



Defense Information Systems Agency

A Combat Support Agency

**DEPARTMENT OF DEFENSE
INFORMATION NETWORK
(DODIN) APPROVED
PRODUCTS LIST (APL)
PROCESS GUIDE**

**Defense Information Systems Agency (DISA)
Infrastructure Directorate (IE)**

Version 2.6

December 2019

<https://aplits.disa.mil/>

EXECUTIVE SUMMARY

This Department of Defense Information Network (DoDIN) 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 DoDIN APL and the customer process guide describing steps that must be followed for a product to be listed on the DoDIN APL.

This DoDIN APL Process Guide:

Updates and cancels the previous DoDIN APL Process Guide, Version 2.4, dated December 2016.

This guide is approved for public release and is available on the DISA website at <https://aplits.disa.mil/>

The instructions in this guide are effective immediately.

SIGNATURE PAGE

The undersigned agrees with the Department of Defense Information Network Approved Products List process for products defined in this document.

Approval:

Charles H. Osborn
Acting Executive, Infrastructure Directorate

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 | December 2012 | Baseline document. |
| 2.1 | December 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 UC APL timeline, IO LoCs will be 'frozen' prior to testing, and 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. |
| 2.4 | December 2016 | Added CA Roles/Responsibilities. Updated NIAP/NIST requirements. Added LoC Template and Test Plan locked-in date. Updated "IA" to read "Cybersecurity" throughout the guide. ICM scheduled-by due date added. IO process clarified. Vendor IO POA&M and IO Out-brief due date updated. Clarification to DTR Documentation. DTR testing recommendations updated. Added RAE Appendix I and updated Mobility Appendix H. General updates/ /clarification made throughout the guide. Updated Appendix D to remove redundant information already documented in DoDI 8100.04. 18-Month Rule clarification/updates (Appendix F) and DoD Annex information added (Appendix G). Updated to include DoDIN and remove UC. Updated UCCO to APCO. |
| 2.5 | July 2017 | Update to FIPS, APL extension requirements, and MAP documentation requirements. Removal of 180 day POA&M requirements. SF-328 Corporate Seal requirement removed. Update to APL timelines. Minor verbiage updates/clarification. IO V&V clarification added. Sponsor role clarification added. |
| 2.6 | December 2019 | Add requirement for Vendors to provide a list of findings/POA&Ms being addressed via the DTR and/or |

| | | |
|--|--|--|
| | | <p>updated LoC as applicable (Section 3.3, Item 1). Add guidance for embedded OSs (Appendix C, Section 1.2). Add option for AOs to schedule an ICM for DTRs (Section 3.3, Item 6). JITC FFS/CRADA specific language removed from Appendix E. Remove requirement for Sponsors to be present for ICMs/Out-briefs (Section 2.2). Remove MUDG requirement to include list of CoF (Section 1.7). Updated IASE references to Cyber Exchange.</p> |
|--|--|--|

1 INTRODUCTION..... 1

1.1 Overview 1

1.2 Purpose..... 1

2 ROLES AND RESPONSIBILITIES 1

2.1 Approved Products Certification Office (APCO) 1

2.2 Sponsors 1

2.3 Vendors 2

2.4 Action Officers..... 2

2.5 JITC..... 3

2.6 Certifying Authority..... 3

3 STANDARD OPERATING PROCESS 3

3.1 DoDIN APL Process Rules and Guiding Principles 4

3.2 SUT Adjustment Requests 8

3.3 Desktop Review (DTR) Process 9

3.4 DoDIN Modified APL Process (MAP)..... 11

APPENDIX A - ACRONYMS 1

APPENDIX B- REFERENCES..... 1

APPENDIX C- DODIN APL DOCUMENTATION GUIDE 1

1.1 System Diagram 1

1.2 System Description and Component List Template..... 3

1.3 STIG Questionnaire..... 3

1.4 Letters of Compliance (LoC) Template and Cover Letter 3

1.5 Standard Form 328 (SF-328) - Certification Pertaining to Foreign Interests 4

1.6 Vendor Self-Assessment Report (SAR)..... 4

1.7 Military Unique Deployment Guide (MUDG) 5

1.8 Modified APL Process (MAP) Documents..... 5

APPENDIX D- MITIGATIONS AND POA&MS 1

1.1 Format Examples..... 1

1.2 Cybersecurity POA&M Rules of Engagement 2

1.3 IO POA&M Rules of Engagement 3

APPENDIX E- TESTING COSTS 1

APPENDIX F- UCR 18-MONTH RULE 1

APPENDIX G- NIAP & NIST CERTIFICATIONS 1

1.1 National Information Assurance Partnership (NIAP) 1

1.2 National Institute of Standards and Technology (NIST) 1

APPENDIX H- MOBILE DEVICE POLICY AND PROCESS..... 1

APPENDIX I- REQUIRED ANCILLARY EQUIPMENT (RAE) 1

APL RAE List..... 1

1 INTRODUCTION

1.1 Overview

The Department of Defense Information Network (DoDIN) Approved Products List (APL) process is developed in accordance with DoD Instruction (DoDI) 8100.04. The DoDIN APL process is managed by the Defense Information Systems Agency (DISA) – Infrastructure Directorate (IE) Approved Products Certification Office (APCO). 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 in accordance with (IAW) DoDI 8100.04.” The APL process provides for an increased level of confidence through Cybersecurity and Interoperability (IO) certification. The DoDIN APL (hereinafter referred to as ‘APL’) is 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).

1.2 Purpose

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

2 ROLES AND RESPONSIBILITIES

2.1 Approved Products Certification Office (APCO)

The APCO acts as the staff element for DISA IE to manage the APL. The APCO provides process guidance, coordination, information, and support to government Sponsors and Vendors throughout the entire process - from the registration phase to the attainment of APL status. In addition, the APCO manages the APL Removal List which consists of products that have been removed from the APL. In the DoD distributed testing environment, the APCO is the primary Point of Contact (POC) for scheduling and coordination of partnering test labs.

2.2 Sponsors

The main Sponsor responsibilities for APL certification are as follows:

- Assist DISA with developing requirements for the desired product and product features (if applicable) and ensure acquisition of applicable products aligns with DoD policy and direction.
- Attend the Initial Contact Meeting (ICM), Cybersecurity out-briefs, IO out-briefs, and any applicable Test Discrepancy Report (TDR) adjudication meetings to discuss test results and assist with Vendor mitigation strategies and Plan of Actions and Milestones (POA&Ms) in accordance with the guidance provided in this process. Note: Sponsor attendance to the above listed meetings is encouraged but is not required so long as the Sponsor reviews the meeting minutes and provides feedback when necessary.
- Assist the APCO, Action Officer, and Vendor with the coordination of all testing activities, logistics, and funding (if applicable) for the assigned DoD test facility.

