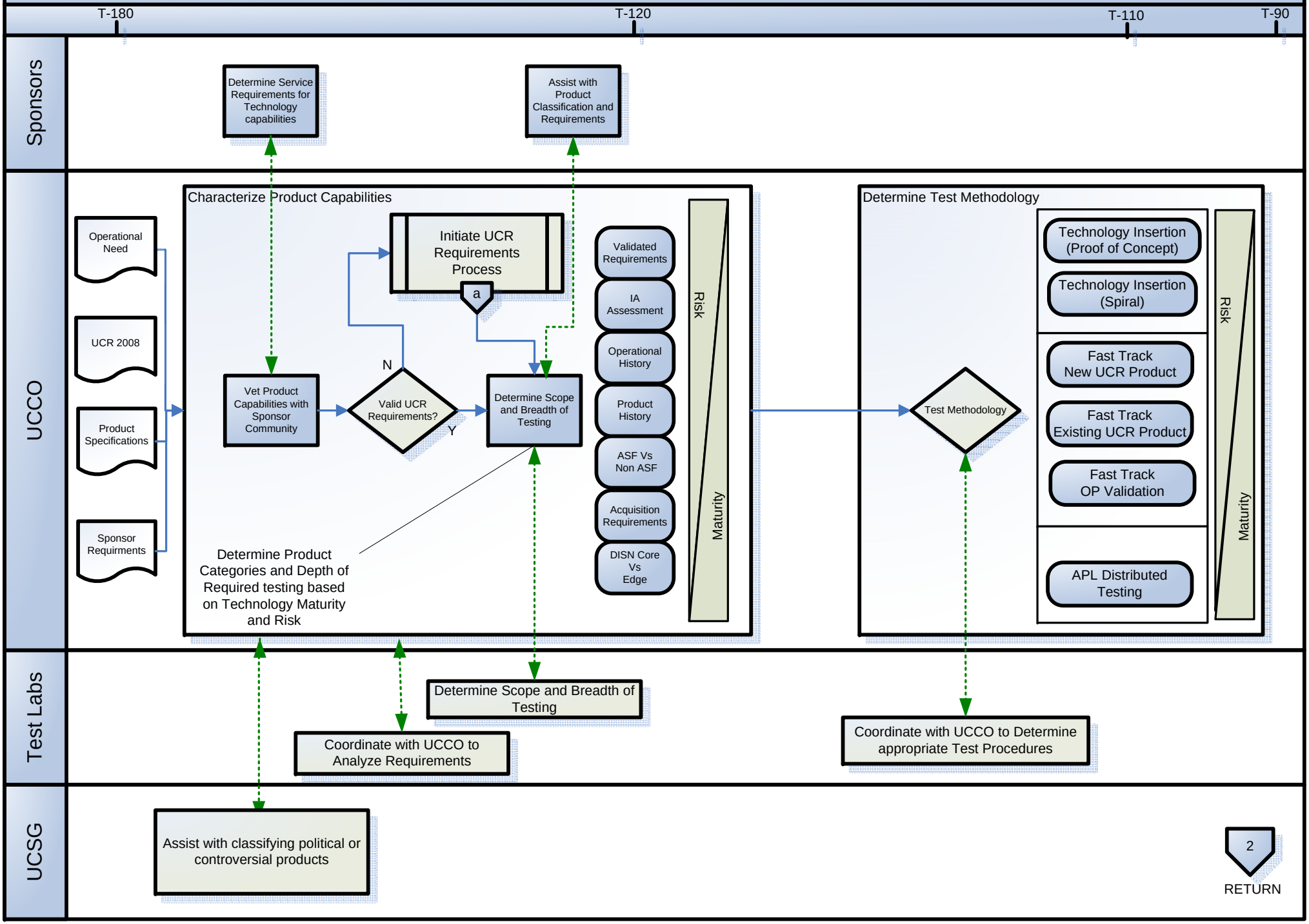
The following Appendix is comprised of the UC APL Process Charts. These are provided for reference only and any questions as to interpretation and implementation should be directed to DISA NS2 ucco@disa.mil.


