

**Unified Capabilities Approved Products List (UC APL)
Security Technical Implementation Guide (STIG)
Applicability Questionnaire**

For Developers and Vendors

Version 4, Release 1



February 2016

Developed by DISA for the DoD

1. INTRODUCTION

Per the Unified Capabilities (UC) Approved Product List (APL) Process Guide, the vendor is required to complete the Security Technical Implementation Guide (STIG) Questionnaire. All products or systems on a Department of Defense (DoD) network is required to be secured in accordance with the applicable DoD STIGs. To use this questionnaire, answer the questions below by checking the boxes. Each checked box indicates one or more required STIGs, checklists, Security Requirements Guides (SRGs), or tools. Please refer to the Information Assurance Support Environment (IASE) website for a list of all of the STIGS, checklists, SRGs, Security Content Automation Protocol (SCAP) Benchmarks, and Security Readiness Review (SRR) Evaluation Scripts.

<http://iase.disa.mil/>
<http://iase.disa.mil/stigs/index.html>

If you do not have access to the IASE website, please request the items from your sponsor.

An engineer who is fully knowledgeable of the system to be tested must complete this technical questionnaire. This engineer should also be knowledgeable in Information Assurance (IA) and participate in or will directly support the testing effort.

Name of the Product or System: _____

Model of the Product or System: _____

Version and patch level of the Product or System: _____

Firmware/Kernel: _____

First time in the UC Process Product currently on APL- what changed:
 Version(s) Component(s)

If the product has been tested by another US Government or Department of Defense (DoD) entity, please complete this section and upload documentation with submission.

 Purpose for the test

 Name and location (if known) of the entity conducting the test

 The dates (rough estimate is okay) testing occurred

List each component - defined as a single device or box that has a single instance of an operating system. (if you need more space, please print this page and add the additional devices)

1. Functional name of the device: _____

Function performed: _____

2. Functional name of the device: _____

Function performed: _____

3. Functional name of the device: _____
 Function performed: _____
4. Functional name of the device: _____
 Function performed: _____
5. Functional name of the device: _____
 Function performed: _____
6. Functional name of the device: _____
 Function performed: _____
7. Functional name of the device: _____
 Function performed: _____
8. Functional name of the device: _____
 Function performed: _____

2. SOLUTION OR SYSTEM GENERAL TYPE AND/OR FUNCTION

UC Category

Voice, Video, and Data Services

- Classified Voice
- Classified Video
- Data
- SBU Voice
- SBU Video
- Multi Function Mobile Devices

Network Infrastructure

- Transport
- Routers/Switches
- Security
- Enterprise Network Management
- Storage

Device Type/Functions

Check all that applies:

- | | |
|--|--|
| <input type="checkbox"/> OTS | <input type="checkbox"/> Operation Support System |
| <input type="checkbox"/> Fixed Network Element (F-NE) | <input type="checkbox"/> Customer Edge Router (CER) |
| <input type="checkbox"/> Deployed Network Element (D-NE) | <input type="checkbox"/> Access IP Switch |
| <input type="checkbox"/> Access Aggregate Function M13 | <input type="checkbox"/> Distribution IP Switch |
| <input type="checkbox"/> Data Firewall (DFW) | <input type="checkbox"/> Wireless LAN (WLAS) |
| <input type="checkbox"/> An Application | <input type="checkbox"/> Core IP Switch |
| <input type="checkbox"/> Element Management System (EMS) | <input type="checkbox"/> Mobile Devices |
| <input type="checkbox"/> Data Storage Controller | <input type="checkbox"/> Enterprise Session Controller (ESC) |
| <input type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> Network Access Control (NAC) |
| <input type="checkbox"/> WAN Soft Switch | <input type="checkbox"/> Link Encryptors |
| <input type="checkbox"/> Wireless Intrusion Detection System
(WIDS) | <input type="checkbox"/> Intrusion Detection System
(IDS)/Intrusion Protection System (IPS) |
| <input type="checkbox"/> AS-SIP End Instrument | <input type="checkbox"/> Local Session Controller (LSC) |

- | | |
|--|--|
| <input type="checkbox"/> Session Boarder Controller (SBC) | <input type="checkbox"/> Mass Notification Warning System (MNWS) |
| <input type="checkbox"/> Internet Protocol End Device (IPED) | <input type="checkbox"/> Multifunction Mobile Device Backend Support System (MBSS) |
| <input type="checkbox"/> Network Infrastructure Product (NISP) | <input type="checkbox"/> Wireless End Bridge (WEB) |
| <input type="checkbox"/> Wireless End Instrument (WEI) | <input type="checkbox"/> Radio Gateway |
| <input type="checkbox"/> Passive Optical Network (PON) | <input type="checkbox"/> Cybersecurity Tool (CYBT) |
| <input type="checkbox"/> Soft Switch (SS) | <input type="checkbox"/> Multifunction Mobile Device (MMD) |
| <input type="checkbox"/> Conference Bridge | |
| <input type="checkbox"/> Assured Services LAN (ASLAN) | |

Solution Management

- The management application includes a vendor application and coding. The **Application Security and Development STIG** is applicable.
- No separate management application – part of the device operating system - built into the network device. The **Network Device Management SRG** is applicable.