- Provide Vendors with the Security Technical Implementation Guides (STIGs) and Cybersecurity Assessment Reports (CAR) that are Public Key Infrastructure (PKI)-restricted.
- The Primary Sponsor for a product must be a DoD Civilian or Uniformed Military Personnel. The Alternate Sponsor can be a DoD Civilian, Uniformed Military Personnel, or a DoD Contractor.

2.3 Vendors

The main Vendor responsibilities for APL certification are as follows:

- Review the APL Documentation Guide ([Appendix C](#)) and submit documentation in accordance with the guide.
- Assist the assigned testing center in developing test plans and test procedures (if applicable).
- Assist the APCO, Action Officer, and Sponsor with the coordination of all testing activities, logistics, and funding ([Appendix E](#)) for the assigned DoD test facility.
- Apply applicable STIG requirements to the submitted product and submit the Self-Assessment Report (SAR) results to the APCO as directed in Section 3.
- Ensure on-site engineering support is provided during all phases of APL testing assigned for the system under test (SUT).
- Attend the ICM as well as the Cybersecurity out-briefs, IO out-briefs, and any applicable TDR meetings to discuss test results, Vendor mitigation strategies, and POA&Ms in accordance with the guidance provided in this process.
- Provide a Military Unique Deployment Guide for the SUT to the APCO ([Appendix C](#)).
- Provide Cybersecurity Mitigations and IO POA&Ms within the specified timeframes. Also, provide product and management descriptions that will serve as input to the Cybersecurity Assessment Report (CAR).

2.4 Action Officers

The main Action Officer (AO) responsibilities for APL certification are as follows:

- Attend APCO Scheduling Meetings to provide Cybersecurity and IO testing dates for products that have been assigned for testing.
- Assign a Testing AO to be the testing POC for each SUT and if the testing is being conducted at a Distributed Lab, coordinate with Joint Interoperability Test Command (JITC) to have a JITC AO assigned.
- Coordinate the cost model for each product with the APCO, Vendor, and Sponsor.
- Schedule and attend the ICM, Cybersecurity out-briefs, and IO out-briefs and work with the UCR team to schedule any applicable TDR adjudication meetings.
- Work with the product engineers on site during setup and testing of SUTs.

- Draft and disseminate the ICM minutes, SAR template, Draft and Final Cybersecurity Assessment Report, Cybersecurity and IO out-brief minutes, TDRs, and an IO Certification in the approved formats and timelines as specified in this document.
- Provide Desktop Review (DTR) recommendations and coordinate DTR IO Certification memorandum extensions with the JITC AO.
- Review Cybersecurity Assessment Reports 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 the Action Officer responsibilities, JITC also has responsibilities for:

- Overall format and content of the APL test and certification documentation (test procedures, test reports, certification memorandum, etc.).
- Development, staffing, and posting of the IO Certification memorandum.
- Develop and maintain an Implementation Guide based on the labs' unique business models.

2.6 Certifying Authority

The main Certifying Authority (CA) responsibilities for APL certification are as follows:

- Attend the ICM and Cybersecurity Out-briefs as the CA for applicable products.
- Provide guidance on applicable STIGS, Security Requirement Guides (SRG), and other Cybersecurity requirements to be held against products being tested for APL certification.
- Provide a CA Cybersecurity Certification Recommendation Letter and CA Concurrence for Desktop Reviews for APL products.

3 STANDARD OPERATING PROCESS

The standard APL process, as identified in the DoDI 8100.04, is shown in Figure 1.

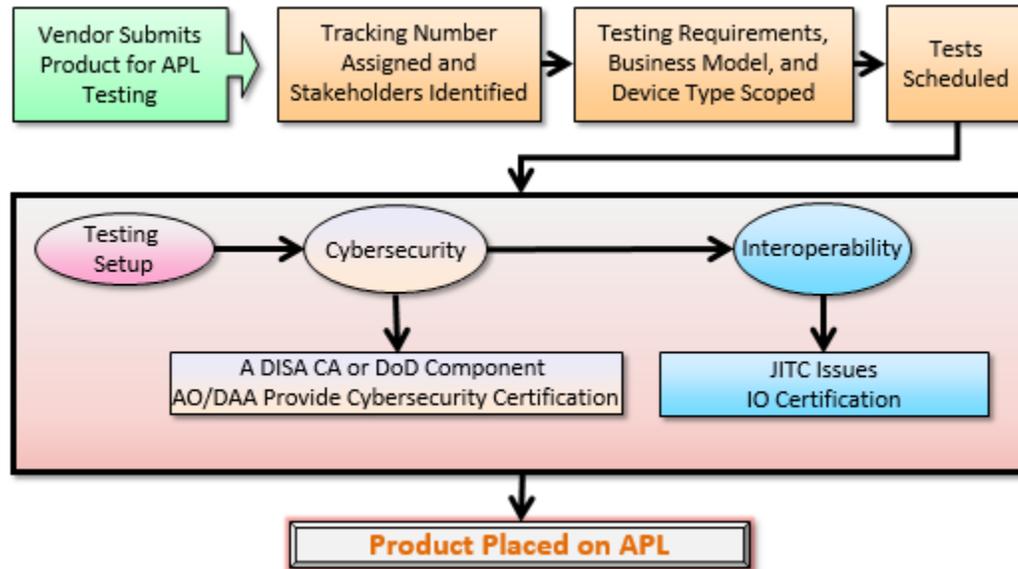


Figure 1: Standard Process for DoDIN APL Certification

Note: From the time Testing Setup begins to Placement on the DoDIN APL, the target estimated timeline for a typical product is 12-16 weeks.

3.1 DoDIN 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 Initial Contact Meetings (ICM) and out-briefs. Two Vendor POCs, primary and alternate, are required for submission.
2. Vendor submits product for testing via [APLITS](#) including a complete documentation package as identified in [Appendix C](#) of this process guide.

Note: Product submittals will not be processed until the APCO receives a complete product documentation package. Failure to do so will result in unnecessary delays to the process. See Appendix C for additional documentation details (as applicable).

3. Once the complete documentation package is received, the APCO sends a verification request to the government Sponsors to confirm Sponsorship.
4. The Sponsor will be asked to concur/agree to the below items:
 - The Sponsor contact information the APCO has on file is correct and the submitted product is in accordance with DoDI 8100.04.
 - Agree to attend the ICM as well as the Cybersecurity out-briefs, IO out-briefs, and any applicable Test Discrepancy Report (TDR) adjudication meetings to discuss test results and assist with Vendor mitigation strategies and Plan of Actions and Milestones (POA&Ms) in accordance with the guidance provided in this guide.
 - Agree to the configuration and device type submitted by the Vendor.
5. The APCO issues a Tracking Number (TN) for complete submissions. Once a TN is assigned, the current version of the Letter of Compliance (LoC) template submitted by

the Vendor is locked in and is the version that will be applicable to the SUT during testing. The product is then assigned a test lab, Testing AO, and JITC AO. The Testing AO coordinates scheduling of the ICM to occur within 10 business days of being assigned to the product. Required ICM attendees include the Vendor, Sponsor, Testing and JITC AO, Certifying Authority (CA) representative, and APCO. The outcome of the ICM will be the assignment of a Unified Capabilities Requirements (UCR) device type, agreement on applicable UCR requirements, business model determination, SUT configuration, Cybersecurity and IO requirements (finalized STIGs and UCR LoC templates), test location, products included by similarity (if applicable), certification document deliverables, and confirm test dates (if available). 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 Cooperative Research and Development Agreement (CRADA) products, the LoC may be used to write and adjudicate TDRs prior to testing. This may not apply to all DISA core-funded products and does not apply to any Fee for Service (FFS) events.

