DISA

Defense Information Systems Agency

A Combat Support Agency

NETWORK SERVICES DIRECTORATE (NS)

DEFENSE INFORMATION SYSTEMS NETWORK (DISN) & GLOBAL INFORMATION GRID (GIG) SERVICE MANAGEMENT (GSM) PROGRAM MANAGEMENT OFFICE (NSP)

UNIFIED CAPABILITIES APPROVED PRODUCTS LIST (UC APL) PROCESS GUIDE

Version 2.3

December 2014

Defense Information Systems Agency
DISN & GSM Program Management Office (NSP)

www.disa.mil/ucco

EXECUTIVE SUMMARY

This Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) Process Guide implements the requirement in Department of Defense Instruction (DoDI) 8100.04, Unified Capabilities, 9 December 2010, and Chairman, Joint Chiefs of Staff Instruction (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 2.2, dated June 2014.

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 L.
Showers

Digitally signed by Jessie L. Showers
DN: cn=Jessie L. Showers, o=NSP,
ou=DISA,
email=jessie.l.showers.civ@mail.mil,
c=US
Date: 2014.12.17 12:33:10 -05'00'

Jessie L. Showers, Jr., PMP
Vice Director for Network Services

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.
2.1	Dec 2013	Updated information, consistency, hyperlinks, process flow and definitions. Applied formatting changes. Removed test cost estimate language. Removed original process charts due to redundancy.
2.2	June 2014	DTRs can be used to extend the APL timeline, IO LoCs will be ‘frozen’ prior to testing, IO and IA certification activities post-testing will be done concurrently
2.3	December 2014	Additional DTR update/clarification on the extension of DTRs and which level of code updates can be facilitated by a DTR. Update to Deployment Guide Requirements. Clarified that SAR Template will be distributed to Vendors post-ICM.

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 (DoDI) 8100.04. The UC APL process is managed by the 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, 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 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 (POC) for scheduling and coordination of partnering test labs.

2.2 Sponsors

The 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 (ICMs).
- 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 the UCCO and vendors.
- Provide vendors the security technical implementation guides (STIGs) and security readiness review checklists that are public key infrastructure (PKI)-restricted.

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

2.3 Vendors

The 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 funding with DoD test facility (Appendix E).
- Apply applicable STIG requirements to the submitted product and submit results to the 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 the UCCO.
- Coordinate all testing activities and logistics with the UCCO, government sponsors and test facility.
- Assist testing centers in developing test plans and test procedures.
- Provide IA and IO POA&Ms within specified timeframes.
- Provide product and management descriptions that will serve as input to the Information Assurance Assessment Report (IAAR).

2.4 Testing Labs

The 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 POC for a given tracking number.
- Coordinate the cost model that will be applied to vendor product with DISA NS. Cost models are either Fee For Service (FFS) or equipment Cooperative Research and Development Agreement (CRADA). Although there is no funding required for a no-cost test all equipment tested under the Cooperative Research and Development Agreement (CRADA) will become the property of the testing center upon expiration of the CRADA.
- Generate and submit a cost estimate to the vendor (or sponsor) if the product falls under a FFS cost model.
- Schedule and attend ICM and out-brief meetings.
- Work with the product engineers on site during setup and testing of SUTs.

- Disseminate the ICM minutes, a Self Assessment Report (SAR) template, an IA findings summary report, IAAR, disseminate the out-brief minutes, and an IO certification summary in the approved formats and timelines as specified in this document.
- Develop TDRs for UC requirements that the SUT does not meet.
- Coordinate TDRs with the Joint Interoperability Testing Command (JITC) AO.
- Attend TDR adjudication meetings.
- Develop a test summary report within the specified guidelines.
- Provide IO test certification recommendations to JITC.
- Provide DTR approval recommendation to the JITC AO.
- Coordinate DTR extension memorandum updates with JITC.
- Develop a UC implementation guide based on the lab's unique business models.
- Review IAARs for quality assurance prior to uploading into the APL Integrated Tracking System (APLITS).
- Assist JITC in the development of test procedures.

2.5 JITC

Above and beyond its test lab responsibilities, 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 IO 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 products to be placed on the UC APL.

