DEPARTMENT OF DEFENSE UNIFIED CAPABILITIES APPROVED PRODUCTS LIST TEST SUBMITTAL DOCUMENTATION GUIDE

April 2009

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

The following document outlines the minimum requirements for acceptable documentation intended for submittal to the Unified Capabilities Certification Office (UCCO) in support of the Unified Capabilities Approved Products List (UC APL) testing. Anyone attempting to access the UC APL Test Submittal Form is first routed through an introductory banner page where the following documentation requirements are outlined:

1.1 Pre-Tracking Number Documentation

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

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

The preferred method to receive documents is via electronic means. Vendors and sponsors are welcome to email the documents if less than 10MB or create an FTP site for download. If this cannot be accomplished, regular mail may be used. The UCCO will confirm receipt of documentation when the above requirements have been satisfied.

All documentation should be submitted to the UCCO at the following address:

Oberon Associates Inc.,
ATTN: UCCO UC APL Documentation
9700 Capital Court, Suite 301
Manassas, VA 20110
E-mail:
ucco@disa.mil
Phone:
UCCO Process Manager : (703)882-0762
UCCO Process Questions : (520)538-3234

2 Solution Documentation

2.1 Documentation Format

Acceptable formats for product documentation are the following:

- Microsoft PowerPoint,
- Microsoft Word,
- Adobe Acrobat Portable Document Format (PDF),

- Microsoft Visio (Preferred), and
- Microsoft Paint.

If Visio is used, please note the Visio version (i.e., 2000 Technical, 2002 Standard or 2003 Professional, etc.). When submitting the documentation, include the .vsd file. If the diagram is incorporated inside the system and component description document, the .vsd file is still required to be sent. If an Adobe Acrobat file is sent, ensure that the file is not protected against copying, printing, or selection.

Table 2.1 – Documentation Checklist

Diagram	□
System description	□
Component description	□
Maintenance and operating manuals	□
Whitepapers	□
STIG Questionnaire	□

2.2 System Description

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

2.3 Solution Components

All solution components that will be involved in the testing of the solution need to be clearly identified in the solution’s product documentation. If there are components needed to provide proof of functionality for the System Under Test (SUT), but not targeted for Interoperability (IO) and Information Assurance (IA) certification, these components need to be clearly identified and remain outside the test boundary. The test boundary should be clearly identified within the diagram using lines around the components of the SUT. The only solution components that are represented in the diagram as part of the SUT should be those components desired by the government sponsor of the solution. No optional solution components that are available for purchase not requested by the government sponsor should be included in the SUT diagram submitted to the UCCO. See Figure 2.1 as example of an acceptable solution diagram.