6. The Testing AO will upload ICM minutes and a tailored Self-Assessment Report (SAR) template to APLITS within 5 business days after the ICM and will send a notice to all attendees that the documents are available for review. The AO will also coordinate the business model with the Vendor, Sponsor, and APCO.

7. Products with a complete business model will be placed on the next APCO scheduling meeting agenda. Scheduling meetings take place bi-weekly; however, updates to the schedule may be performed at any time if test dates are available.

8. The Vendor is required to submit a completed SAR to the APCO 10 business days prior to the Cybersecurity testing start date. Refer to [Appendix C](#) of this guide for additional information on SAR requirements.

9. The APCO has 3 business days to review the SAR for completeness and distribute it to the test team.

10. The Cybersecurity and IO Test Plans for the SUT will be locked in 30 days prior to testing setup.

11. Cybersecurity testing commences. If Category (CAT) I findings exist, the Vendor will submit for a Verification and Validation (V&V) test window. If the Cybersecurity V&V test(s) fails to demonstrate a CAT I correction, the TN will be retired and 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 a V&V once 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 V&V testing is determined to be necessary during the Cybersecurity out-brief, the Vendor must be ready for V&V testing within 20 business days of the Cybersecurity out-brief. Regardless of whether a V&V is being conducted to correct excessive CAT II or CAT I findings, a maximum of two V&Vs can be requested in one testing cycle before the solution will be retired.

12. IO testing commences upon completion of Cybersecurity testing.

13. Upon successful completion of Cybersecurity testing, the Testing AO must upload the Draft Cybersecurity Assessment Report (CAR) within 10 business days to APLITS and

notify the APCO, Vendor, and Sponsor that the report is ready. Test events that result in multiple reports being generated can be granted additional processing time if coordinated with the APCO. If the Vendor does not have access to APLITS to retrieve the report, the Sponsor must provide the report to the Vendor.

14. The Vendor has 10 business days after receiving the Draft CAR to turn in mitigations and POA&Ms for findings reported within the Draft CAR. Failure to update the Draft CAR with mitigations and POA&Ms by the set deadline could result in TN retirement and the Vendor will need to reinitiate the APL process. See [Appendix D](#) for guidance on the construct of proper mitigations, POA&Ms, and comments.

15. The Testing AO schedules the Cybersecurity out-brief meeting to take place within 10 business days after receiving the Vendor's cybersecurity mitigations. Required Cybersecurity out-brief attendees include the Sponsor, Vendor, Testing and JITC AO, CA representative, and APCO.

16. The AO disseminates the Cybersecurity out-brief meeting minutes within 5 business days after conclusion of the meeting.

17. The Cybersecurity out-brief meeting attendees will complete all assigned action items listed in the meeting minutes within 10 business days of receiving the minutes. If the Vendor fails to submit action items by the deadline, the TN could be subject to retirement and the Vendor would need to reinitiate the APL process.

18. The AO submits the Final Cybersecurity Assessment Report (CAR) to the APCO within 10 business days of receiving all of the assigned Cybersecurity out-brief action items. Test events that result in multiple reports being generated can be granted additional processing time if coordinated with the APCO. If a Cybersecurity Assessment Report is returned to the Vendor or AO for corrections of discrepancies in the report (i.e. product description, diagrams, mitigation errors or missing POA&Ms), delays to the Authorizing Official (AO)/CA timeline can be expected.

19. The APCO has 3 business days to review the Final CAR and request a Cybersecurity Recommendation Letter from the DISA CA or DoD component AO/CA.

20. DISA CA or DoD component AO/CA has 15 business days to complete the Cybersecurity Recommendation Letter and return it to the APCO.

Note: Products with open CAT I findings and/or unmitigated or excessive CAT II findings may be denied APL placement per the discretion of the CA reviewer.

21. (Conditional step – as necessary) Per decision criteria, if the product is to go to the Defense Security Accreditation Working Group (DSAWG), the APCO has 3 business days to prepare a read-ahead briefing for DSAWG 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 IE.

22. CA provides the APCO with a Cybersecurity Recommendation Letter or the AO/DSAWG provides an Authorization to Operate (ATO)/Interim ATO (IATO).

Note: In the product's lifecycle, if the Vendor's Cybersecurity POA&Ms are not met, the product may be removed from the APL based on the guidelines in Appendix D of this document. 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 Desktop Review (DTR) process. See Section 3.3 for further details on the DTR process.

23. IO testing is completed.

24. If no TDRs were generated during testing and JITC did not perform the testing, the Testing AO will draft and provide the IO certification to the JITC AO within 10 business days of IO testing completion. The JITC AO then has 10 business days to approve and post the IO certification letter to the JITC IO certification page. If JITC is the lab that performed the IO testing, the JITC AO will have up to 10 business days after IO testing completion to draft and post the IO certification letter to the JITC IO certification page. Test events that result in multiple reports being generated can be granted additional processing time if coordinated with the APCO.

25. If IO TDRs were generated during IO testing, the testing AO will provide a record of any open TDRs to the Vendor and will schedule an IO out-brief (if needed) within 10 business days of IO testing completion. Participants of the IO out-brief include the Testing AO, Sponsor, Vendor, and JITC AO.

26. The Testing AO disseminates the IO out-brief meeting minutes within 5 business days of the meeting being held.

27. After receiving the TDR report, the Vendor will have 10 business days to provide a response (IO POA&Ms) to the open TDRs. Refer to [Appendix D](#) of this guide for further guidance on IO POA&Ms.

28. The Testing AO will prepare an open TDR synopsis in accordance with the prescribed format and staff to the IO Adjudication Board Chair for TDR adjudication within 10 business days of receiving the Vendor's IO POA&Ms.

29. The IO TDR Adjudication Meeting is conducted. Any TDRs based on failure to meet UCR standards will be adjudicated for severity and a way-ahead will be provided to the Vendor. All adjudications with an outcome that would prevent certification (i.e., critical) will be reviewed by DoD CIO, DISA IE, and/or JITC. A final adjudication decision will be provided to the APCO, Vendor, and JITC for appropriate action (i.e. TN retired, APL listing contingent on POA&M completion, etc.). *Please note if approved by CIO, no critical POA&MS will be accepted for a period longer than 6 months.*

Note: V&V testing is carried out if the Vendor believes the problems discovered during IO testing can be resolved rapidly. If the Vendor requests a V&V once IO testing is completed, the Vendor must submit and be ready for V&V testing within 20 business days of the end of the original IO test window. If V&V testing is determined to be necessary during the IO out-brief or during the TDR Adjudication process, the Vendor must be ready for V&V testing within 20 business days of when V&V testing was determined necessary.