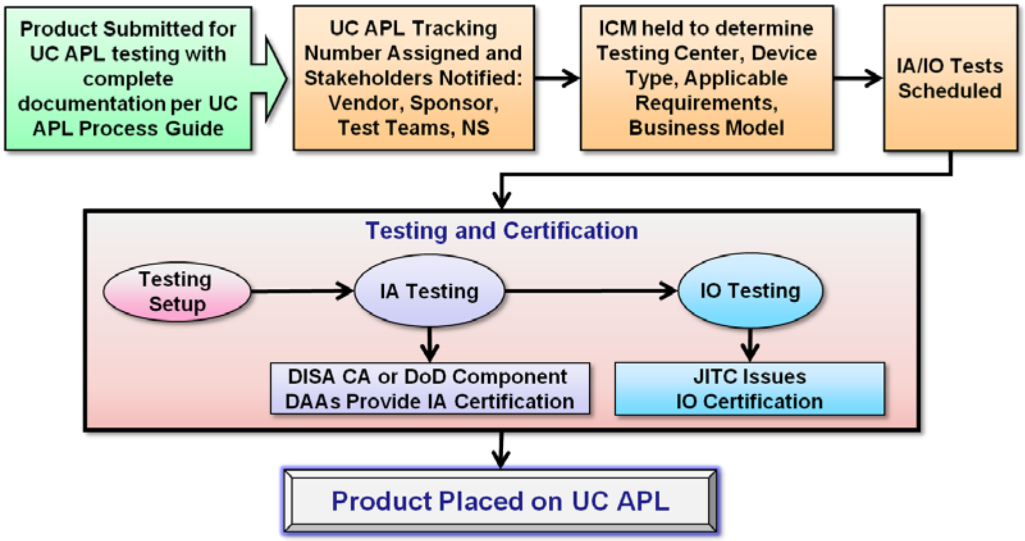
Product Submitted for UC APL testing with complete documentation per UC APL Process Guide
UC APL Tracking Number Assigned and Stakeholders Notified: Vendor, Sponsor, Test Teams, NS
ICM held to determine Testing Center, Device Type, Applicable Requirements, Business Model
IA/IO Tests Scheduled
Testing and Certification
Testing Setup
IA Testing
IO Testing
DISA CA or DoD Component DAAs Provide IA Certification
JITC Issues IO Certification
Product Placed on 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. Two government sponsors, primary and alternate, are required to ensure sponsor availability for attending ICMs and out-briefs. A minimum of two Vendor POCs are required for submission.

2. Vendor submits product for testing via APLITS. 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:

- System diagram in Visio format
- System description and solution component list
- A completed Security Technical Implementation Guide (STIG) Questionnaire
- Letter of Compliance (LoC) template and signed cover letter to be submitted in .pdf format.
- SF 328 Form: Certificate Pertaining To Foreign Interests

Note: Certain UC APL products must be validated by the National Information Assurance Partnership (NIAP). 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 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. Once the complete documentation package is received, the UCCO sends a verification request to the government sponsor to confirm sponsorship:

- The sponsor confirms that the submitted product is in accordance with DoDI 8100.04.
- The sponsor agrees to attend the ICM, out-brief, and TDR adjudication meetings.
- The sponsor agrees to the configuration submitted by the vendor.

4. Sponsor approves SUT configuration and verifies contact information.

5. UCCO issues a Tracking Number (TN) for complete submissions. The product is assigned a test lab and the AO coordinates scheduling of the ICM. ICM attendees include the vendor, sponsor, applicable DoD component lab POCs, Certifying Authority (CA) representative, JITC AO, and a UCR subject matter expert. The outcome of the ICM will be the assignment of an APL product type, agreement on applicable UCR requirements, business model determination, SUT configuration, IA/IO requirements (finalized STIGs and UCR LoC templates), 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 choose to delay or cancel testing based on non-compliance or unacceptable POA&Ms.

Note: In limited cases of equipment CRADA products the LoC may be used to write and adjudicate TDRs prior to testing. This may not apply to all DISA NS core-funded products and does not apply to any FFS events.

6. The assigned test lab AO will provide ICM minutes and tailored SAR template to all attendees and coordinate the business model with the 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. The vendor is required to submit a complete SAR to UCCO 10 business days prior to the IA test start date. Conditions are 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 a SAR.
- Failure to comply with the SAR requirement will result in a cancellation of the scheduled test dates and retirement of the TN.
- The IA test team will provide the SAR template to the vendor after the ICM.
- The SAR template to be used for IA testing will lock in on the 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 submitted in the vendor's SAR will be transferred to the new, updated template 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 is provided in conjunction with the ICM minutes.

9. UCCO has three business days to review the SAR for completeness and distribute it to the test team.

10. IA testing commences.

11. IA testing is completed per the test lab. If Category (CAT) I findings exist, the vendor will submit for a Verification and Validation (V&V) test window. If the IA V&V test fails to demonstrate CAT I correction, the TN will be retired. The vendor will then need to resubmit the product for testing after the findings have been corrected 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 requests V&V after testing is completed, 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 the vendor will need to reinitiate the UC APL process at a later date.

12. IO testing commences.

13. The IA test team disseminates the IA findings summary to the UCCO and vendor within 10 business days of testing completion. Test events that result in multiple reports (e.g., ASLAN, wireless, and LSC) will be granted additional time as coordinated during the ICM.