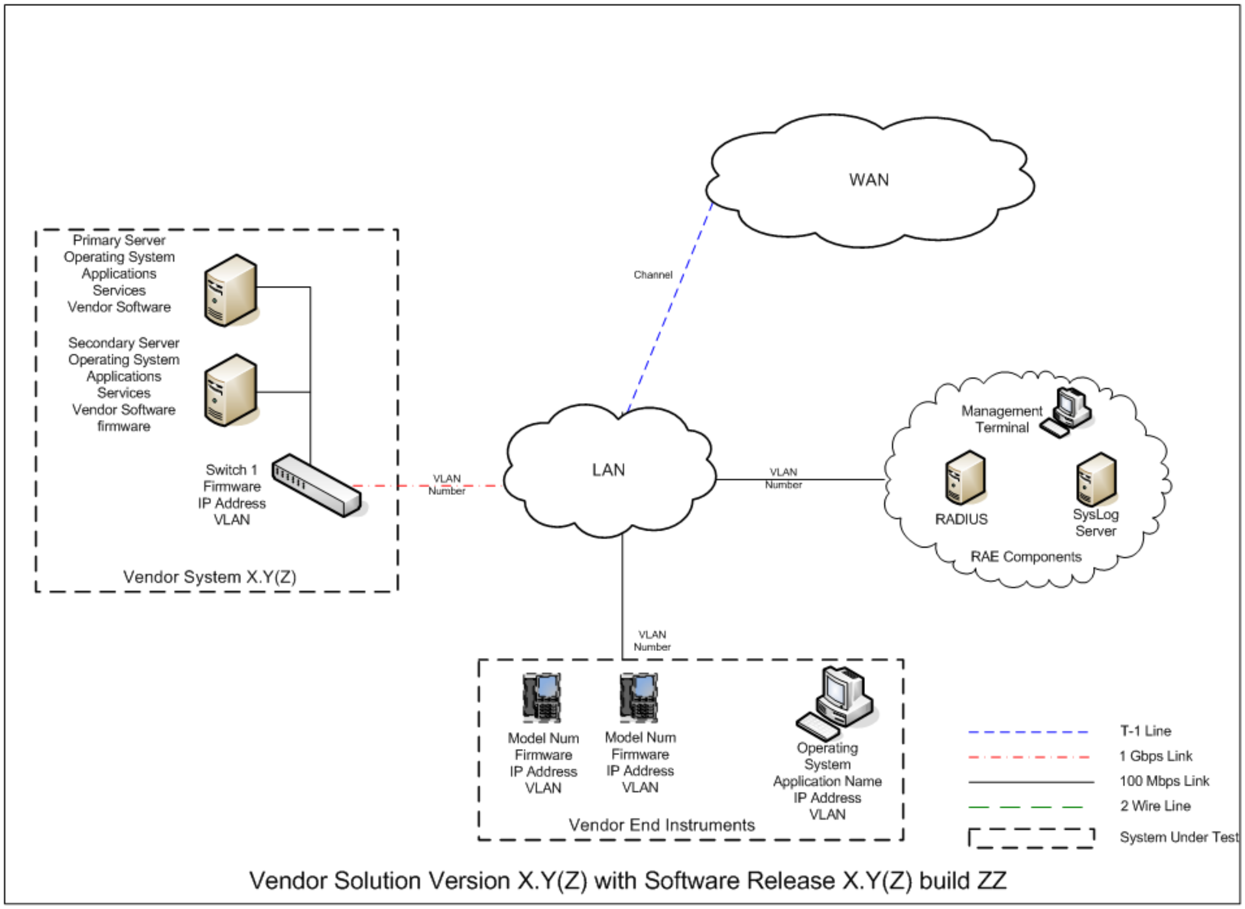

Figure 2.1 – Sample Diagram for Submission

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

2.4 Component Description

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

Use the following format as an example:

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

1) Hardware. The model, not the host name,

2) OS. This includes versions and any Service Pack (SPs),

3) Application. Custom vendor software version 4.2, Microsoft Structured Query Language (SQL) 2000 SP4, McAfee Enterprise 8.0.0i.,

4) Firmware, and

5) IP address (If known).

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

1) Hardware. The Model, not the host name (i.e., Vendor Chassis):

    a. Card 1- Card 1's description,

    b. Card 2- Card 2's description, and

    c. Additional components as needed,

2) OS. This includes versions and any SPs,

3) Application. Custom vendor software Version 4.2, SQL 2000 SP4, McAfee Enterprise 8.0.0i.,

4) Firmware, and

5) IP address.

2.5 Solution OSs

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

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

2.6 Solution Applications

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

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

2.7 Solution Connections

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

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

2.8 Solution Management/Administration

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

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

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

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

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

2.9 DISN UC APL 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 break out of all the components, software applications, general environment configuration, protocols and management methods used by the solution.

Once the applicant has completed the STIG Questionnaire and submitted it to the UCCO, the applicant must then complete a Self-Assessment of the solution. The Self-Assessment is due to the UCCO two weeks prior to all scheduled UC APL testing (IO or IA), and consists of applying all STIGs identified from completing the STIG Questionnaire.

For all STIGs that have automated scripts available, the results from applying those to all components of the solution showing all status (i.e., open, closed, Not Applicable [N/A], etc.) need to be included in the Self-Assessment package. The majority of the automated scripts generate multiple files for different uses, with one containing all the consolidated findings. If that document is available from the automated script, then it is sufficient instead of sending all the raw output data from the scripts. Other acceptable options are pulling all the vulnerability data from the raw output of the scripts and consolidating into either a Microsoft Excel, Microsoft Word, etc.