30. The IO Adjudication Board Chair has 10 business days after the Adjudication Meeting to provide the final adjudication results.

31. The APCO will notify the Testing AO that final adjudication results have been received and the IO certification is due within 10 business days. If JITC did not perform the testing, the Testing AO will draft and provide the IO certification to the JITC AO within 10 business days. The JITC AO then has 10 business days to approve and post the IO certification letter to the JITC IO certification page. If JITC is the lab that performed

the IO testing, the JITC AO will have up to 10 business days after receiving the final adjudication results to draft and post the IO certification letter to the JITC IO certification page. Test events that result in multiple reports being generated can be granted additional processing time if coordinated with the APCO.

Note: The IO adjudication and certification process will progress independently from the Cybersecurity process once testing is complete. Depending on the situation, the IO certification may be received prior to the Cybersecurity Recommendation Letter.

32. The Vendor submits the Military Unique Deployment Guide for review by the APCO and approval by IE prior to the issuance of the APL approval memorandum.

33. The APCO has 3 business days to prepare the APL approval memorandum and submit to IE for signature after receipt of the signed and posted IO certification letter.

34. The APCO sends APL approval notification to the Testers, Sponsors, and Vendors.

35. The APCO posts the product on APL website: <https://aplots.disa.mil/apl> APL listing of the product is for no longer than three years.

36. From the date of the APL approval memorandum, APCO has 10 business days to compile the Cybersecurity Assessment Package (CAP).

37. Exceptions to the preceding processes will be coordinated with DISA IE and/or DoD CIO 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 SUT Adjustment Requests

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

- Sponsor POC
- Vendor POC
- Software Version
- Product Model
- System Configuration
- Test Date Adjustment
- 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 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 Information Assurance Vulnerability Management (IAVMs), in order to meet DoD requirements. The implementation of IAVMs will not change the status of a product on the APL. APCO must be notified via DTR so as to ensure that any documentation changes are addressed.

The process to update a SUT is as follows:

1. The Vendor submits Adjustment Request(s) via the [APLITS website](#) and uploads updated supporting documentation. See the [APLITS User Guide](#) for instructions.
2. The APCO distributes the Adjustment Request(s) to the Sponsor, Vendor, Testing AO, and JITC AO to review for accuracy.

3.3 Desktop Review (DTR) Process

For any changes, patch updates, or POA&M closures to a product that is already on the APL, a DTR application must be submitted to the APCO. 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 the existing APL-approved configuration and minor software versions, not major software or major platform changes. Major software version updates and major platform changes will be required to be processed under a new Tracking Number submission.

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 APL. Only after evaluation by the original test team and with concurrence from IE will a final decision be made. For a DTR that does not require additional testing or TDR adjudication, the estimated timeline for DTR completion is 15 business days after the AO provides their recommendation. For DTRs that require testing, the estimated timeline for typical DTR completion is six to nine months from the start of testing setup.

DTRs can also be used to request an extension to the APL certification expiration date for products whose originally approved APL version is still being sold, maintained, and supported through the extended certification period being requested. These products may receive up to an additional 3 years on the APL from the original APL expiration date. An APL extension request can be submitted no earlier than 6 months prior to the original APL expiration date. The Vendor should address all outstanding Cybersecurity POA&Ms and IO TDRs in the DTR submission documentation to include updated POA&M resolution timelines and associated software resolutions as applicable. In limited instances, critical requirements for Cybersecurity or Interoperability may necessitate additional testing for DTR extensions.

1. The Vendor submits a DTR request for review via the APLITS website <https://aplots.disa.mil>. See the [APLITS User Guide](#) for instructions. The Vendor is required to submit release notes and other supporting documentation as applicable (Change Description, updated System Diagram, Delta Summary, etc.) within 5 business days of the DTR request submission. If the supporting documentation package is not received within the 5-business-day window, the DTR request will be cancelled. Note: If the Vendor intends on updating or closing Cybersecurity and/or IO POA&Ms, a list of the applicable findings/POA&Ms being addressed via the DTR needs to be provided in the DTR submission. Additionally, if updating or closing IO POA&Ms that result in a change to the LoC, the Vendor should submit an updated LoC reflecting those changes. If a DTR request includes additional components or products that were not previously included in the SUT and are considered new hardware or new functionality, the Vendor may be asked to provide an updated

System Diagram, System Description and Component List, STIG Questionnaire, and/or LoC, or to make a new submission for a new product.

2. The APCO validates the DTR request against DTR criteria and distributes the DTR request information to the Testing AO for review within 3 business days.
3. The Testing AO conducts a Cybersecurity and IO review and provides a recommendation to the APCO within 5 business days. If testing was not originally conducted at JITC, the Testing AO will provide the JITC AO with a DTR recommendation within 5 business days. The JITC AO will then review and provide APCO its recommendation/concurrence to the Testing AO's recommendation within 5 business days. The JITC AO will present one of the following recommendations to the APCO:
 - a. No testing is required. Recommends that the Final CAR, IO certification, and APL memo be updated.
 - b. Recommends minimal testing. The AO will provide a short, detailed description/justification for the recommendation.
 - Minimal Cybersecurity and IO Testing Required
 - Minimal IO Testing Required with Cybersecurity Vulnerability Scans
 - c. Recommends a new submission. The AO will provide a short, detailed description/justification for the recommendation.

Note: If minimal IO testing only is recommended for a DTR, Cybersecurity scans will still be conducted prior to IO testing to ensure the security posture of the product has not changed.

4. If additional testing is NOT recommended:
 - a. The APCO forwards the recommendation to the APCO Government Lead for review and to provide concurrence or non-concurrence of the recommendation within 3 business days.
 - b. Once the APCO Government Lead concurs with the recommendation, the Testing AO will update the Final CAR and post the IO certification extension within 10 business days of receiving concurrence.
 - c. If JITC is not the assigned test lab, the Testing AO will draft and provide the IO certification to the JITC AO. The JITC AO then has an additional 10 business days to approve and post the IO certification letter to the JITC IO certification page.
5. If additional testing is IS recommended:
 - a. The APCO forwards the recommendation to the APCO Government Lead for review and to provide concurrence or non-concurrence of the recommendation within 3 business days.
 - b. Once the APCO Government Lead concurs with the testing recommendation, testing dates will be scheduled and documentation updates, out-briefs, TDR steps, etc. will be completed post-test as depicted in the APL Process Rules and Guiding Principles section of this guide.

6. During the review and processing of the DTR, an ICM may be scheduled by the assigned AO should further discussion be required to better determine the scope of testing needed.
7. If a change to the SUT is made via the DTR process, the Vendor will provide an updated Military Unique Deployment Guide once the updated Final CAR has been received.
8. Once all required documentation is received, the APCO will proceed with updating the APL memorandum and the CAP with the DTR information.