The solution is managed – Check all that apply:

- From a client via HTTPS
- Installed executable locally on server
- Installed executable on a client
- Locally via a directly connected external terminal or emulator

Specify Interfaces and Technology(s): _____

- Remotely across a Network_____

Specify Interfaces and Technology(s): _____

- Remotely via Dialup_____

IA/Encryption

- Encryption is used. Type_____
- The encryption module or software tool kit is FIPS 140-2 validated.
To verify: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>
- The encryption is NSA type 1 certification.

Listing of the encryption module(s)/algorithm(s) used

Encryption module(s) vendor(s)

Certification number(s)

Validation level(s)

- If IA or IA-Enabled product, the product is Common Criteria or NIST certified
To verify: <https://www.niap-ccevs.org/Product/VPL.cfm> (submit certificate)
- If IA or IA-Enabled product, the product is in the process of seeking Common Criteria or NIST certification (submit letter with status or acceptance in the process)

Name of the Common Criteria Testing Laboratory (CCTL)

Protection Profile (PP)

Evaluation Assurance Level (EAL)

Evaluation Report Number

Date of Issuance

- The product use PKI or X.509 type certificates.
- The system is DoD PKI enabled or compatible.
- The system supports DoD Common Access Card

To request test certificates:

http://jitc.fhu.disa.mil/projects/pki/pke_lab/app_testing/app_testing.aspx

3. NETWORK

- IPV6 is supported

Backbone Transport STIG/Checklists: (check all that applies)

- | | | |
|--|--|---|
| <input type="checkbox"/> Optical Transport | <input type="checkbox"/> DWDM NE | <input type="checkbox"/> Router |
| <input type="checkbox"/> SONET NE | <input type="checkbox"/> ODXC | <input type="checkbox"/> MPLS |
| <input type="checkbox"/> MSPP NE | <input type="checkbox"/> Backbone/Core | <input type="checkbox"/> Internet Access Points |

Router Checklists: (check all that applies)

- Cisco Router Procedure Guide (Supplement to BTS)
- Juniper Router Procedure Guide (Supplement to BTS)
- Router SRG

Network Infrastructure Checklists: (check all that applies)

- Firewall
- Router Layer 3 Switch
- Layer 2 Switch
- Other Device
- Perimeter Router Layer 3 Switch
- Network WLAN

- Network WMAN
- Network Policy
- Other – Please Specify with version: _____

Arista Multilayer Switch (MLS) DCS-7000 Series

- NDM
- Router
- Layer 2 Switch

Palo Alto Networks

- Application Layer Gateway
- IDPS
- NDM

Riverbed SteelHead

- Application Layer Gateway
- NDM

4. OPERATING SYSTEM

Windows Operating System, check the applicable checklist and benchmark:

- Windows 2008 Server - Stand Alone/Member Domain Controller R2
- Windows 2012 Server - Stand Alone/Member Domain Controller R2
- DNS
- Windows 7 Professional
- Windows 8 Professional
- Windows 10 Professional
- Windows Vista

Mac Operating System, check the applicable checklist and benchmark:

- MAC OS X 10.5 10.6 10.8
- Apple OS X 10.8 10.9 10.10

- Operating System Security Requirements Guide

UNIX flavor Operating System, check the applicable checklist and benchmark:

- SUN Solaris 10 11 AND SPARC X86
- Red Hat (CentOS) 5 6
- HPUX 11.23 11.31
- AIX 6.1

The **General Purpose Operating (SRG)** is applicable to all other flavors not listed above

Other – Please Specify with version: _____
(ie VxWorks,)

The UNIX or Linux is embedded

Note: The STIGs are not applicable if the OS is embedded and there is no access to a command line from any interface to make OS configuration changes. Additionally, a password must be enabled on the BIOS and bootloader.)

5. SOFTWARE AND APPLICATIONS

Web Server and/or Application Services STIG, check the applicable checklist.

- Apache 2.2
- IIS 6
- IIS 7 (use for 7.5)
- IIS 8 and 8.5 (Use Webserver SRG)
- Web Policy
- Web Server SRG
- Other – Please Specify: _____

The application uses a HTTP browser or mobile code such as Internet Explorer or Mozilla (or other) to access any portion of its functionality or management.

- Mozilla Firefox SRG
- Google Chrome STIG
- Web Policy Manual STIG

Supported	Required	Test with	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Firefox
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IE v6
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IE v10
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IE v11
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Other: Please Specify - _____

If application uses mobile code.