For those STIGs that do not have an automated script available and have to be completed manually, the results from applying the STIG should be documented in the STIGs support Security Checklist and included in the Self-Assessment package.

The format of how a Self-Assessment is developed is at the discretion of the applicant, as long as it is done using one of the tools identified earlier as supported by DOD users (i.e., Microsoft Word, Microsoft Excel, etc) and contains the following minimum requirements necessary to be considered a complete Self-Assessment:

1) Shows the status of all STIG identified in the STIG Questionnaire (open, closed, N/A, etc.),
2) Has completed mitigations for each Open finding. If a status is marked N/A please include a short comment detailing why it is considered N/A., and
3) If the Self-Assessment is for a retest, have additional requirement to show resolution of all items identified during the previous solution outbrief.

2.10 Post Tracking Number Documentation

1) Self-Assessment Review (SAR), and
2) Deployment Guide.

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

2.10.1 SAR

Once the applicant has completed the STIG Questionnaire and submitted the completed questionnaire into the UCCO, and the questionnaire has been validated during the Initial Contact Meeting, the applicant must then complete a Self-Assessment of the solution. The Self-Assessment is due to the UCCO two weeks prior to all scheduled APL testing (IO or IA). For all STIGs/checklists that have automated scripts available, the results from applying those to all components of the solution showing all status (i.e., open, closed, N/A, etc.) need to be included in the Self-Assessment package. For those STIGs/checklists that do not have an automated script available and must be completed manually, the results from applying the checks should be documented in the STIG’s support Security Checklist and included in the Self-Assessment package.

2.10.2 SAR-Updated November 06, 2007

All testing applicants must submit a SAR of their solution to the UCCO prior to IA testing. A completed SAR is a representation of findings from current STIGS applicable to the solution (identified by the STIG questionnaire and verified during the Initial Contact meeting) to include mitigation statements for all open findings. The SAR is due to the UCCO two weeks prior to scheduled APL testing. Our office highly encourages Self-Assessment Reports be submitted at least one-week prior to the 2-week deadline to prevent last minute cancellations.

The submitted STIG Questionnaire is part of the documentation requirement and located within this document. During the Initial Contact Meeting, any questions regarding the complete process will be addressed, to include IO and IA requirements. Also, any additional STIGs that need to be applied to a product will be identified during the ICM and will be required for the SAR.

For all STIG(s)/checklists that have automated scripts available, the results from applying them to all components of the solution, showing all status (i.e., open, closed, N/A, etc.) need to be included in the SAR package. For those STIG(s)/checklists that do not have an automated script available and must be completed manually, the results from applying the checks need be documented in the STIG's support Security Checklist and included in the Self-Assessment package.

****Note** -** If the SAR is incomplete (STIGs identified during the ICM are not present or mitigation statements are missing for open findings) and it is beyond the 2-week deadline, the result will be to retire and cancel the testing effort.

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

2.10.3 Sample SAR Verbiage

STIG Format (Example)

VULID/STIGID: VMS ID: V0004369/PDI: GEN003960

Requirement: The traceroute command is not owned by root.

Finding: Excessive permissions for the traceroute command are given to the switch user account. If a packet filter firewall is configured incorrectly, an attacker can use the traceroute command, through the firewall, to obtain knowledge of the network topology inside the firewall. The information may allow an attacker to determine trusted routers and other network information that may lead to system and network compromise.

Mitigation: All system commands and functions performed by root account are audited and flag for immediate review by system on a daily basis.

Components Affected (5): Insert which components are affected here (Component A primary and secondary, Component B common, Component C and D Backup.)

3 DEPLOYMENT GUIDE

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

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

- Screen shots,
- Device configuration files,
- Reference table to specific portions of a solution’s User Guide that provides information on addressing a specific issue, and
- Vendor configuration details/release notes/tweaks implemented during testing.

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