3.4 DoDIN Modified APL Process (MAP)

The MAP is intended to expedite new device types onto the APL, or to use existing artifacts (test results, LoCs, etc.) to aid in placing products on the APL. The MAP 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 periodically. If the UC Steering Group (UCSG) agrees that new device types and/or new products should be included in the UCR, the DoD Sponsors and Vendors do not have to wait for an updated UCR in order for a product to be tested and placed on the APL. APL testing can begin based on existing requirements that will be placed in the next version of the UCR.

MAP Product Categories

There are three MAP 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 requirements will be verified prior to placement on the APL with coordination of DISA IE and JITC.
2. Operationally Validated- These include current UCR or approved MAP products that are currently fielded and successfully performing from both an IO and Cybersecurity perspective in DoD networks, have an IATO or ATO, and are in compliance with appropriate STIGs. 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 requirements verified prior to APL placement with coordination of DISA IE and JITC based upon an LoC for requirements and/or operational field artifacts (testing artifacts, reports, certifications, etc.).
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.

MAP Submission

To submit a product for APL MAP 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 initial documentation submission. Once the documentation set is complete, a meeting will be scheduled to evaluate product maturity, features affecting assured service, and suitability for APL testing. Meeting participants will include the Vendor, Sponsors, APCO, Action Officers, and the UCR team. The UCSG will be used to provide guidance and issue resolution, as necessary. APCO will disseminate the results of the meeting and related discussions and clarify the way forward to all parties.

APPENDIX A - ACRONYMS

| Acronym | Definition |
|------------------|---|
| AAA | Authentication, Authorization, and Accounting |
| ADFS | Active Directory Federation Services |
| AO | Action Officer |
| AO | Authorizing Official |
| APCO | Approved Products Certification Office |
| APL | Approved Products List |
| APLITS | Approved Products List Integrated Tracking System |
| ATO | Authorization to Operate |
| CA | Certifying Authority |
| CAP | Cybersecurity Assessment Package |
| CAR | Cybersecurity Assessment Report |
| C & A | Certification and Accreditation |
| CCB | Configuration Control Board |
| CRADA | Cooperative Research and Development Agreement |
| CJCSI | Chairman Joint Chiefs of Staff Instruction |
| 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 |
| DoDIN | Department of Defense Information Network |
| DSAWG | Defense IA/Security Accreditation Working Group |
| DSN | Defense Switched Network |
| DTR | Desktop Review |
| FFS | Fee for Service |
| FSO | Field Security Operations |
| ICM | Initial Contact Meeting |
| IATO | Interim Authorization to Operate |
| IA | Information Assurance |
| ICM | Initial Contact Meeting |
| IO | Interoperability |

| Acronym | Definition |
|------------------|---|
| IP | Internet Protocol |
| JIC | Joint Interoperability Certification |
| JITC | Joint Interoperability Test Command |
| JS | Joint Staff |
| LDAP | Lightweight Directory Access Protocol |
| LoC | Letter of Compliance |
| MAP | Modified Approved Products List Process |
| MILDEP | Military Department |
| MIPR | Military Interdepartmental Purchase Request |
| MMD | Multifunction Mobile Device |
| MUDG | Military Unique Deployment Guide |
| NAC | Network Access Control |
| NIAP | National Information Assurance Partnership |
| NIIN | Networks and Information Integration |
| NIPRNet | Sensitive but Unclassified Internet Protocol Router Network |
| NII | Networks and Information Integration |
| NTP | Network Time Protocol |
| NS | Network Services |
| ODC | Other Direct Costs |
| OTPT | One Time Password Token |
| OSD | Office of the Secretary of Defense |
| OSs | Operating Systems |
| PKI | Public Key Infrastructure |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| RADIUS | Remote Authentication Dial-In User Service |
| RAE | Required Ancillary Equipment |
| RTS | Real Time Services |
| SAR | Self-Assessment Report |
| SRG | Security Requirements Guide |
| STIG | Security Technical Implementation Guide (STIG) |
| SUT | System Under Test |
| TACACS+ | Terminal Access Controller Access-Control System |
| TDR | Test Discrepancy Report |

| Acronym | Definition |
|----------------|-------------------------------------|
| TN | Tracking Number |
| TP | Test Procedures |
| T&E | Testing and Evaluation |
| UC | Unified Capabilities |
| 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 2013 (UCR 2013) Change 1, June 2015
- 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
- DoDI 8500.1E, “Information Assurance (IA),” 24 October 2002
- DoDI 8500.2, “Information Assurance (IA) Implementation,” 06 February 2003
- DoDI 8510.01 Change 1, “Risk Management Framework (RMF) for DoD Information Technology (IT),” 24 May 2016

APPENDIX C- DODIN APL DOCUMENTATION GUIDE

INTRODUCTION

Following are the minimum documentation requirements for products submitted to the APCO in support of the APL testing. All products submitted for APL testing must include the initial and follow-on documentation as described below. All submission documentation templates can be found on the [APLITS](#) website.

Initial Required Documentation

- System Diagram
- System Description and Component List Template
- STIG Questionnaire
- LoC Template with signed Cover Letter
- SF-328 Form: Certificate Pertaining to Foreign Interests

All applicants attempting to complete a submission must provide these documents to the APCO to have a Tracking Number assigned and begin processing of the submission for testing. The APCO will confirm receipt of documentation when these requirements have been satisfied.

Follow-on Documentation

- Self-Assessment Report
- Military Unique Deployment Guide

All applicants attempting to complete placement on the APL must first agree to provide these two documents to the APCO in order to receive final APL approval. All documentation should be submitted to the APCO using [APLITS](#).

DOCUMENTATION REQUIREMENTS

1.1 System Diagram

The detailed diagram of the test environment must be submitted in Visio format (.vsd) and include a SUT boundary line and legend. See Figure 2 for an example of an acceptable diagram. Note the Operating Systems (OSs), applications, databases, web servers, Internet Protocol (IP) addresses, etc. applicable to the solution. If there are components needed to provide proof of functionality for the SUT, but not targeted for Cybersecurity and IO certification, these components need to be clearly identified and remain outside the test boundary. The SUT boundary line should clearly identify SUT components. Solution components and connection types that are desired by the Sponsor should be represented in the diagram. Optional components or connection types not requested by the Sponsor should not be included in the SUT diagram submitted to the APCO. The specific details of all connection types supported by the SUT that are to be covered within the certified configuration of the product must be clearly detailed and labeled in the diagram.