UC APL Certification and Testing
Vendor
Sponsor
Unified Capabilities Coordination Office
JITC
MILDEP Lab
Obtain DOD Sponsorship
Accept Pre-Submittal Responsibilities
Submit UC APL Test Request to UCCO
UCCO initial Screening Meeting
UCCO initial Screening Meeting
UCCO initial Screening Meeting (See Tab 2)
2
Determine Test Methodology (See Tab 3)
3
Test Methodology
TECHNOLOGY INSERTION
Spiral Testing Proof of Concept
4
FAST TRACK
OP Validation
5
Existing UCR product
6
New UCR product
7
Distributed APL Testing
8
UCCO initial Screening Meeting
UCCO initial Screening Meeting
Coordination Line

(Tab 2) UCCO Initial Screening Meeting



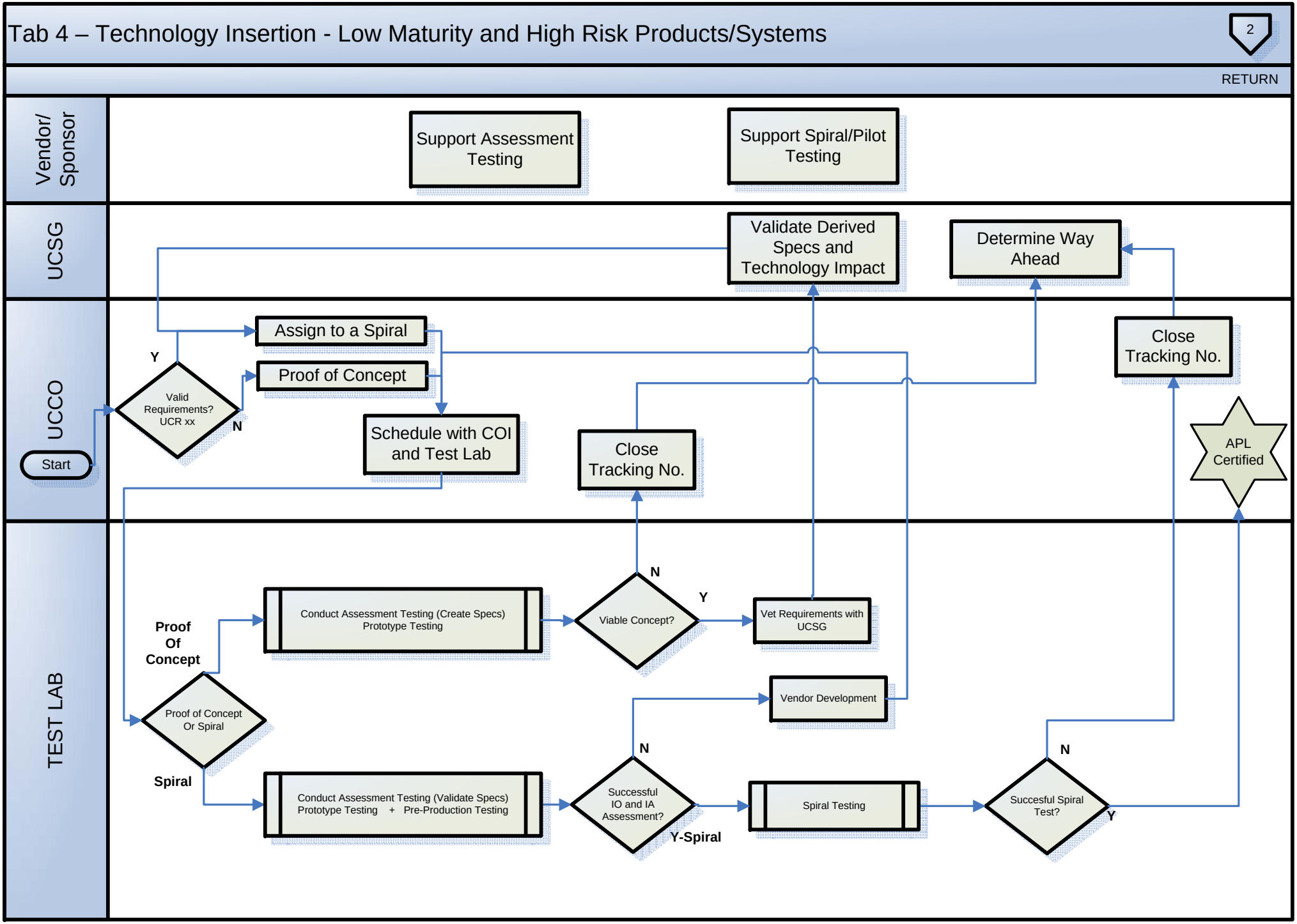
(Tab 3) Determine Test Methodology