14. The 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 the set deadline will result in TN retirement and the 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. The IA test team schedules the IA out-brief meeting to take place within 10 business days of receiving the IA findings mitigations from the vendor. Required out-brief attendees include the sponsor, vendor, AOs (lab and JITC, as applicable), IA test team, DISA CA or DoD component Designated Accrediting Authority (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 the vendor will need to reinitiate the UC APL process. A maximum of two V&Vs can be requested in one testing cycle before the solution will be retired.

16. The IA test team disseminates IA out-brief meeting minutes within five business days after conclusion of the meeting.

17. The 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. The IA test team submits final draft 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 three business days to review the final draft IAAR for quality assurance.

20. UCCO requests an IA Certification Letter from DISA CA or DoD component DAA/CA.

21. DISA CA or DoD component DAA/CA has 15 business days to complete the IA Certification Letter and return it to the UCCO.

Notes:

1. If the DISA CA or DoD component DAA/CA issues a negative IA Certification 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.

2. If an IAAR is returned to the vendor or IA test team 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 three 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 Letter or the DAA/DSAWG provides an Authorization To Operate (ATO)/Interim ATO (IATO).

24. 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 Section 3.3 for further details on the DTR process.

25. The IO test team will coordinate TDRs with the JITC AO during the IO test window.

26. Once IO testing has been completed, the test team will provide a record of any open TDRs to the vendor. The vendor will have five business days to provide a response (IO POA&Ms) to the open TDRs; responses should be made with the input and concurrence of the sponsor.

Note: Responses should minimally include an IO POA&M addressing whether the vendor plans to resolve the discrepancy, the planned resolution timeline; and software/hardware implications if the currently defined SUT is not fixed (hardware/software).

27. An IO out-brief will be held within five business days of IO test completion to discuss the completion of IO testing, POA&Ms, and the TDR adjudication schedule. Participants include the test team, sponsor, vendor, JITC AO, and UCCO. The AO will provide a comprehensive TDR report and IO test summary.

28. If no IO POA&M is received within five 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).

29. The distributed test lab AO will prepare an open TDR synopsis in accordance with the prescribed format and staff to the DISA NS Capabilities Center (NS2) IO Adjudication Board Chair for TDR adjudication.

30. The distributed test lab IO team will coordinate the IO certification summary with the AO. The distributed test lab will staff the IO certification summary and recommendation to JITC within 10 business days after the IO adjudication board meeting at which time 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 additional time as coordinated at the ICM.

31. 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 additional time as coordinated at the ICM.

Note: The IO adjudication and certification process will progress independently from IA once testing is complete. Depending on the situation the IO certification may be received prior to the IA certification; the UCCO will be responsible for ensuring both certifications have been received prior to UC APL listing.

Note: If the IO adjudication board determines that the IO test fails and there is a critical TDR, the TN will be retired. The 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.

32. The vendor submits the deployment guide, which reflects the SUT, for review by the UCCO and approval by NSP prior to the issuance of the UC APL approval memorandum.

33. UCCO has three 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 three years.

34. UCCO sends UC APL approval notification to the configuration control board members, sponsors, and vendors.

35. UCCO posts the product on UC APL website: https://aplits.disa.mil

36. From the date of the APL approval memorandum, UCCO has 10 business days to compile the IA Assessment Package (IAAP).

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

37. 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.

38. 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 Adjustments to Current SUT

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

- Sponsor POC
- Vendor POC
- Software release
- Product model
- System configuration
- Test date request
- V&V request

Notes:

1. Vendors are allowed two test deferral requests. If the vendor is not available to test by the second test deferral date, the TN will be retired and the vendor will need to reinitiate the UC APL process.

2. 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. The vendor submits adjustment request(s) via the UCCO website. See the APLITS User Guide for instructions. For system configuration updates, an updated Visio drawing needs to be submitted to the UCCO.
2. UCCO distributes the adjustment request(s) to sponsor/vendor/test team to review for accuracy.
3. If there are no objections by the sponsor or test team, UCCO makes the adjustment.

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 the UCCO. DTR requests will result in either:

- An update to the APL memo with no additional testing required.
- Minimal testing as the same TN resulting in an update to the APL Memo.
- A new submission for testing resulting in a new TN.

A DTR is for changes/updates to existing APL-approved software releases not major platform changes.

Note: If the Version change is an update and not a wholesale code or platform change, then limited V&V testing could be used to update the UC APL. Only after evaluation by the original test team, with concurrence from UCCO Government Lead, would a final decision be made.

DTRs can also be used to request an extension to the UC APL certification length for products whose originally approved UC APL version is still being marketed and supported. These products may receive up to an additional 3 years on the UC APL. For DTRs to extend APL certification dates, the designated Distributed Testing (DT) lab will assess the deltas between the IO Test Procedures (TPs) used in the initial, base certification, and the current TPs for that product. The DT lab will recommend new/modified TPs (if any) that should be applied as part of any V&V testing for this DTR.

