



DEPARTMENT OF THE AIR FORCE  
AIR FORCE RESEARCH LABORATORY  
WRIGHT-PATTERSON AIR FORCE BASE OHIO 45433

AFRLGM2016-33-02

8 July 2016

MEMORANDUM FOR SEE DISTRIBUTION

FROM: AFRL/CA  
1864 Fourth Street  
Wright-Patterson AFB OH 45433-7130

SUBJECT: Air Force Research Laboratory (AFRL) Guidance Memorandum (GM) on  
Software Certification

RELEASABILITY: There are no releasability restrictions on this publication.

1. By Order of the Executive Director, Authorizing Official for the Air Force Research Laboratory, this AFRL Guidance Memorandum immediately implements new policies, processes and AFRL authorities for the certification of AFRL software products. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other AFRL instructions; the information herein prevails, in accordance with (IAW) AFI 33-360, *Publications and Forms Management*. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).
2. The use of uncertified software within AFRL environments can cause the introduction of malicious logic, back doors, viruses and other cybersecurity vulnerabilities. In order to maintain our security posture and mitigate risks associated with software use, AFRL is implementing a new Enterprise Software Certification Policy requiring software that hasn't already been assessed/evaluated by a trusted source (see attachment 6 for list of trusted sources) be certified for use prior to operation. This policy applies to software to include but not limited to Commercial off the Shelf (COTS), Government off the Shelf (GOTS) (locally developed), open source and freeware/shareware. Other software instances outside the aforementioned categories will be reviewed on a case-by-case basis to determine if a full certification is required.
3. This guidance memorandum becomes void after 180 days has elapsed from the date of this memorandum, or upon publication of the affected publication, whichever is earlier.

4. If you have any questions, please contact Ms. Roselyn Richardson, AFRL/RCC, DSN 785-2082 and roselyn.richardson.1@us.af.mil.

C. DOUGLAS EBERSOLE, SES  
Executive Director

Attachments:

1. Application Request Worksheet (ARW)
2. Certification Memo
3. Software Testing Checklist
4. Software Certification Process Narrative
5. Software Certification Process Flowchart
6. List of Trusted Sources

DISTRIBUTION:

AFRL/DO

DP

EN

FM

IG

JA

PK

RC

SB

SE

XP

711 HPW/HP/RH/USAFSAM

AFOSR

AFRL/RD/RI/RQ/RV/RW/RX/RY

<b>Application Request Worksheet (ARW)</b>		
<p><b>*** Please, click the “Enable All Features” button above ***</b></p> <p><b>This ARW must be completed by an AF sponsor, and then digitally signed by their unit IAO/IAM. All application requests must be submitted through your unit Information Assurance Office. E-mail subject line format: ‘Application/Product request: Full Application/Product Name, Complete Version’ Please limit the use of acronyms in the product name.</b></p>		
<b>Desktop Application</b>	<b>Full Application Name</b>	<b>Version: Requested Version</b>
<p><b>Once evaluated, the application/product may receive a Certification and be added to the Enterprise Evaluated Products List (EEPL)</b></p> <p><b>It is the sponsor’s responsibility to identify the exact version and to supply the application/product for testing.</b></p> <p><b>*** Please, click the “Enable All Features” button above ***</b></p>		

<b>Table Of Contents</b>
<b>PRE-CERTIFICATION CHECKLIST</b>
<b><u>SECTION 1 – AIR FORCE SPONSOR INFORMATION</u></b>
<ul style="list-style-type: none"> <li>• Contact, Organization, Email and Phone Information</li> </ul>
<b><u>SECTION 2 –APPLICATION/PRODUCT INFORMATION</u></b>
<ul style="list-style-type: none"> <li>• Name and Version</li> <li>• Application/Product Information</li> <li>• Vendor Information – Including System for Award Management information</li> <li>• Testing Background</li> </ul>
<b><u>SECTION 3 – APPLICATION/PRODUCT FUNCTIONALITY</u></b>
<ul style="list-style-type: none"> <li>• Application/Product Category</li> <li>• Functionality/Use/Capabilities</li> <li>• Fielding Information</li> <li>• Type of Data Processed</li> </ul>
<b><u>SECTION 4 – SPONSOR TESTING OF DESKTOP APPLICATIONS</u></b>
<ul style="list-style-type: none"> <li>• Testing Requirements</li> <li>• Desktop Testing Procedures</li> <li>• Testing Entity Information</li> </ul>
<b><u>SECTION 5 – APPLICATION REQUEST ENDORSEMENT SIGNATURE</u></b>