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

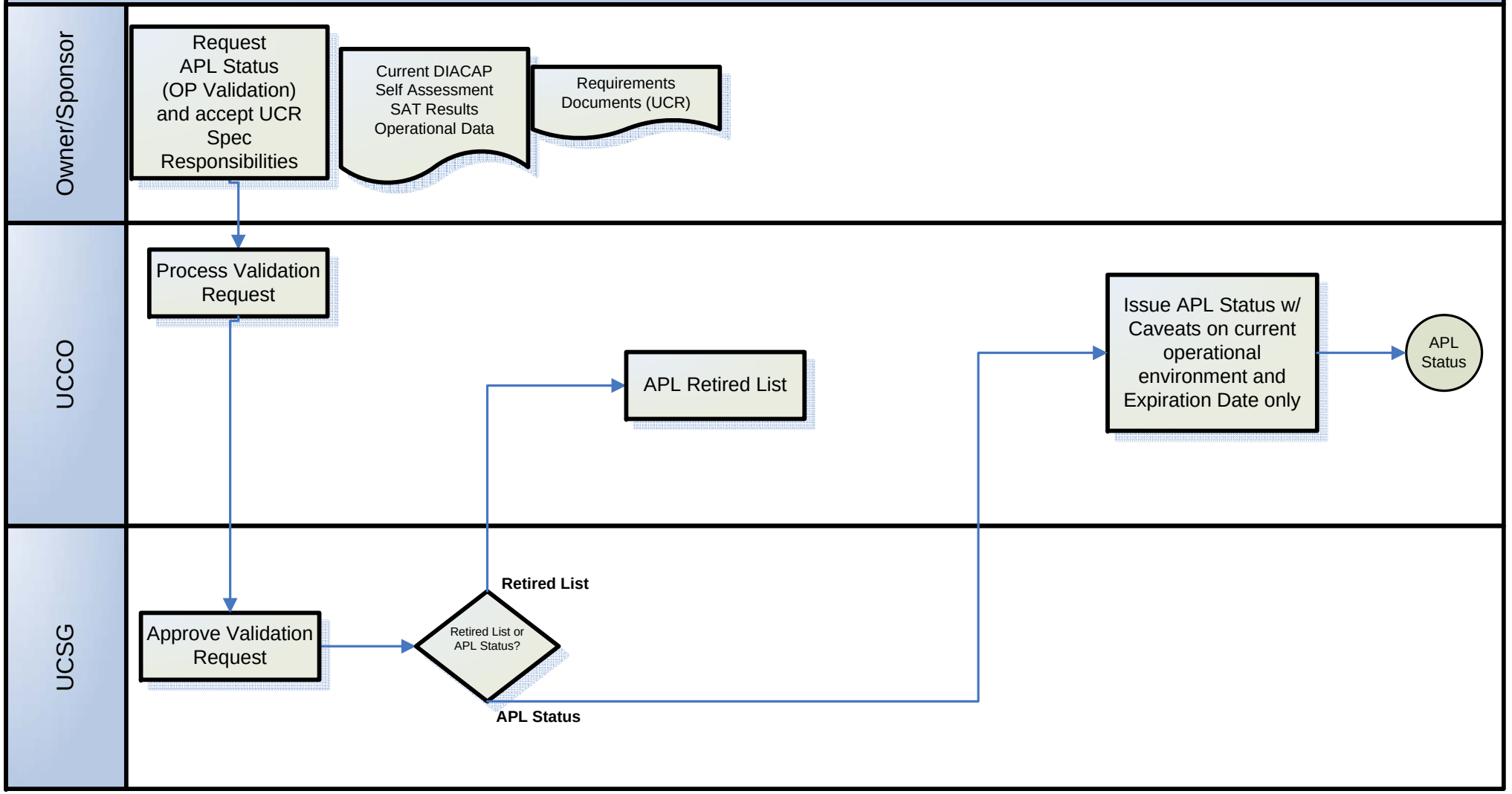
2

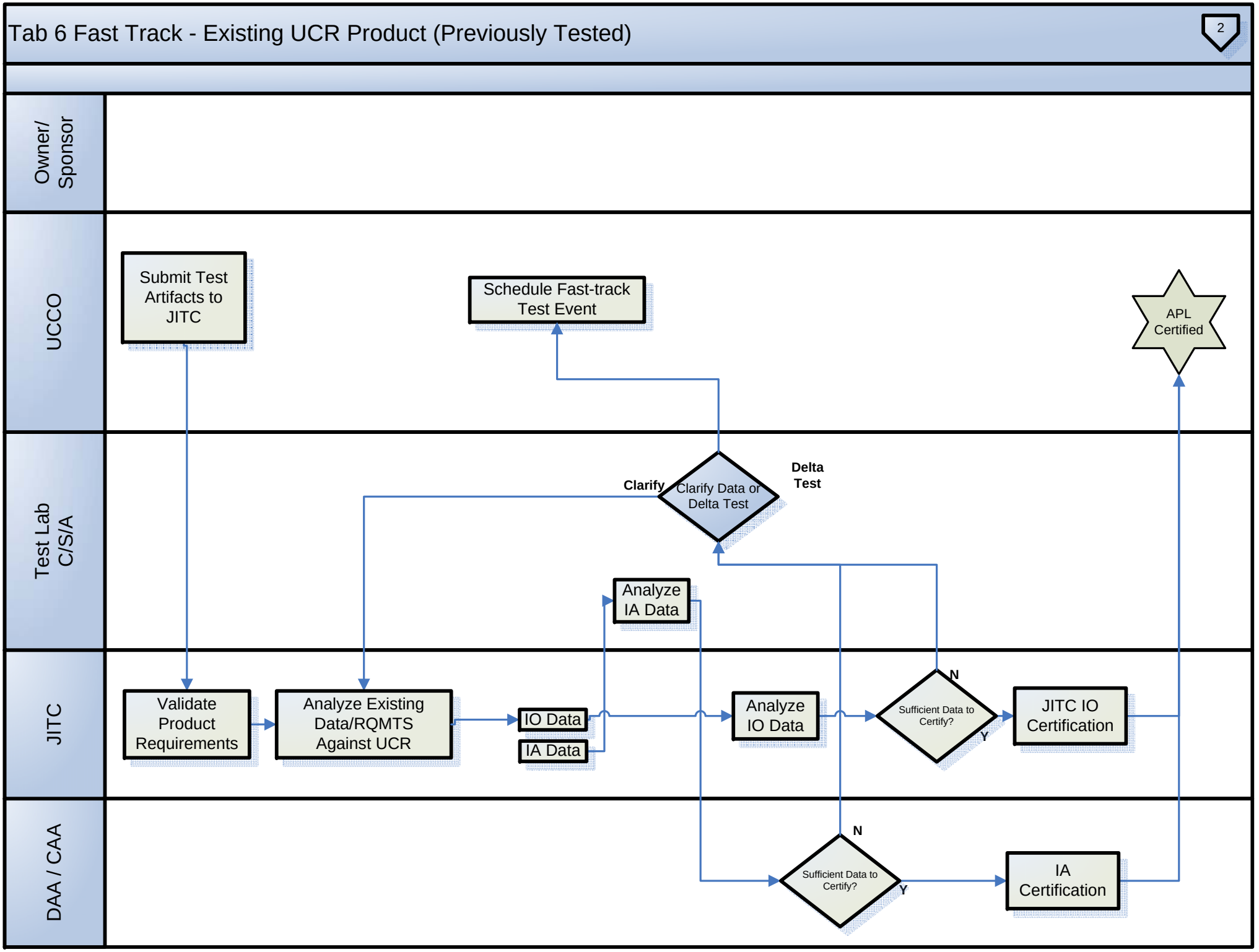
RETURN

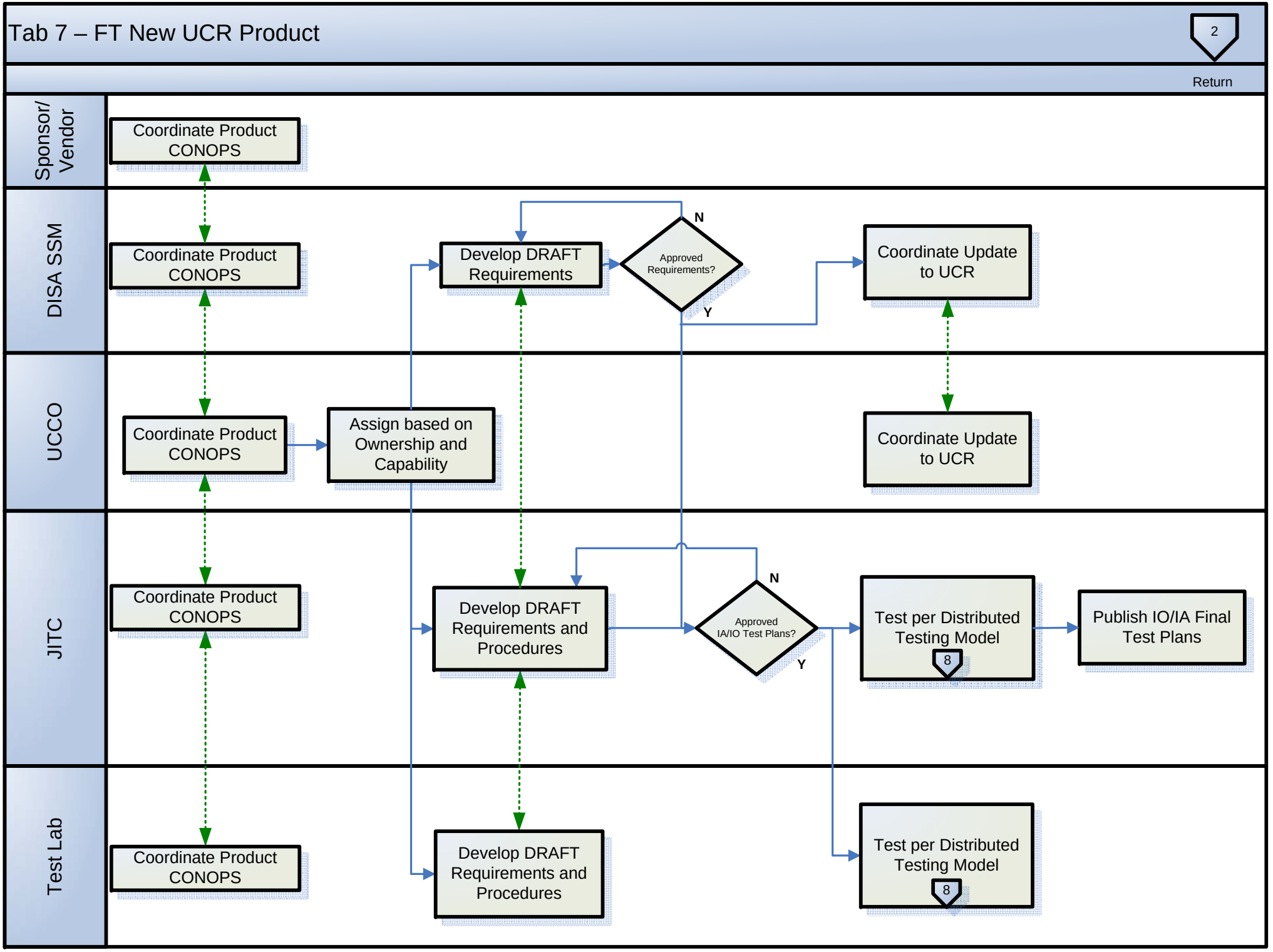


Tab 5 – Fast Track - Operational Validation (Product currently in operation)