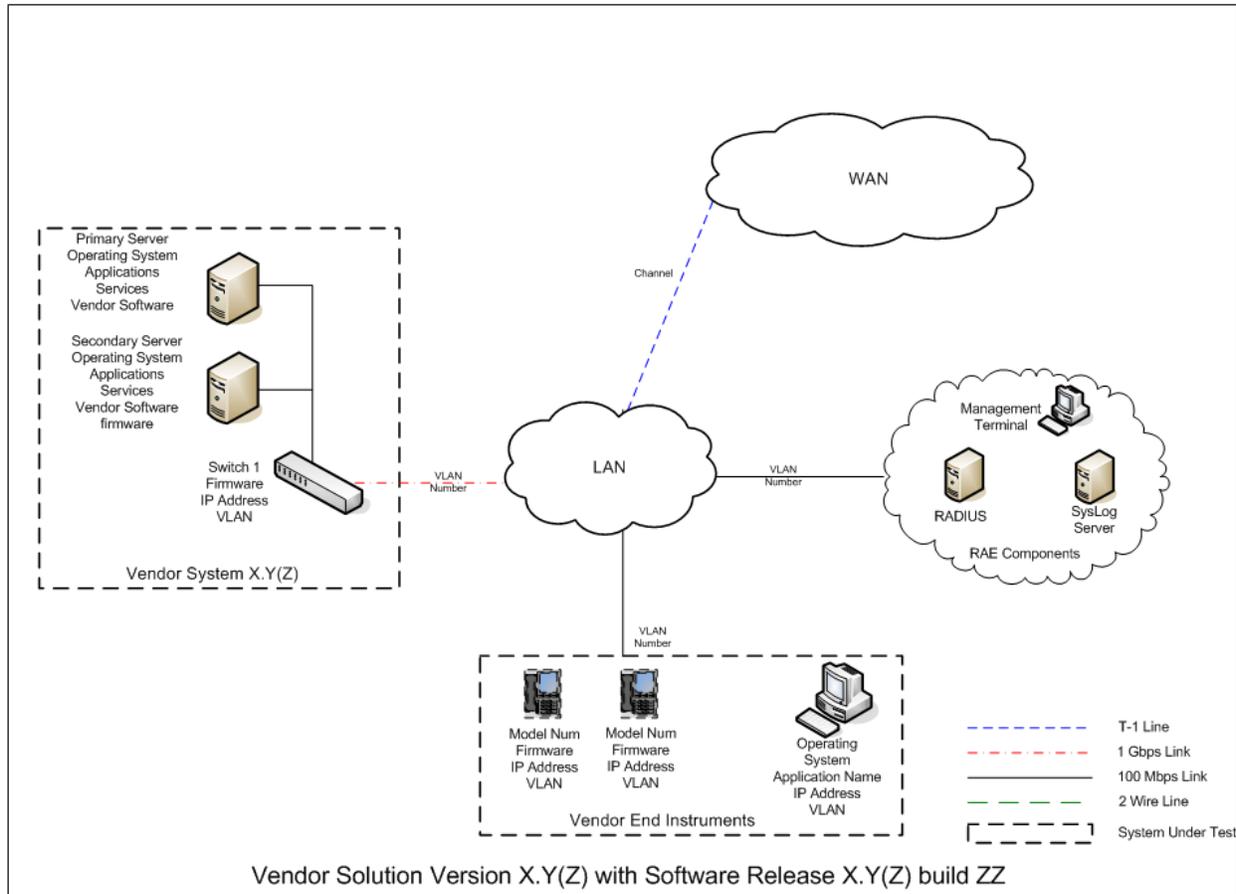


Figure 2: Sample System Diagram

Solution Management

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

- Local Management Only:
 - Management directly connected to the terminal
 - Management directly connected to an administrative Personal Computer (PC)/laptop
- 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.
- 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, the modem must be included in the SUT and subject to full Cybersecurity testing.

Include security features used 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 system diagram. If the solution intends to support option 3, the diagram needs to include remote management and 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.

1.2 System Description and Component List Template

The System Description and Component List Template can be found on the [APLITS](#) website under the DoDIN APL Submission Templates section. Within the template, the Vendor should 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.

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.

If the submitted product has an embedded OS based on a Linux distribution (such as Red Hat Enterprise Linux, CentOS, Ubuntu, etc.), the Vendor must provide the testing center with root or root-level access for a read-only evaluation of the underlying OS and applications (web server, database, etc.) against the appropriate STIG(s)/SRG(s).”

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 APCO.

1.3 STIG Questionnaire

The STIG Questionnaire has been developed to help Vendors analyze their solutions and assist with determining which 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. The STIG Questionnaire template can be found on the [APLITS](#) website under the DoDIN APL Submission Templates section.

1.4 Letters of Compliance (LoC) Template and Cover Letter

Detailed requirements for products and/or functions are provided or referenced in the UCR documentation. In accordance with the UCR, systems are required to have IPv6 capability for testing. All LoC templates can be found on the [JITC Document Depot](#). A link to the JITC Document Depot web page is also available on the [APLITS](#) website under the DoDIN APL Submission Templates section. The LoC template should be submitted for the respective UCR device type with the following requirements included:

- Provide a status for all requirements marked as Required (R).
 - For any partial compliance, state specifically the requirements not complied with.
 - For all non-comply and partial comply responses, provide a POA&M.

- The LoC template must be submitted in Portable Document Format (.pdf) and contain a signed cover letter.
- The signed cover letter must adhere to the following:
 - Submit in .pdf format and be included with LoC Template as the cover page
 - Provide on company letterhead
 - Contain a Vice President-level authority signature

Note: Within each LoC Template, refer to the Instructions tab and Vendor Cover Letter Template tab for further guidance.

1.5 Standard Form 328 (SF-328) - Certification Pertaining to Foreign Interests

All companies submitting for APL testing must submit a current SF-328 with their product documentation. Instructions for filling out the SF-328 can be found at https://www.dcsa.mil/Portals/69/documents/foci/sf328_instructions.pdf. All SF-328 forms must be signed and dated. Any attachments or references mentioned in the Remarks section must be provided. The SF-328 template can be found on the [APLITS](#) website under the DoDIN APL Submission Templates section.

1.6 Vendor Self-Assessment Report (SAR)

A complete Vendor 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 identified open findings. An incomplete Vendor SAR will not be accepted. The Vendor SAR is due to the APCO 10 business days prior to the scheduled Cybersecurity testing start date.

- Previous Cybersecurity testing reports will not be accepted in place of a Vendor SAR. Failure to comply with the Vendor SAR requirement could result in cancellation of the scheduled test dates and possible retirement of the TN.
- The Vendor SAR template will be locked in once received after the ICM. If applicable STIGs have been updated after the Vendor was provided the Vendor SAR template, the Testing AO will include these updated STIGs during testing and the input received in the Vendor's SAR can be transferred to the STIG checklist at the start of Cybersecurity testing.
- All Vendor SARs must be in Excel format using the template provided by the Testing AO.
- To meet the minimum requirements, a Vendor SAR must:
 - Show the status of all STIGs identified in the Vendor SAR template (open, closed, N/A, etc.)
 - Provide mitigations for all open findings. If a status is marked Not Applicable (N/A) please include a short comment explaining why.
 - For retests, provide additional information to show resolution of all items identified during the previous 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, Not a Finding (NF)). 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.

