Department of Defense Information Network (DoDIN) Approved Products List (APL) Security Technical Implementation Guide (STIG) Applicability Questionnaire

For Developers and Vendors

Version 4, Release 5

JULY 2018

Developed by DISA for the DoD

1. INTRODUCTION

Per the Department of Defense Information Network (DoDIN) 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 Cybersecurity (CS) and participate in or will directly support the testing effort.

Vendor/Company Name of the Product or System:

_____

Model Name of the Product or System:

_____

Version and patch level of the Product or System: _____

Firmware/Kernel: _____

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

If the product has been tested by another US Government or 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:

- ☐ DISN OTS
- ☐ Fixed Network Element (F-NE)
- ☐ Deployed Network Element (D-NE)
- ☐ Access Aggregate Function M13
- ☐ Data Firewall (DFW)
- ☐ An Application
- ☐ Element Management System (EMS)
- ☐ Data Storage Controller
- ☐ Virtual Private Network (VPN)
- ☐ WAN Soft Switch
- ☐ Operation Support System
- ☐ Customer Edge Router (CER)
- ☐ Access IP Switch
- ☐ Distribution IP Switch
- ☐ Wireless LAN (WLAS)
- ☐ Core IP Switch
- ☐ Mobile Devices
- ☐ Enterprise Session Controller (ESC)
- ☐ Network Access Control (NAC)
- ☐ Link Encryptors

- ☐ Wireless Intrusion Detection System (WIDS)
- ☐ AS-SIP End Instrument
- ☐ Session Boarder Controller (SBC)
- ☐ Internet Protocol End Device (IPED)
- ☐ Network Infrastructure Product (NISP)
- ☐ Wireless End Instrument (WEI)
- ☐ Passive Optical Network (PON)
- ☐ Soft Switch (SS)
- ☐ Conference Bridge
- ☐ Assured Services LAN (ASLAN)
- ☐ AEI Voice
- ☐ Data Storage Controller
- ☐ DoD Secure Communications Device (DSCD)
- ☐ EDS Gateway
- ☐ UC Conference System
- ☐ Wireless Access Bridge (WAB)
- ☐ Wireless
- ☐ Intrusion Detection System (IDS) / Intrusion Protection System (IPS)
- ☐ Local Session Controller (LSC)
- ☐ Mass Notification Warning System (MNWS)
- ☐ Multifunction Mobile Device Backend Support System (MBSS)
- ☐ Wireless End Bridge (WEB)
- ☐ Radio Gateway
- ☐ Cybersecurity Tool (CYBT)
- ☐ Multifunction Mobile Device (MMD)
- ☐ Customer Premise Router (CPE)
- ☐ DISN Router (DISN-R)
- ☐ E911 Management System
- ☐ UC Collaboration Product (UCCP)
- ☐ Video Distribution System (VDS)
- ☐ Video Teleconferencing (VTC)
- ☐ Wide Area Router/Transport (WRT)
- ☐ XMPP Client/Server

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

Required Ancillary Equipment (RAE)

Please see Appendix I of the DoDIN APL Process Guide for approved RAE technology.
If RADIUS/TACAC+ is supported: TACACS+, CHAP-types, PAP/SPAP, and use of MD5 are invalid due to lack of FIPS-approved algorithms.

Cybersecurity/Encryption

☐ Encryption is used. Type_____
☐ The encryption module or software tool kit is FIPS 140-2 validated by NIST.
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 Cybersecurity or Cybersecurity-Enabled product, check the appropriate box:

☐ The product is NIAP certified
To verify: https://www.niap-ccevs.org/Product/VPL.cfm (vendor submit certificate)

☐ The product is in the process of seeking NIAP certification (vendor submit letter with status or acceptance in the process)

_____
Name of the Common Criteria Testing Laboratory (CCTL)

_____
Protection Profile (PP)

_____
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)

☐ Optical Transport ☐ DWDM NE ☐ Router
☐ SONET NE ☐ ODXC ☐ MPLS
☐ MSPP NE ☐ Backbone/Core ☐ Internet Access Points

Router Checklists: (check all that applies)

☐ Cisco Router Procedure Guide (Supplement to BTS)
☐ Router SRG

Cisco IOS XE: ☐ Router STIG ☐ NDM STIG

Network Infrastructure Checklists: (check all that applies)

☐ Firewall
☐ Application Layer Gateway SRG
☐ Layer 3 Switch ☐ Router ☐ CISCO ☐ Juniper
☐ Layer 2 Switch ☐ CISCO
☐ Other Device
☐ Perimeter Layer 3 Switch ☐ Router ☐ CISCO ☐ Juniper
☐ Network WLAN
☐ Network WMAN
☐ Network Policy
☐ Other – Please Specify with version: _____

Arista Multilayer Switch (MLS) DCS-7000 Series

☐ NDM
☐ Router
☐ Layer 2 Switch

Riverbed SteelHead CX

☐ Application Layer Gateway
☐ NDM

HP FlexFabric Switch

☐ Layer 2 Switch ☐ Router ☐ NDM

Juniper SRX Services Gateway

☐ Application Layer Gateway ☐ IDPS ☐ NDM ☐ VPN

☐ McAfee MOVE
☐ McAfee Virus

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 2016 ☐ Windows 10 Professional