Operational Waivers Approved by UCSG

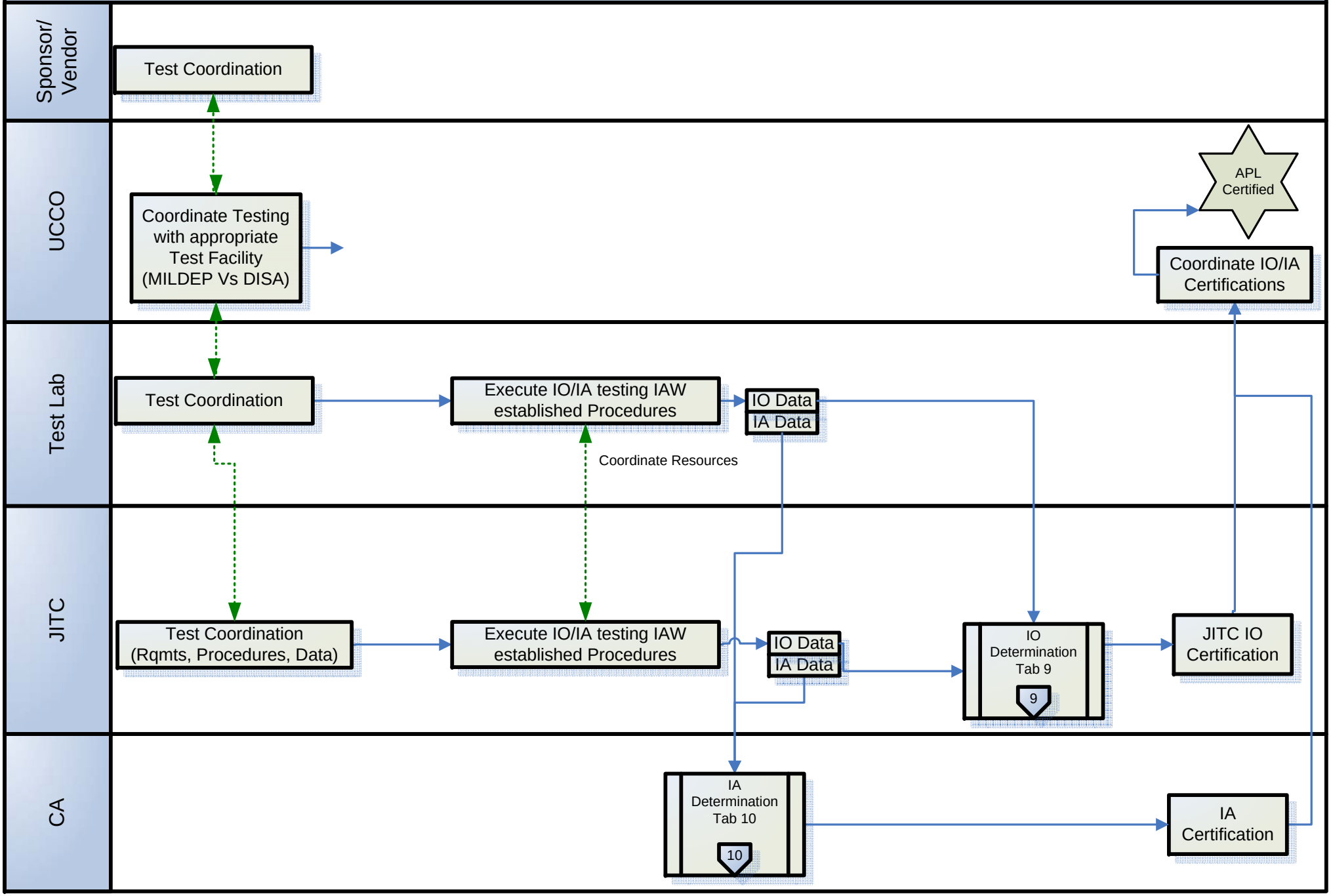


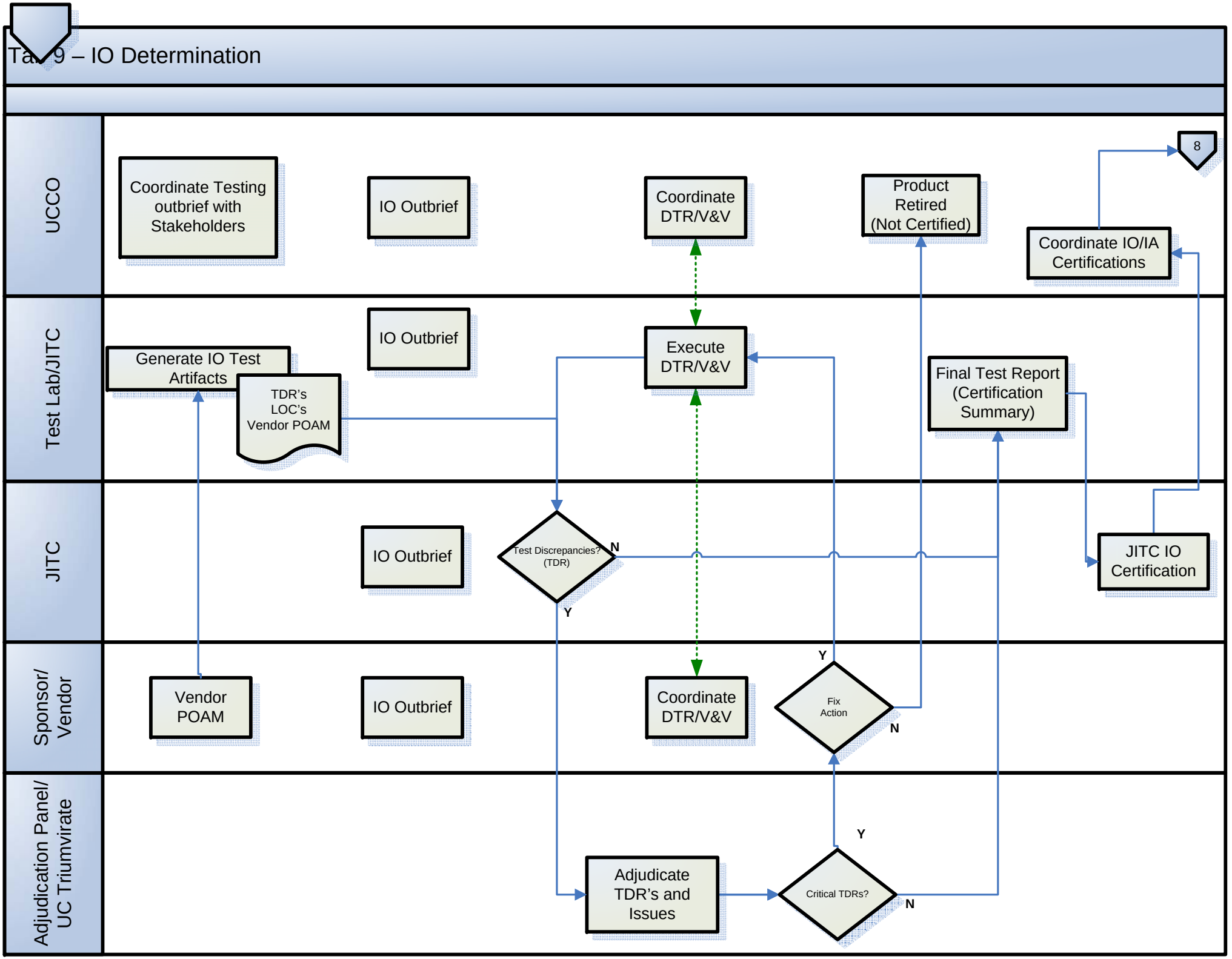

Tab 6 Fast Track - Existing UCR Product (Previously Tested)
2
Owner/ Sponsor
UCCO
Test Lab C/S/A
JITC
DAA / CAA
Submit Test Artifacts to JITC
Schedule Fast-track Test Event
APL Certified
Clarify
Clarify Data or Delta Test
Delta Test
Analyze IA Data
Validate Product Requirements
Analyze Existing Data/RQMTS Against UCR
IO Data
IA Data
Analyze IO Data
N
Sufficient Data to Certify?
Y
JITC IO Certification
N
Sufficient Data to Certify?
Y
IA Certification