*\*Note: This worksheet must be fully completed then digitally signed to be processed; incomplete requests will not be processed and returned to the sponsor.*



Pre-Certification Checklist*		
	YES	NO
1. Is the Program Manager/Sponsor responsible for configuration management, vulnerability management, and Security Technical Implementation Guide (STIG) compliance management for the hardware (e.g., physical computers), firmware, or underlying system software (e.g., operating system, database management system, web server, application server, client/server)?	<input type="radio"/>	<input type="radio"/>
2. Is the application/product public domain software commonly known as freeware or shareware that is only available in binary format? (Ref. NIST SP 800-53r4 ( <a href="http://csrc.nist.gov/publications/PubsSPs.html">http://csrc.nist.gov/publications/PubsSPs.html</a> ))	<input type="radio"/>	<input type="radio"/>
3. Is this a pre-production application/product? (e.g. beta version)	<input type="radio"/>	<input type="radio"/>

SECTION 1 – AIR FORCE SPONSOR INFORMATION			
Sponsor POC* AF Official Required	Name		
Organization, Proponent Agency, or Direct Reporting Unit Address:	Organization		
Email (must provide af.mil address):	E-mail Address		
Phone (commercial):	123-123-1234	Phone (DSN):	123-4567

Unit IAO*:	Name		
Organization, Proponent Agency, or Direct Reporting Unit Address:	Organization		
Email (must provide af.mil address):	E-mail Address		
Phone (commercial):	123-123-1234	Phone (DSN):	123-4567

\* **Note:** There must be at least two different POC's for each submission.



SECTION 2 –APPLICATION/PRODUCT INFORMATION			
2.1 Full Name/Acronym	Full Application Name		
2.2 Version	Requested Version		
2.3 Is this a request for an older version of the application/product? Provide justification for older versions as an attachment.			No
2.4 What is the type of the application/product? For Web Applications, PMs/sponsors must provide additional information and documentation.			Desktop Application
2.5 On what Operating System will it be installed?		Windows	
2.6 Is this an open source, commercial off the shelf (COTS), or government off the shelf (GOTS) application/product?	Open Source: <input type="radio"/>	COTS: <input type="radio"/>	GOTS: <input type="radio"/>
2.7 Vendor Name, Open Source Organization, or GOTS Agency responsible for developing the application/product	Enter Vendor's Name		
2.7.1 Vendor (address, and phone) - Note: vendor information (to include information listed in question 2.10) must match the www.sam.gov website record; <b>Note: Not applicable for open source applications</b>	Enter Vendor's Mailing Address		
2.7.2 Application/product Information Website - <b>Note: Must be link to application/product information page, not the vendor's home page.</b> This helps us identify the application/product.	Required to be Application Information Page		
2.8 Is the application developed by a foreign (non-US) company? Unknown: <input type="radio"/>		Yes: <input type="radio"/>	No: <input type="radio"/>
2.9 Is the vendor listed as an exclusion on System for Award Management (SAM) formally known as the "Excluded Parties List"? (Go to <a href="https://www.sam.gov/">https://www.sam.gov/</a> ) <b>Note: Not applicable for open source applications.</b>		Yes: <input type="radio"/>	No: <input type="radio"/> N/A: <input type="radio"/>
2.10 For COTS: Vendor/Manufacturer SAM validation information <i>must</i> be provided. <b>Note: Not applicable for GOTS or open source applications.</b> Per FAR 4.11 prospective contractors must be registered prior to award/purchase. For further information visit <a href="https://www.sam.gov/">https://www.sam.gov/</a>		DUNS No: Enter #	
		CAGE Code: Enter #	
2.11 Does the end user license agreement (EULA) specify limitations such as: <ul style="list-style-type: none"> <li>• Restriction for government use?</li> <li>• User's permission to monitor and/or accept automatic updates?</li> <li>• User's permission for the application/product to harvest system or personal information?</li> </ul> <b>Note: If Yes, provide the exact verbiage in an attachment.</b>		Yes: <input type="radio"/>	No: <input type="radio"/>