1. The vendor submits a product for review via the UCCO website https://aplits.disa.mil. See the APLITS User Guide for instructions. Additionally, the vendor will submit a detailed description of the patch to be evaluated within five business days of the DTR request. If the documentation package is not received within the five-business-day window, the DTR request will be cancelled.
2. UCCO validates the 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. The testing lab AO will provide the JITC AO with a DTR recommendation within five business days. The JITC AO will present one of the following recommendations to the UCCO:
    a. No testing is required. Recommends that the IO and UC APL memo be updated.
    b. Recommends minimal testing. The lab will provide a short, detailed description/justification for the recommendation.
    c. Recommends a new submission. The lab will provide a short, detailed description/justification for the recommendation.
5. UCCO forwards the recommendation to UCCO Government Lead for review and coordination with the Service manager, if applicable. UCCO Government Lead has three business days to provide:
    a. Concurrence on the testing/update recommendation, or the testing recommendation is accepted.
    b. For items 4b and 4c (recommendation for minimal testing or a new submission), 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 whether or not testing was required.
7. JITC updates the IO certification letter within 10 business days of the DTR approval or DTR test event, whichever is applicable.

Note: If the product was placed on the APL without a JITC certification (fast track), JITC will coordinate with NSP to determine if a certification requires development. Development of a certification summary report/memorandum will result in additional time allocation to complete the certification process.

8. Upon receipt of the updated IO certification letter from JITC, UCCO posts the updated product on the UC APL and updates the IAAP with the DTR information.
9. If a change to the SUT is made via the DTR process, the vendor will provide an updated deployment guide.

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 on the UC APL. The FT process is structured to accommodate DoD sponsors that may need 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 (UCSG) 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 include:

- 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) that are currently fielded and successfully performing from both an IO and IA perspective in operational networks.
- Products that should be added to the UCR per the UCSG.

3.4.1 FT Product Categories

There are three FT product categories:

1. Products within Current UCR Product Categories. These are 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.
2. Operationally Validated. These include current UCR products or approved FT products that are currently operating in DoD networks, have an IATO or ATO, are in compliance with appropriate STIGs, and are submitted for APL status. These 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 IO test certification

memorandum and certification summary report will be developed using the specified artifacts.

3. 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 are considered to be in a new product category.

3.4.2 FT Submission

To submit a product for UC APL FT consideration, the same rules regarding sponsorship and product documentation apply as stated in Section 3.1 of this document. For products being presented as a new UCR product category, the 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 to evaluate product maturity, features affecting assured service, and suitability for UC APL testing. Meeting participants will include the vendor, sponsors, UCCO, JITC, the distributed test lab (if applicable), and the NS engineering team. 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
APLITS	Approved Products List Integrated Tracking System
ATO	Authorization to Operate
CA	Certifying Authority
C & A	Certification and Accreditation
CCB	Configuration Control Board
CRADA	Cooperative Research and Development Agreement
CJCSI	Chairman Joint Chiefs of Staff Instruction
DAA	Designated Accrediting Authority
DATO	Denial of Authorization to Operate
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DoDI	Department of Defense Department Instruction
DSAWG	Defense IA/Security Accreditation Working Group
DSN	Defense Switched Network
DTR	Desktop Review
FFS	Fee for Service
FSO	Field Security Operations
FT	Fast Track
IATO	Interim Authorization to Operate
ICM	Initial Contact Meeting
IA	Information Assurance
IAAP	Information Assurance Assessment Package
IAAR	Information Assurance Assessment Report
IO	Interoperability
JIC	Joint Interoperability Certification
JITC	Joint Interoperability Test Command

Acronym	Definition
JS	Joint Staff
LOC	Letter of Compliance
MILDEP	Military Department
MIPR	Military Interdepartmental Purchase Request
MMD	Multifunction Mobile Device
NIAP	National Information Assurance Partnership
NII	Networks and Information Integration
NIPRNet	Sensitive but Unclassified Internet Protocol Router Network
NS	(DISA) Network Services (Directorate)
ODC	Other Direct Costs
OSD	Office of the Secretary of Defense
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	Point of Contact
RAE	Required Ancillary Equipment
RTS	Real Time Services
SAR	Self Assessment Report
STIG	Security Technical Implementation Guide (STIG)
SUT	System Under Test
T&E	Testing and Evaluation
TDR	Test Discrepancy Report
TN	Tracking Number
TP	Test Procedures
UC	Unified Capabilities
UCCO	Unified Capabilities Certification Office
UCR	Unified Capabilities Requirements
UCSG	Unified Capabilities Steering Group
USD	Under Secretary of Defense
V&V	Verification and Validation

APPENDIX B

REFERENCES

- Department of Defense (DoD) Unified Capabilities Requirements (UCR), 2013 January 2013
- The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, Interoperability and Supportability of Information Technology and National Security," 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

UNIFIED CAPABILITIES (UC) APPROVED PRODUCTS LIST (APL) DOCUMENTATION GUIDE

1 INTRODUCTION

What follows are the minimum documentation requirements for products submitted to the Unified Capabilities Certification Office (UCCO) in support of the UC APL testing. All products submitted for UC APL testing must include the initial and follow-on documentation described below. All submittal documentation templates can be found on the APL Process Guide web page under the UC APL Product Submittal Documentation section.