1.7 Military Unique Deployment Guide (MUDG)

Prior to final APL approval, the Vendor is required to submit a Vendor-developed Military Unique Deployment Guide to the APCO. The purpose of this document is to collect, document and make available to the DoD community all configuration changes made to the solution to pass Cybersecurity and IO requirements during testing. The MUDG will provide enough detail to allow a customer to take an out-of-box solution and reconstruct the final configuration of the solution as it was tested and approved.

The following evaluation factors should be considered by the Vendor when developing the document:

- Title the document: Military Unique Deployment Guide
- Include the Vendor's Logo.
- Deployment Guide Date: Must be dated after the final Cybersecurity out-brief or DTR submittal date.
- Include version numbering, document change control history page, specific POC information (email address) for who to submit recommendations for comments/changes, and a page numbering scheme.
- Include a statement instructing the user to reference and follow the Conditions of Fielding (CoF) listed in the Final CAR.
- Include clarifying and/or necessary screen shots, device configuration files, reference tables, and Vendor configuration details/release notes/tweaks that were implemented during testing.

The Deployment Guide can be submitted to the APCO via APLITS at any point after the Final CAR has been received from the AO.

1.8 Modified APL Process (MAP) Documents

Vendors, with assistance from their Sponsors, at a minimum will need to provide the following documentation to be reviewed by the APCO. Additional documentation may be required depending on the MAP category that the product is being submitted under.

- Provide all appropriate ATO supporting documentation including:
 - DIACAP/RMF Scorecard and Artifacts and a copy of the valid ATO/IATO
 - ATO AO Executive Package: This includes the supporting documentation that was provided at the time of the request for an ATO.
 - DoDIN APL New Submission Package:
 - a. System Diagram
 - b. System Description and Component List Template
 - c. STIG Questionnaire
 - d. LoC Template and Cover Letter
 - e. SF 328 Form: Certificate Pertaining to Foreign Interest

APPENDIX D- MITIGATIONS AND POA&MS

INTRODUCTION

This appendix is designed to provide guidance on developing mitigations and POA&Ms for both Cybersecurity and IO.

1.1 Format Examples

The following two examples of mitigations and POA&Ms are provided to assist in the development of Cybersecurity Assessment Reports and include the level of detail required by the CA. It is highly recommended that the following format be used and the mitigations, POA&Ms and comments be provided in blue font.

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. Please specify the date in the MM/DD/YYYY format (i.e. If the fix was to change the products configuration file, the POA&M would state: “The fix is to change the product configuration file to include the directive.....which implementsby MM/DD/YYYY.)

(Note: If the finding cannot be fixed, because of such reasons as technology limitations or the product requires a third party product, then you must request the AO/CA to accept the risk. To do so, please specify: “The Vendor requests the AO/CA 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 some time in Quarter Number or stating a specific date cannot be provided at this time is unacceptable and will delay the process.)

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.

| |
|---|
| <p>a) VULID/STIGID: VMS ID: V0006173/PDI: APP6140</p> <p>Requirement: Log files are not retained for at least one year.</p> <p>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.</p> <p>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.</p> <p>Components Affected (2): Vendor Network Controller A, Vendor Network Controller B</p> <p>Mitigated by RAE: Yes, as proven by the use of an external SYSLOG server.</p> <p>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.</p> |
|---|

Finally, all Internet Protocol Version (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. All Open Ports Table findings should state the use of each port in the Vendor Comment column.

1.2 Cybersecurity POA&M Rules of Engagement

- The Vendor provides quarterly updates, and updates to coincide with scheduled finding POA&M completions.
- The CA and AO approve APL listing with expectation to close POA&Ms.

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 V&V testing necessary to update the solution's 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 IE leadership's discretion:
 - The Vendor either does not respond or responds negatively to the POA&M notification. This results in product removal from the 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 the closure to IE. This results in the product remaining on the APL with the expectation of an expeditious resolution. Timeline to be granted at IE 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 the APL, based on IE leadership decision.

1.3 IO POA&M Rules of Engagement

- Once IO testing has been completed and open TDRs are documented, the Vendor will have 10 business days to provide a response (IO POA&Ms) for the open TDRs. Responses should be made with input and concurrence of the Sponsor. Responses should minimally include:
 - An IO POA&M addressing whether the Vendor plans on resolving the discrepancy
 - Planned resolution timeline
 - Software/hardware implications if the currently defined SUT is not fixed.
- All adjudications with an outcome that would preclude certification (i.e., critical) will be reviewed by DoD CIO, DISA IE, and/or JITC. A final adjudication decision will be provided to the APCO, Vendor, and JITC for appropriate action (i.e. TN retired).
- In the product's lifecycle, if the Vendor's IO POA&Ms are not met, there will be a review of the product's APL validity. 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, IE, and/or JITC for final determination.

APPENDIX E- TESTING COSTS

After a DoDIN APL Tracking Number has been assigned to a submitted product, an Initial Contact Meeting will be scheduled to discuss the scope of testing and the cost model that applies to the product. Costs and fees associated with DoDIN APL testing are arranged between the assigned testing lab and the Vendor or Sponsor, as applicable.

Vendor products used within the DISN core network have the potential to be tested under an Equipment (No Cost) Cooperative Research and Development Agreement (CRADA). DISN edge products are typically tested as Fee for Service (FFS) under a Cost CRADA. The Equipment/No Cost CRADA and FFS Cost CRADA models are defined as follows:

- **Equipment/No Cost CRADA:** The Vendor and Sponsor agree through a legal document that the cost of the Cybersecurity and IO testing will be paid for with the Vendor equipment that is left at the government test facility. With the Equipment/No Cost CRADA, the Government agrees to exchange the cost of their test labor for Vendor equipment. The Government can support Equipment CRADAs for any product determined to be part of the DISN core or essential to the DISA transition to end-to-end IP connectivity for all DoD users.
- **FFS Cost CRADA:** The Vendor or the Sponsor agree through a legal document to pay the Government for the cost of APL testing and for costs 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 CRADA document.

APPENDIX F- UCR 18-MONTH RULE

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

1. If the requirement has been lessened, Vendor compliance is immediate.
2. If the requirement change affects public safety, and is noted as such in the UCR, then compliance is immediate.
3. If the requirement addresses a critical or major Cybersecurity risk, compliance is immediate.
4. If the requirement is necessary for multivendor interoperability, compliance may be immediate as noted in the UCR.
5. All other requirements will become applicable 18 months after the UCR publication date.

If the UCR does not state whether a new requirement is immediate or in 18 months, the requirement is considered an 18-month requirement. If a product is submitted to the DoDIN APL testing process prior to the 18-month effective date, requirements deemed not effective immediately do not have to be met. If a submission is received after the 18-month date, all new requirements will have to be met. Requirement modifications occurring between UCR versions will be posted to the [APLITS](#) website in the UCR section to which it applies. Only critical or major Cybersecurity risk requirement changes between UCR versions will apply to products and will be deemed immediate. Coordination of the requirements that will apply to a product test window to achieve APL status will occur at the ICM and will be based on the scheduled/projected day for the start of testing.