### SECTION 3 – APPLICATION/PRODUCT FUNCTIONALITY

<b>3.1 Application/Product Category</b> (help others by selecting the most appropriate category – marking “Other” should be the last option)	Audio/Visual <input type="radio"/> Database <input type="radio"/> Internet <input type="radio"/> Logistics <input type="radio"/> Multimedia <input type="radio"/>	<input type="radio"/> Business Finance <input type="radio"/> Desktop Enhancements <input type="radio"/> IT Utilities/Security <input type="radio"/> Medical <input type="radio"/> Program Development	<input type="radio"/> Communications <input type="radio"/> Education <input type="radio"/> Geospatial <input type="radio"/> Model/Simulation <input type="radio"/> Other		
<b>3.2 Provide a description of the functionality/capability of this application/product (required)</b> - Enter a description of what this application does					
<b>3.3 Is this a client-server application/product? Note: If yes, then two ARW's must be submitted, one for the client and one for the server. One ARW cannot be used for both.</b>			Yes: <input type="radio"/>	No: <input type="radio"/>	
<b>3.4 Does the application/product use any peripheral hardware products? If yes please specify.</b> Yes: <input type="radio"/> No: <input type="radio"/>			If yes specify		
<b>3.5 Does the application/product require any software not provided by the SDC/DSCC? If yes please specify.</b> Yes: <input type="radio"/> No: <input type="radio"/>			Additional Software		
<b>3.6 Does this application use cloud services?</b>			Ukn: <input type="radio"/>	Yes: <input type="radio"/>	No: <input type="radio"/>
<b>3.7 On what network will this application/product be used? (Standalone, NIPR, DREN etc.)</b>			Enter Network		
<b>3.8 Type of data this application/product will process (Unclassified, Classified, NATO, Coalition, FOUO, HIPAA, PII etc.)</b> (Ref DoDD 5400.11, para E2.2) ( <a href="http://www.dtic.mil/whs/directives/index.html">http://www.dtic.mil/whs/directives/index.html</a> )			Enter what type of data this application will process/store		



SECTION 4 – SPONSOR TESTING OF DESKTOP APPLICATIONS			
4.1 Will this be sponsor tested? (Please send test results)		Yes: <input type="radio"/>	No: <input type="radio"/>
4.2 Testing POC		Enter person we can contact	
4.3 Testing Organization/Unit/Office Symbol:		Enter Unit	
4.4 Email:		Enter testers e-mail address	
4.5 Phone (commercial):	123-123-1234	Phone (DSN):	123-1234

SECTION 5 – APPLICATION REQUEST ENDORSEMENT SIGNATURE	
Information Assurance Officer/Manager	
	Enter Name and Office Symbol
	Name and Office Symbol

**SECTION 8 – REVISION HISTORY – Remove from PDF**

<b>Version</b>	<b>Reviewer Name</b>	<b>Date</b>	<b>Comments</b>
1.0	AFNIC	July 1, 2015	- Original format derived from AFNIC
1.1	Suman Goel	July 22, 2015	- Made changes per group consensus
1.2	Hand over to RCC	February 11, 2016	- Made changes for Enterprise use
1.3	AFRL/RCC Cybersecurity Office	June 3, 2016	- Made modifications based on feedback from management
			-
			-



FOR OFFICIAL USE ONLY  
**DEPARTMENT OF THE AIR FORCE**  
**HEADQUARTERS AIR FORCE RESEARCH LABORATORY**  
 Research and Collaboration Computing Directorate  
 Wright Patterson AFB, OH 45433

MEMORANDUM FOR Enterprise AFRL

FROM: Air Force Research Laboratory  
 <UNIT Address>

SUBJECT: Software Certification for Product Name Version (major version for example version 18).x

1. Product Name version (major version).x is hereby certified in accordance with AFI 33-210 for use on Enterprise [RDT&E workstation or Enterprise RDT&E server] systems connected to Enterprise RDT&E Network and placed on the Enterprise Evaluated Products List (Enterprise EPL). *This certification expires three years from the date of the digital signature below* and does not apply to subsequent major application revisions. For example, version 19.x would not be grandfathered under this certification.

2. Product Name version (major version).x description of the product. Please do not give the company sales pitch. What does the software do? Please give others a good description to help them decide if this software may help their mission. All text shall be the same **color**, the same font and size before submitting the Certification Memo ...'black, Arial 12!' RCC presents this information in different colors to assist in filling out this Certification Memo and for informational purposes only. DO NOT CHANGE THE CANNED WORDING IN THIS TEMPLATE<Include the following only if there are additional applications/product that will be included in this certification.> This certification includes the following additional software components:

Software	Version	Software	Version
List included applications/products here (For example, if certification was for For the Record you would list: FTR Player; FTR Manager; Chronotron etc.)		List included programs here– <b>note</b> only list applications/products that a user could use/purchase separately – this is not a list of the 'installed' applications/products from question 6.3	

3. **Include the following parts between the "<>" only if used otherwise delete them. Of course remove the blue text.** My decision is based on the validation of test data reviewed by RCC, <tested by [list sponsor]> and documented in this certification.