Initial Required Documentation

- System diagram in Visio format
- System description and solution component list
- A completed Security Technical Implementation Guide (STIG) Questionnaire
- Letter of Compliance (LoC) template and signed cover letter in .pdf format
- SF 328 Form: Certificate Pertaining To Foreign Interests

All applicants attempting to complete a submittal must provide these documents to the UCCO to have a tracking number assigned and begin processing of the product submittal for testing. The UCCO will confirm receipt of documentation when these requirements have been satisfied.

Follow-on Documentation

- Self-Assessment Report (SAR)
- 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 follow-on documentation assists solution vendors and sponsors by reducing the amount of time involved in achieving acceptable product documentation packages. All documentation should be submitted to the UCCO using APLITS and in accordance with the APLITS User Guide.

Table 1: Documentation Checklist

System Diagram	□
System Description/Component List	□
STIG Questionnaire	□
LOC Template and Cover Letter	□
SF-328 Form	□
SAR	□
Deployment Guide	□

2 SOLUTION DOCUMENTATION

2.1 System Diagram

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

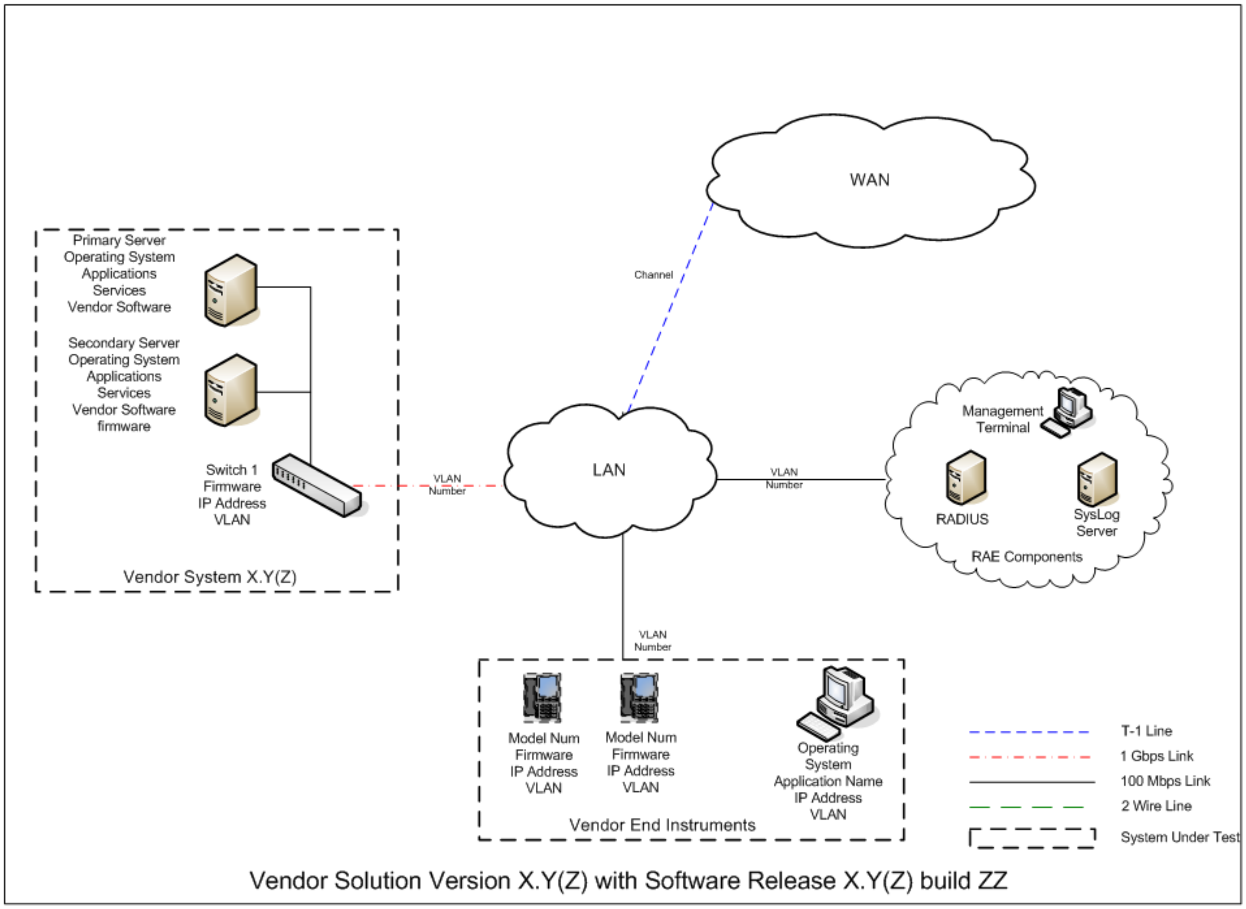

Figure 2: Sample Diagram for Submission

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 OSs, applications, databases, web servers, Internet Protocol (IP) addresses, etc. applicable to the solution. A legend is required. All acronyms used will be defined in the drawing and in the documentation upon first use. 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 SUT components. 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.