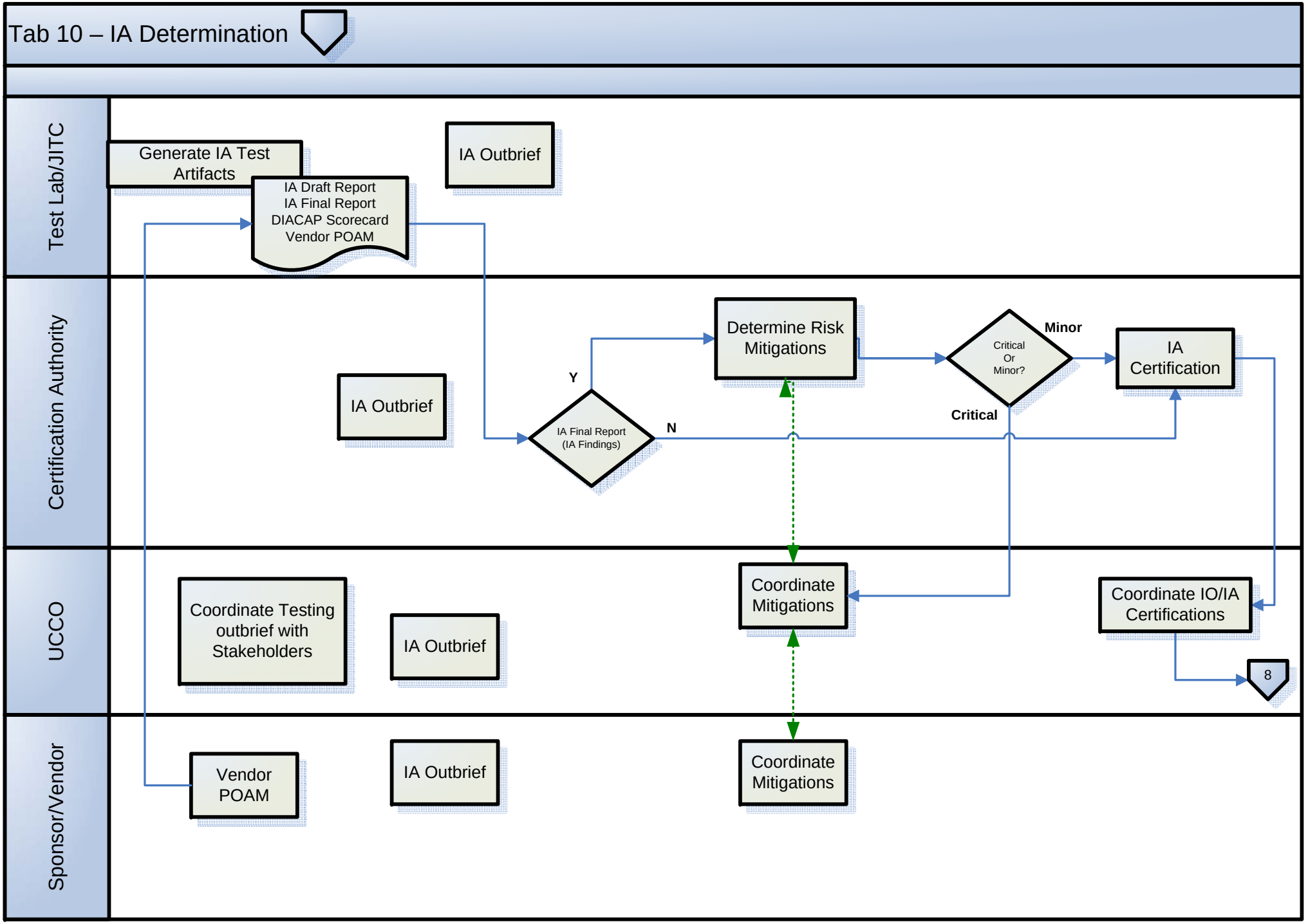

Tab 7 – FT New UCR Product
2
Return
Sponsor/ Vendor
DISA SSM
UCCO
JITC
Test Lab
Coordinate Product CONOPS
Coordinate Product CONOPS
Develop DRAFT Requirements
Approved Requirements?
N
Y
Coordinate Update to UCR
Coordinate Product CONOPS
Assign based on Ownership and Capability
Coordinate Update to UCR
Coordinate Product CONOPS
Develop DRAFT Requirements and Procedures
Approved IA/IO Test Plans?
N
Y
Test per Distributed Testing Model
8
Publish IO/IA Final Test Plans
Coordinate Product CONOPS
Develop DRAFT Requirements and Procedures
Test per Distributed Testing Model
8

Tab 8 – APL Distributed Testing

8 8 8




Task 9 – IO Determination
UCCO
Test Lab/JITC
JITC
Sponsor/ Vendor
Adjudication Panel/ UC Triumvirate
Coordinate Testing outbrief with Stakeholders
IO Outbrief
Coordinate DTR/V&V
Product Retired (Not Certified)
8
Coordinate IO/IA Certifications
IO Outbrief
Execute DTR/V&V
Generate IO Test Artifacts
TDR's LOC's Vendor POAM
Final Test Report (Certification Summary)
IO Outbrief
Test Discrepancies? (TDR)
N
Y
JITC IO Certification
Vendor POAM
IO Outbrief
Coordinate DTR/V&V
Y
Fix Action
N
Adjudicate TDR's and Issues
Y
Critical TDRs?
N


Tab 10 – IA Determination
Test Lab/JITC
Certification Authority
UCCO
Sponsor/Vendor
Generate IA Test Artifacts
IA Draft Report
IA Final Report
DIACAP Scorecard
Vendor POAM
IA Outbrief
IA Outbrief
IA Final Report (IA Findings)
Y
N
Determine Risk Mitigations
Critical Or Minor?
Minor
Critical
IA Certification
Coordinate Testing outbrief with Stakeholders
IA Outbrief
Coordinate Mitigations
Coordinate IO/IA Certifications
8
Vendor POAM
IA Outbrief
Coordinate Mitigations