If question 1.2 is marked 'Yes' add: *<Because Product Name version (major version).x stores/produces/processes sensitive data, users and/or the local Information Assurance Officer shall ensure all Product Name version (major version).x <Select according to ARW item 3.9 [controlled unclassified] [controlled unclassified and classified] [classified]> information is protected IAW CJCSI 6510.01.> <If question 2.3 is marked yes., Place any restrictions here: e.g. Product Name version (major version).x is restricted to administration use only..>< If questions 4.5, 5.1, 5.2 and Table 5.6.1 indicate the application uses the network add: <Any and all ports, protocols, and services (PPS) identified below shall only be used according to DoDI 8551.1, and per the vulnerability assessment report for each PPS.> If question 6.2 is answered 'Yes' and providing the application does implement according to the guidance add: <Product Name version (major version).x application uses mobile code technology, which shall be implemented and configured in accordance with the Application Security and Development STIG and DISA's guidance at <https://powhatan.iie.disa.mil/mcp/mcpdocs.html>.> **List all high and medium risk vulnerabilities and their mitigation(s) in the table below. Note: A vulnerability table is required for each vulnerability. (if possible, group like vulnerabilities together) List High vulnerabilities first followed by mediums.** <If the application has 'No' vulnerabilities use: < AFRL/RCC confirmed there are no high or medium risk vulnerabilities and the product presents a low risk to the system or enclave. If the application has vulnerabilities use:> [list sponsor] discovered high/medium/low risk Microsoft ity(y/ies) with this application that shall be mitigated prior to use. Once the administrator implements the mitigation actions described in the table below, the vulnerabilities will be mitigated and the application will present a low risk to the system or enclave.*

4. Software versions earlier than *<this information comes from the Mkruntest reginstalls test results Product Name Version X (use exact version found in mkruntest reginstalls test results e.g. WinZip Version 18.5)>* were not assessed and may contain vulnerabilities; therefore administrators should install this version or later. In addition, all applicable security patches for this product shall be implemented in accordance with the associated using system or enclave Approval to Operate (ATO).

5. This memorandum does not serve as an authorization, but solely as a certification that this software has been evaluated. Before this software can be used on a system or enclave, the terms of the End User License Agreement (EULA) shall be understood and the system or enclave ATO shall be updated to include this software version. For questions or to obtain supporting documentation, my Information Assurance representative POC is AFRL/RCC, (937) 255-5199 (DSN 785-5199) or e-mail: [eileen.dennehy.ctr@us.af.mil](mailto:eileen.dennehy.ctr@us.af.mil)

Roselyn Richardson, DR-III (GS-14)  
AF S&T Security Control Assessor (SCA)  
Research Collaboration and Computing  
Directorate

## SOFTWARE TESTING CHECKLIST

### Vulnerabilities for [Abstract]:

<b>Vulnerability One:</b>	List one vulnerability per table. Same type of vulnerabilities may be grouped. List high and medium vulnerabilities first and those must be listed in paragraph 3 (or 4 if there are multiple vulnerabilities) as vulnerability and mitigation. Low vulnerabilities should be listed last and lows are not listed in paragraph 3. See wording in paragraph 3 above. – if there are no vulnerabilities enter 'None' in this cell
<b>CVE Affected:</b>	List any CVE to which this vulnerability applies. List all CVE's if grouping.
<b>Note:</b>	Note anything of importance about this vulnerability. Giving extra information here is a good thing.
<b>Severity Category:</b>	From the NVD – unauthorized installed FireWall rule exceptions are considered a medium risk.
<b>Mitigating Factors:</b>	List how this vulnerability is to be mitigated. Give details! All high and medium risk vulnerabilities require mitigation before it will be certified. High and Medium vulnerabilities will say the administrator 'shall'...for low use the comment of it is recommended the administrator...