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.

2.2 System Description and Solution Components List

Provide a brief description of the functionality and purpose of the entire solution. This is usually one paragraph. The description gives the reader a clear understanding the solution type (session controller, network element, etc.). Be sure to define all acronyms. All solution components that will be involved in the testing of the solution need to be clearly identified in the solution's product documentation.

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:

<u>Component 1:</u> 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.

- Hardware: The model, not the host name
- OS: Include versions and any service pack (SP)
- Application: Custom vendor software (e.g., version 4.2, Microsoft Structured Query Language (SQL) 2000 SP4, McAfee Enterprise 8.0.0i)
- Firmware
- IP address (if known)
- Rack space and power requirements

<u>Component 2:</u> 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.

- Hardware: The model, not the host name (e.g., vendor chassis)
- Card 1: Card 1 description
- Card 2: Card 2 description
- Additional components as needed
- OS: Includes versions and any SPs
- Application: Custom vendor software (e.g., version 4.2, Microsoft Structured Query Language (SQL) 2000 SP4, McAfee Enterprise 8.0.0i)
- Firmware
- IP address (if known)
- Rack space and power requirements

The specific application details of any non-standard applications (e.g., 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.

Table 2: Sample Solution Component Table

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				

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 Management/Administration Description:

Most solutions have numerous options available to manage the solution. The main options fall under the following categories:

1. Local Management Only:

Management directly connected to the terminal

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:

In-Band Management: Management done via Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Network Management Protocol (SNMP)

Out-of-Band 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.

Include security features used between in managing the SUT. 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, the diagram needs to include remote management, the port, protocol, and version being used by the system to support remote management.

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

2.3 STIG Questionnaire

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 breakout of all the components, software applications, general environment configuration, protocols and management methods used by the solution. All submittal documentation templates can be found on the APL Process Guide web page under the UC APL Product Submittal Documentation section.

2.4 Letters of Compliance (LoC) Template and Cover Letter

Detailed requirements for UC products and/or functions are provided or referenced in the Unified Capabilities Requirements (UCR) documentation. In accordance with the UCR, systems are required to have IPv6 capability for testing. All submittal documentation templates can be found on the APL Process Guide web page under the UC APL Product Submittal Documentation section.

- Submit a completed LoC template with signed cover letter which includes the respective category for your solution.
- Include the nomenclature(s) and respective software release(s) applicable to this submission.
- Submit the LoC template and cover letter in .pdf format with a Vice President-level authority signature.

2.5 SF-328 Form Certification Pertaining to Foreign Interests

All companies submitting for UC APL testing must submit a current 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 . All submittal documentation templates can be found on the APL Process Guide web page under the UC APL Product Submittal Documentation section.

2.6 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 the action officer (AO) will provide the vendor the appropriate SAR template format with the ICM minutes.

- The most recent and applicable SAR template will be provided by the AO. All SARs must be in Excel format using the template provided.
- SAR checklists to be used for IA testing will lock in on the SAR suspense date.
  - 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-submitted SAR will be transferred to the new, updated templates at the start of IA testing.
- To meet the minimum requirements, a SAR must:
  - Show the status of all STIGs identified in the SAR template (open, closed, N/A, etc.)
  - Have completed mitigations for each open finding. If a status is marked N/A. please include a short comment explaining why.

- For retests – Provide additional requirements to show resolution of all items identified during the previous solution out-brief
- For all STIGs that have automated scripts available – Provide the results for all components of the solution and indicate the status (i.e., open, closed, N/A). 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, it is preferred over the raw output data from the scripts. Another acceptable option is to pull the vulnerability data from the raw output of the scripts and consolidate them into a Microsoft Excel or Word file.

The SAR is due to the UCCO two weeks prior to scheduled IA testing start date. The UCCO highly encourages SARs be submitted as soon as possible to avoid delays or confusion regarding test preparation.

2.7 Deployment Guide

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

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

- Is the deployment guide titled to reflect that it is the Military Unique Deployment Guide?
- Does the deployment guide include the vendor's Logo?
- Is the deployment guide dated? Is the date after the final IA out-brief?
- Is there version numbering, document change control history page, contact information for submitting recommendations for comments/changes, and a page numbering scheme?
- Does the deployment guide instruct the user to refer to the conditions of fielding that are listed within the IAAR?
- Does the deployment guide include any clarifying or necessary screen shots?
- Does the deployment guide include any clarifying or necessary device configuration files?
- Does the deployment guide 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 deployment guide include clarifying or necessary vendor configuration details/release notes/tweaks implemented during testing?