MAC Operating System, check the applicable checklist and benchmark:

MAC OS X ☐ 10.6
Apple OS X ☐ 10.8 ☐ 10.9 ☐ 10.10 ☐ 10.11

☐ 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) ☐ 6 ☐ 7
☐ HPUX ☐ 11.31
☐ AIX ☐ 6.1
☐ SUSE Linux Enterprise Server

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

☐ Other – Please specify with version: _____
(i.e. VxWorks)

☐ The UNIX or Linux is embedded
Note: Embedded means there is no access to a command line from any interface to make OS configuration changes. A system built on a proprietary OS (such as Cisco's IOS) or built on the Linux Kernel (such as HPE Aruba's ArubaOS) will also be considered embedded. However, if the embedded OS Linux distribution, such as CentOS, then the test lab must be given root access and the GPOS SRG/OS STIG will be applied. This will be discussed during the ICM.

5. SOFTWARE AND APPLICATIONS

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

☐ Apache 2.2 ☐ Windows ☐ UNIX
☐ IIS 7 (use for 7.5)
☐ IIS 8 (Use 8.5)

☐ IIS 8.5
☐ 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	
☐	☐	☐	Firefox
☐	☐	☐	IE v10
☐	☐	☐	IE v11
☐	☐	☐	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 2010 ☐ MS Office System 2010
☐ MS Office 2013 ☐ MS Office System 2013
☐ MS Office 2016 ☐ MS Office System 2016
☐ 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 HTTP Server
☐ Oracle Linux 5 ☐ Oracle Linux 6
☐ Oracle Exadata
☐ SQL Server 2012 ☐ SQL Server 2014
☐ Access 2010 ☐ Access 2013 ☐ Access 2016
☐ 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 ☐ Oracle Weblogic Server 12c
☐ Sun Java
☐ JVM J2SE

☐ Application Server
☐ JBoss
☐ Oracle JRE 8 Windows ☐ Oracle JRE 8 Unix

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, Release 3, Release 4
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: _____

Other
☐ HBSS

6. MOBILE DEVICES

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

☐ Apple iOS 10
☐ Mobile Device Management (MDM) Server Policy STIG
☐ Mobile Policy
☐ Samsung Android 5 ☐ Samsung Android 6 ☐ Samsung Android 7
☐ Samsung SDS EMM
☐ Other: _____

BlackBerry

☐ Blackberry BES ☐ BlackBerry Enterprise Service
☐ BlackBerry Device Service ☐ BlackBerry OS ☐ 10.3

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.

☐ Video Services Policy
☐ Video Tele-Conference STIG

The system supports Virtual Network, check the applicable checklist.

☐ ESXi5 Server
☐ ESXi5 Virtual Machine
☐ ESXi5 vCenter Server
☐ VMware vSphere 6.0 vCenter Server for Windows
☐ VMware vSphere 6.0 VM
☐ VMware vSphere 6.0 ESXi

☐ VMware NSX Distributed FW
☐ VMware NSX Distributed Logical Router
☐ VMware NSX Manager

The system is a MS Exchange Server

☐ MS Exchange 2010
☐ MS Exchange 2013

The system is an Intrusion Detection System / Intrusion Protection System

☐ Intrusion Detection and Prevention System SRG

DBN-6300

☐ IDPS STIG
☐ NDM STIG

Palo Alto Networks

☐ Application Layer Gateway
☐ IDPS
☐ NDM

The system is Network Access Controller

☐ Remote Access Policy STIG (contains NAC requirements)

Fore Scout CounterACT

☐ ALG STIG
☐ NDM STIG

The system is an IPSEC VPN

☐ IPSEC VPN Gateway STIG

The system is an SSL/TLS VPN

☐ Remote Access VPN STIG

☐ RSA SecureID AM Secure Configuration Guide

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. Note: "remote access" is defined as traversing a non-DoD owned/managed network (i.e. across the unprotected Internet).

☐ Remote Access VPN STIG
☐ Remote Endpoint STIG
☐ Remote XenAPP ICA Thin Client

The system supports VVoIP technology.

☐ Voice and Video over Internet Protocol
☐ Remote Access Server STIG
☐ Voice Video Endpoint
☐ Voice Video Services Policy ☐ Voice Video Session Management

☐ The system supports Wireless technology.
☐ Network WLAN STIG
- ☐ Controller-based WLAN - Network WLAN Controller
- ☐ WLAN Bridge - Network WLAN Bridge
- ☐ Access Point for NIPRNet (not controller-based) - Network WLAN Access Point Enclave NIPRNet Connected Role
- ☐ Access Point for Internet only (not controller-based) - Network WLAN Access Point Internet Gateway-Only Connection Role

8. PROTOCOLS

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

☐ FTP	☐ TLS Version_____	☐ SIP-TLS
☐ TFTP	☐ IPSEC	☐ AS-SIP
☐ SFTP	☐ SSH Version_____	☐ SIP
	☐ SSL Version _____	

☐ BootP ☐ h.323 ☐ RTP
☐ RCP-l ☐ h.320 ☐ SRTP

☐ LDAP
☐ SMTP
☐ SNMP Version _____

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