### [Abstract] Testing Checklist:

(Note: Exact version means the 'exact' version installed from the reinstalls test results. Do not list from the menu Help => About This is different from the 'major' version requested in the memo part. The software version information is found in the Mkruntest reinstalls test report. Please fill out comments only as needed. Delete the informational comments (in RED and GREEN) below, DO NOT state the obvious or repeat the question. Keep comments brief and to the point...all text color should be black, Arial 12pt... Use 'X' in the columns below...DELETE THIS NOTE BEFORE SUBMITTING)

1. Desktop Review	Yes	No	N/A	Comments
1.1 Will the requested application be deployed on an Enterprise infrastructure?				OS Type – Windows/Linux/Redhat/Ubuntu
1.2 Does the application process, produce, or store sensitive data (e.g., Classified, Privacy Act, HIPAA, etc.)?				If answer is Yes, add the appropriate wording in paragraph 3 and: Since this application stores/produces/processes sensitive data, users and/or the local Information Assurance Officer shall ensure all controlled unclassified information is protected IAW CJCSI 6510.01.
1.3 Is the application developed/controlled by a foreign country?				<b>REQUIRED FOR ALL:</b> Enter: Company name, Mailing Address City, State Zipcode (Must match what is on the ARW and DUNS/CAGE)
1.4 Is the application vendor listed as an exclusion on System for Award Management (SAM)?				Check <a href="https://www.sam.gov/">https://www.sam.gov/</a> if the vendor is excluded! The product will not be certified!
1.5 Are there any known vulnerabilities for the application?				Example sources: Vendor support info; <a href="http://nvd.nist.gov/">http://nvd.nist.gov/</a> ; <a href="http://www.securityfocus.com/">http://www.securityfocus.com/</a> <a href="http://www.cvedetails.com/">http://www.cvedetails.com/</a> <a href="http://cve.mitre.org/cve/cve.html">http://cve.mitre.org/cve/cve.html</a> If yes, fill-in vulnerability table for each vulnerability and include the CVE (or ID#). You may group similar CVE's into a single table, but you must still list the CVE's in the Note's section. Include mitigations. Highs and Mediums require mitigation! Include highs and mediums in paragraph 3 and add tables. Note: This is for the application being certified only. Additional installed software vulnerabilities are listed in question 6.4.

1. Desktop Review	Yes	No	N/A	Comments
1.6 Is the request for an older version of the product?				<p>Check vendor's website. If this is for an older version then enter a justification also look for supportability of the older version. If the product is no longer supported then the application cannot be certified. For Microsoft products use this link:  <a href="http://support.microsoft.com/lifecycle/search/">http://support.microsoft.com/lifecycle/search/</a></p>
<p>1.7 Are there hardware/software requirements not provided by the current ITCC Buying Standards and the SDC (e.g., License Dongle, sound/video card, RAM; OS, perl, SQL server, etc.) that are required for the application to run?            (Current buying standards: <a href="https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=s6925EC134D400FB5E044080020E329A9">https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=s6925EC134D400FB5E044080020E329A9</a>)</p>				<p>During the desktop review and software installation process and make note of any additional applications or plug-ins needed in addition to the application/program installation. Any additional software installs will also need to be checked for known vulnerabilities and addressed in Vulnerability table of this checklist.</p>
1.8 Are administrator rights required to install the application?				<p>Does it require an administrator to install the software?</p>
1.9 Does the application require configuration steps or extra permissions for standard users to execute the application (e.g., manually creating directories or files, setting up another application to run, etc.)?				<p>Additional testing may be required to determine this. Explain extra permission or configuration steps if needed for a standard user.</p> <p>Note: checklist question 4.7</p>

1. Desktop Review	Yes	No	N/A	Comments
1.10 Is this an IA or IA-enabled product?				<p><a href="#">IA/IA-enabled products will not be included on the Enterprise-EPL.</a> DoD requires IA products to be evaluated and validated by NSA in accordance with an NSA-approved process through one of the following sources: International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Question 2 of the ARW – should have been answered ‘Yes’ meaning the certification process might not be the correct process.</p>
1.11 Are there specific bandwidth requirements?				<p>Does the software require a specific bandwidth to operate? Check users or maintenance documentation</p>

2. Testing Documentation Review	Yes	No	N/A	Comments
2.1 If testing a trial or unregistered version, does it have the same functionality as the full version?				<p>If ‘No’, only comment on the differences the trial version may have over the full version. An ‘X’ in the ‘N/A’ column means you tested the full version – no need to comment.</p>
2.2 Does the documentation provide clear guidance for installing and configuring the application?				<p>If there is no installation documentation, provide comments such as ‘GUI installation was self-explanatory’ or the GUI stunk and didn’t help at all.</p>

<b>2. Testing Documentation Review</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
2.3 Are dedicated personnel required to operate and/or maintain (vs. simply using the product in process/analyze/transfer data, etc.)?				An 'X' in the 'Yes' column means that people such as system administrators, or database administrators or certified application users or specifically certified users (medical technicians) are routinely required for running or maintaining the application.