The Deployment Guide can be submitted to the UCCO via APLITS at any point after the final IAAR is completed.

E-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil

APPENDIX D

MITIGATIONS, PLAN OF ACTION AND MILESTONES (POA&Ms), AND COMMENTS GUIDANCE

1 INTRODUCTION

This appendix is designed to provide guidance on developing Information Assurance (IA) mitigations and POA&Ms for both IA and Interoperability (IO).

1.1 Background

In accordance with the DoD Instruction (DoDI) 8100.04, dated December 9, 2010, DoD Unified Capabilities (UC), 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.

2 IA POA&Ms

2.1 Policy

The DoD Components shall issue a new or update an existing accreditation decision when UC products are installed, pursuant to DoDI 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 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 UC Certification Office (UCCO) APL process and the results of the testing are documented in an Information Assurance Assessment Report (IAAR) and a DIACAP scorecard.

DoDI 8510.01 provides specific guidance regarding the issuance of ATOs with regard 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 Enclosure 3.4 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 [noncompliant] 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. For further information on POA&Ms, see Enclosure 3 of DoDI 8510.01. 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.

2.2 Format

The following two examples of mitigations and POA&Ms are provided to assist in the development of IAARs and includes the level of detail required by the CA. It is highly 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 provide a description of the mitigation utilizing the RAE 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 provide the date the product will be changed in the Vendor POA&M section. 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 IPV 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 state the use of each port in the vendor comment column. **Rules of Engagement**

- The vendor provides quarterly updates, and updates to coincide with scheduled finding POA&M completions.
- The 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 three options is met prior to the expiration date, the POA&M will be closed out and the product will remain on the APL.
- If none of the options to close the POA&Ms have been met by the expiration date, the following will be applied at NS leadership's discretion:

- The vendor either does not respond or responds negatively to the NS POA&M notification. This results in product removal from APL.
- The 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. This results in the product remaining on APL with the expectation of an expeditious resolution. Timeline to be granted at NS leadership discretion.
- The vendor responds that the fix is still in progress and requests additional time for the POA&M. This results in possible removal from APL, based on NS leadership decision.

3 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 government sponsor. Responses should minimally include:
  - An IO POA&M addressing whether the vendor plans on resolving the discrepancy
  - Planned resolution timeline
  - 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).
- The DoD test lab action officer will prepare an open TDR synopsis in accordance with the prescribed format and staff to DISA NS2 for adjudication.
- TDRs will be adjudicated by an NS-led adjudication team. Participants for adjudication should include NS representation, JITC, and the government 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. A 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.

4 WAIVERS AND TDRs FOR DOD UC 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 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 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 DISA (NSP); and approved by the 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 one year. Only in exceptional circumstances, and with DoD CIO approval, shall extensions of waivers be granted. Vendors who do not implement corrective actions or mitigations to resolve waived requirements within the waived period (one 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 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 POA&M for adjudication to the DISA TDR Adjudication Panel (NS2).

    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), 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, the operational impact assessment, and the DoD Component UCR Waiver Request and provide a waiver recommendation to DoD CIO.

5. DoD CIO shall review the DISA (NSP) waiver recommendation and the 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 the government sponsor accept 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). DISN edge products will be targeted for vendor FFS. Generally, if a DISN edge product is sponsored by DISA, it will be tested under the NS2 funding cost model. Products will only be listed on the APL if information assurance (IA) and interoperability (IO) certifications are successful. The equipment CRADA and FFS cost models are defined as follows:

- Equipment CRADA: The vendor and government sponsor agree through a legal document that the cost of the Approved Product List (APL) IA and IO testing 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 government 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 placement on the APL. Costs associated with each FFS product can be estimated by reviewing the document,.

The vendor applicant will be informed of the cost model that applies to their product by the government action officer at the ICM. When the cost model is FFS, the following process will be supported:

1. The 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 ODC
    b. Contractor test labor costs
3. The Government will submit the cost CRADA to the vendor for signature within three 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 four 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 a check, the type of check required, and the government agency to which the check should be issued.
5. If testing is completed early or if the vendor chooses to terminate testing early due to a large number of findings that preclude product listing on the APL, the remaining test funds on task will either be returned to the 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 the vendor's request, but if testing is not completed at the end of the test window, 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, and 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.

APPENDIX F

18-MONTH RULE

When there is an addition, change, or deletion to the Unified Capabilities Requirement (UCR) and the UCR is signed, one of five dispositions will apply on the first day of a product interoperability test window:

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 were notified via the Unified Capabilities Certification Office (UCCO) web page, the requirement compliance may be immediate.