APPENDIX G- NIAP & NIST CERTIFICATIONS

1.1 National Information Assurance Partnership (NIAP)

If a product is a security device or Cybersecurity related tool, it must be either NIAP-certified or proven to be in the NIAP certification process prior to being accepted into the APL process.

If a product is a security device or Cybersecurity related tool, it must fit one of the Protection Profiles (PP) located on the [NIAP website](#) and be submitted for NIAP certification.

The test lab must include the NIAP certification or a status letter as an appendix in the Cybersecurity Assessment Report. Where applicable, the testing lab will utilize existing testing results that cover DoDIN APL Cybersecurity requirements (i.e. DoD Security Annex, NIAP testing, Vendor-Specific STIGS) to minimize the Cybersecurity testing done during the APL process.

1.2 National Institute of Standards and Technology (NIST)

All products providing cryptographic-based security per applicable Federal Law and STIG requirements must be certified to FIPS 140-2 standards per the Cryptographic Module Validation Program (CMVP). Products that are required to have a FIPS 140-2 certification must already be FIPS 140-2 certified or proven to be in process for FIPS 140-2 certification prior to being accepted into the DoDIN APL process. For more information visit the [NIST website](#).

APPENDIX H- MOBILE DEVICE POLICY AND PROCESS

INTRODUCTION

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

Background

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

| USE CASE | 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 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 Services |

Use Cases 1 & 2 Process

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

1. Vendor obtains NIAP PP certification and contacts the [DISA RME](#) to develop a STIG for their product. DISA Approving Officer grants approval to the STIG and the [Cyber Exchange](#) website is updated with a signed STIG Memorandum.
2. Vendor completes the SF-328 form and MMD LoC template. All Use Case #3 requirements in Section 5 should state "N/A to Use Case #2/#1."
3. Vendor submits product on [APLITS](#) website as an MMD or Multifunction Mobile Device Backend Support System (MBSS) and uploads the STIG Memorandum, SF-328, and LoC. The Vendor should specify in the remarks section whether the submission is for Use Case 1 or 2.
4. APCO verifies all submitted documentation and lists the product on the APL within 5 business days.

Use Case 3 Process

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

1. Vendor obtains NIAP PP certification and contacts the [DISA RME](#) to develop a STIG for their product. DISA Approving Officer grants approval to the STIG and the [Cyber Exchange](#) website is updated with a signed STIG Memorandum.

Vendor submits the product in APLITS, specifying that it is a MMD Use Case 3 product and enters the regular APL process identified in Section 3 of this document.

APPENDIX I- REQUIRED ANCILLARY EQUIPMENT (RAE)

Required Ancillary Equipment are systems, servers, devices, or applications deployed in a DoD network with which a Vendor's product (system, device, or application) must interact to meet Cybersecurity requirements in DoD SRGs, STIGs, and DoD policy. Such systems, servers, devices, or applications are external to the Vendor's product or SUT.

RAE typically already exists in the DoD network (enclave or enterprise). If not, the DoD implementer of a Vendor's product may need to deploy specific RAE needed to support the product's deployment. Such systems, servers, devices, or applications support SRG/STIG/policy requirements for, but are not limited to, centralized auditing/logging, centralized network and resource access control, identity management, user/administrator authorization, intrusion detection/prevention, and insider threat.

While RAE may serve as mitigation for, or be required by, various SRG/STIG/policy requirements, RAE may not or cannot address all insider threat and other vulnerabilities, particularly if the RAE is unreachable for whatever reason. This is particularly true for access control to accounts locally provisioned on the system/device and auditing. While mitigating these issues may be done partially through operational constraints, additional mitigations may need to be addressed by the Vendor to minimize operational difficulties.

A list of RAE will be included in each Final Cybersecurity Assessment Report to indicate the minimum list of external systems, servers, devices, or applications with which the Vendor's product must interact to fulfill the Cybersecurity requirements dictated by the SRGs/STIGs and other DoD policy. This list also includes those systems, servers, devices, or applications with which the Vendor's product was tested. It may also include alternate systems, servers, devices, or applications with which the Vendor's product was tested and with which the Vendor's product may interact to fulfill a given Cybersecurity requirement.

NOTE: Some items of RAE may need to be cascaded to fulfill Cybersecurity requirements. For example, an 802.1x authentication server (e.g., Remote Authentication Dial-In User Service (RADIUS) Server) may need to query a PKI server or Directory Server to meet Cybersecurity requirements. Both must be listed as RAE in the Final CAR.

Vendors may provide additional systems, servers, devices, or applications to fulfill the Cybersecurity requirements otherwise fulfilled by DoD provided RAE. Such items would typically be external to the Vendor's core product under evaluation or may be an additional product. Such Vendor provided systems, servers, devices, or applications that fulfill the Cybersecurity requirements otherwise provided by DoD provided RAE must be included in the product's certification boundary/ target of evaluation/SUT or must be evaluated separately as an additional product. As such these devices must be deployed with the Vendor's product and the Final CAR and MUDG must state that fact.

NOTE: RAE items in the Final CAR should be tied to the Cybersecurity requirements they support.

APL RAE List

The APL RAE list contains systems, servers, devices, or applications that may be needed in the DoD environment by a Vendor's product to fulfill its Cybersecurity obligations. This listing does not imply that all Vendors' products must use all items in the list but is, in effect, a menu from which RAE must be selected.

The following is a categorized list of the OPTIONAL systems, servers, devices, or applications that may serve as RAE. The categories are based on the various areas of Cybersecurity

requirements that must be met by all DoD systems including Vendor's products deployed in the DoD environment. A Vendor's product must leverage one or more items in each category.

Auditing/Logging:

- Syslog Server
- SNMP management station
- Other audit/logging record collection server

Access control, identity management, user/administrator authorization:

- Authentication, Authorization, and Accounting (AAA) Servers
 - RADIUS Server
 - Terminal Access Controller Access-Control System (TACACS+) Server
 - Other AAA servers
- 802.1x Network Access Control (NAC) server
- Microsoft Active Directory Server
- Microsoft Active Directory Federation Services (AD FS) (for single sign-on)
- Other Lightweight Directory Access Protocol (LDAP) based Directory Servers
- DoD PKI CA server
- DoD PKI Online Certificate Status Protocol (OCSP) responder server
- One Time Password Token (OTPT) server
 - RSA SecureID Server
 - NC-PASS Server
 - Other OTPT server

Intrusion Detection/Prevention:

- HBSS EPO server

The following is a list of MANDATORY systems, servers, devices, or applications that must be implemented externally to the Vendor's product in the network environment with which it must interact or from which it must obtain service; and which must appear in the Vendor's product's RAE list:

Auditing/Logging:

- External Network Time Protocol (NTP) server – Required for synchronization of audit records across multiple systems in addition to the Vendor's product. A Vendor's product must ingest NTP and use the time codes provided to time stamp audit records.