Please Specify: _____

The system supports antispyware and Commercial-Off-The-Shelf Products (MS Office)
 Select the applicable checklists.

- MS Office 2007
- MS Office 2010
- MS Office 2013
- The Desktop Application General STIG is applicable.
- The Desktop Application Antispyware General STIG is applicable.
- Other – Please Specify: _____

The system store information (such as configuration information) in tables or use a file structure that would typically be known as a database. Determine the applicable database checklist and SRR scripts below:

- Oracle 11g Oracle 11.2g Oracle 12c
- Oracle Linux 5 Oracle Linux 6
- SQL Server 2012
- Access 2007 Access 2010 Access 2013
- MS-SQL Server

The database a back-end-to the application with no user access

The **Database Security Requirements Guide (SRG)** is applicable to all other databases not listed above

Other – Please specify with version: _____
 (MySQL, Access,)

Determine if the **Application Server SRG** is applicable by selecting the below checklists:

- Tomcat
- Weblogic
- Sun Java
- JVM J2SE
- Application Server
- Java Runtime Environment (JRE) 6 STIG
- Java Runtime Environment (JRE) 7 STIG

F5 BIG-IP

- Access Policy Manager (APM) Advanced Firewall Manager (AFM)
- Access Security Manager (ASM) Device Management 11.x
- Local Traffic Manager (LTM)

The system uses **.NET Framework**. Check the applicable checklist

- MS .NET Framework 4 and benchmark
- .NET Framework Security for versions 1.0, 2.1, 2.0, 3.0, and 3.5

Note: See the NSA Guide to Microsoft .NET Framework Security,

The system contains a **Domain Name Services (DNS)** server

- DNS SRG is applicable.
Please Specify: _____
- BIND DNS STIG is applicable.

6. MOBILE DEVICES

The system is a **mobile device**, check the applicable checklist:

- Android OS 5.0
- Apple iOS 9
- Blackberry 10 OS
- LG Android 5.0 ISGC
- Mobile Policy SRG
- Samsung Android
- Samsung Android (with Knox)
- Windows Phone 8.1
- Other: _____

7. OTHER FEATURES AND CAPABILITIES OF THE SYSTEM

The below exists within the system:

- Citrix XenAPP

The system supports telecommunications traffic in the form of voice, video, data (via modem) or fax.

- Defense Switch Network is applicable.
- Video Tele-Conference Services Policy

The system supports Virtual Network, check the applicable checklist.

- | | |
|--|--|
| <input type="checkbox"/> ESXi5 Server | <input type="checkbox"/> VMware vSphere 6.0 vCenter Server for Windows |
| <input type="checkbox"/> ESXi5 Virtual machine | <input type="checkbox"/> VMware vSphere 6.0 VM |
| <input type="checkbox"/> ESXi5 vCenter Server | <input type="checkbox"/> VMware vSphere 6.0 ESXi |
| <input type="checkbox"/> ESX Server | |

The system is a MS Exchange Server

- MS Exchange 2003
- MS Exchange 2010

The system is an Intrusion Detection System / Intrusion Protection System

- Intrusion Detection and Prevention System SRG

The system is an IPSEC VPN

IPSEC VPN Gateway STIG

The system is a Keyboard Video and Mouse (KVM) solution.

Keyboard Video and mouse Switch STIG is applicable.

The system is a Multifunction Devices (MFD) and Printer solution.

The MFD and Network Printers STIG

The system supports remote access and/or management.

- Remote Access Policy STIG
- Remote Access VPN STIG
- Remote Endpoint STIG
- Remote XenAPP ICA Think Client
- Remote Storage STIG

The system supports VVoIP technology.

- Voice and Video over Internet Protocol Pol
- Remote Access Server STIG

The system supports Wireless technology.

Wireless STIG

8. PROTOCOLS

Check off all of the following protocols that are used by the system/device:

- | | | |
|-------------------------------|--|----------------------------------|
| <input type="checkbox"/> FTP | <input type="checkbox"/> TLS Version _____ | <input type="checkbox"/> SIP-TLS |
| <input type="checkbox"/> TFTP | <input type="checkbox"/> IPSEC | <input type="checkbox"/> AS-SIP |
| <input type="checkbox"/> SFTP | <input type="checkbox"/> SSH Version _____ | <input type="checkbox"/> SIP |
| | <input type="checkbox"/> SSL Version _____ | |

- | | | |
|--------------------------------|--------------------------------|-------------------------------|
| <input type="checkbox"/> BootP | <input type="checkbox"/> h.323 | <input type="checkbox"/> RTP |
| <input type="checkbox"/> RCP-1 | <input type="checkbox"/> h.320 | <input type="checkbox"/> SRTP |

- LDAP
- SMTP
- SNMP Version _____

- Proprietary Signaling Protocol – Detail: _____
- Proprietary Bearer Protocol – Detail: _____
- Other – Please Specify: _____