3. If the requirement addresses a critical or major information assurance (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 a test window).

If the UCR does not clarify whether a new requirement is immediate or in 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 plan of action and milestones to close the TDR prior to listing on the APL. 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

NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP) CERTIFICATIONS FOR SECURITY DEVICES

The following device types must be either NIAP-certified or proven to be in the NIAP certification process **prior** to being accepted into the UC APL process.

Acronym	Appliances
FW	Firewall
IAT	Information Assurance Tool
IPC	Internet Protocol Count
IPS	Intrusion Prevention System
ISS	Integrated Security Solution
NAC	Network Access Controller
VPN	Virtual Private Network – concentrator and
WIDS	Wireless Intrusion Detection System

Source: UCR 2013 Table 13.1.1

If a vendor claims a product is a security device or IA-related tool, it must fit one of the protection profiles below and be submitted for NIAP certification. An overview and description of each protection profile is located at https://www.niap-ccevs.org/pp/.

Profile Name	Technology Type
• Protection Profile for Software Full Disk Encryption Version 1.0	• Encrypted Storage
• Protection Profile for USB Flash Drives Version 1.0	Encrypted Storage
• Protection Profile for BIOS Update for PC Client Devices Version 1.0	• Miscellaneous
• Protection Profile for Mobile Operating Systems Version 1.0	• Mobility
• Protection Profile for Mobility - Voice Over IP Application Version 0.6	• Mobility
U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)	Multi Function Device
Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall Version 1.0	Network Devices
Network Device Protection Profile (NDPP) Extended Package SIP Server Version 1.0	Network Devices
Network Device Protection Profile (NDPP) Extended Package VPN Gateway Version 1.1	Network Devices

Profile Name	Technology Type
Protection Profile for Network Devices Version 1.1	Network Devices
General-Purpose Operating System Protection Profile	Operating Systems
Validated Protection Profile - Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 2.1	Peripheral Switch
Enterprise Security Management - Policy Management	Security Management
Protection Profile for Enterprise Security Management - Identity and Credential Management Version 1.4	Security Management
Protection Profile for Enterprise Security Management-Access Control Version 2	Security Management
Protection Profile for IPsec Virtual Private Network (VPN) Clients Version 1.3	VPN
Protection Profile for Wireless Local Area Network (WLAN) Access Systems 15 November 2011 Version 1.0	Wireless LAN
Protection Profile for Wireless Local Area Network (WLAN) Clients Version 1.0	Wireless LAN

The test lab must include the NIAP certification or a status letter as an appendix in the Information Assurance Assessment Report.

APPENDIX H

MULTIFUNCTION MOBILE DEVICE (MMD) POLICY AND PROCESS

1 INTRODUCTION

This appendix is included to address the updated rules of engagement for vendors wishing to submit mobile devices into the UC APL process.

1.1 Background

The UCR recognizes 3 scenarios for Multifunction Mobile Devices (MMD):

USE CASE NUMBER	TITLE	HIGH LEVEL DESCRIPTION
#1	Non Enterprise Activated Use Case: No Connectivity to DoD Network and No Processing of CUI Data Use Case No connectivity to DoD e-mail	MMD that has no connectivity to a DoD network and processes only publicly available DoD data information (Data as defined in this context is clarified in Section 8 of the UCF)
#2	Full Connectivity to DoD Network and Processing of Sensitive UNCLASSIFIED Information Use Case	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks Securely processes and stores DoD information at the CUI level
#3	Full Connectivity to DoD Network and Processing of Sensitive UNCLASSIFIED Information Use Case Full Connectivity to DoD UC Services	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks Securely processes and stores DoD information at the CUI level. This MMD has full connectivity to DoD UC Services

2 USE CASES 1 & 2

All MMDs must be listed on the UC APL, however, in the case of Use Cases 1 and 2 a limited UC APL process is amended as such:

2.1 Process

1. MMD Vendor contacts the DISA FSO at http://iase.disa.mil/stigs/vendor_process/index.html to develop a STIG for their product
2. CIAE grants approval to the STIG; the product is updated in the Mobile Device Manager(MDM)
3. Vendor submits a new product in APLITS, specifying that it is a MMD Use Case 1 or 2.
4. UCCO verifies CIAE approval and list the product on the UC APL within 5 business days.

3 USE CASE 3

Use Case 3 is representative of products or applications which provide full UC services as defined by the UCR.

3.1 Process

1. MMD Vendor contacts the DISA FSO at http://iase.disa.mil/stigs/vendor_process/index.html to develop a STIG for their product
2. CIAE grants approval to the STIG; the product is updated in the Mobile Device Manager(MDM)
3. Vendor submits a new product in APLITS, specifying that it is a MMD Use Case 3 product
4. The product now enters the regular UC APL process identified in Section 3 of this document.