<b>3. Testing Application Installation</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
3.1 Was malicious code detected in the installation files?				Perform a virus scan of the installation files prior to installation. If the answer is 'No' then no comment is needed.
3.2 Does the application add itself to system's application menu?				If the application's run icon is off the Start => All Programs menu for the administrator and standard user mark a 'X' in the 'Yes' column and you do not need to comment. If not then how does a standard user get to use the program?
3.3 Does the application provide an 'Uninstall'?				If the 'Uninstall' is off the Start => All Programs menu mark a 'X' in the 'Yes' column and you do not need to comment. Do not say it can be uninstalled from the 'Control Panel.' We know this already
3.4 Were installation issues found?				If answer is 'Yes', document found issues such as: If you have to install "Widget B" before you install "Widget A," or do you have to download a certain version of JRE before continuing the install, or the program will not "let" you install it in the default Program Files directory. Anything that the installation guideline didn't specifically address.

4. Testing Application Operation	Yes	No	N/A	Comments
4.1 Are there required input files (e.g., .dot, .ini, .config, manifest, etc.)?				Does the application require a configuration file or files to start?
4.2 Does the application produce any files?				List extensions. This question refers to files the application uses, saves, imports or exports (e.g. *.docx, *.xlsx, *.dwg.)
4.3 Are there credentials associated with the application?				If answer is 'Yes', comment what credentials (PKI, username and passwords) are used to login to the application. This is about the application and not the credentials to get into the computer.
4.3.1 Are these credentials configurable?				If credentials (if any) are configurable explain <u>how</u> are they configurable? Are they user configurable? Are they configured by the system administrator?
4.3.2 How are these credentials protected?				Comment on "how" the credentials (if any) are protected.
4.4 Does the application provide encryption of data (data at rest)?				Document type of encryption the application uses for storing its files and if it is FIPS certified. FIPS certification requires proof of the certification. NOTE: this question is about data-at-rest and not about data in transit which is addressed in question 5.3.
4.5 Does the application provide automatic updates/user configurable updates?				If the answer is 'Yes' it must be shown in the packet capture. Add PPS blue notes in paragraph 3. Note: Questions 5.1 & 5.2 are also network related questions.
4.6 Does the application include a Software Improvement Program which automatically sends various types of information back to the Vendor?				Investigate how to opt out of participating in the program and document in the appropriate vulnerability table. This is considered a medium vulnerability

<b>4. Testing Application Operation</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
4.7 Is the application compatible with a standard user account?				It is required to login as a standard user to determine if the application can be successfully operated. Comment on any configuration changes that may be required for proper operation.

<b>5. Testing/Analyzing Network</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
5.1 Was application related network traffic detected during installation?				If 'Yes', complete Table 5.6.1 (use your packet capture program to answer) Add PPS blue notes in paragraph 3.
5.2 Was application related network traffic detected during operation?				If 'Yes', complete Table 5.6.1 (use your packet capture program to answer) Add PPS blue notes in paragraph 3.
5.3 Was data transmitted being protected?				The packet capture will show the data transmitted as being protected or not (e.g. TLS, SSL or HTTPS). (use your packet capture and/or packet analysis program to answer)
5.4 Were exceptions added into the firewall policy?				Can be determined through netsh (pre/post captures) & registry entries (netsh/Registry Analysis – mkruntest).
5.5 If firewall exceptions were added, will reconfiguring them impact the application?				Open ports to 'any' IP address on 'any' port TCP/UDP is cause for concern. Open firewall rules shall be locked down to specific IP addresses and ports or removed and any negative impacts to the application functionality will be noted here.

5. Testing/Analyzing Network	Yes	No	N/A	Comments
5.6 If crossing DoD network boundaries (e.g., enclave boundary), are the ports, protocols, and services (PPS) acceptable according to the DoD PPS CAL?				<p>If the traffic crosses the enclave check the PPS CAL and any VA restrictions:</p> <p><a href="http://iase.disa.mil/">http://iase.disa.mil/</a> if the port is not allowed or if the application is not using the port for the CAL's stated purpose the application is required to go through DIACAP.</p> <p>If a port is not on the CAL and not configurable, the application must go through DIACAP.</p> <p>If a port is not on the CAL but is configurable, add a medium vulnerability with mitigation to use a CAL compliant port.</p> <p>Add PPS blue notes in paragraph 3.</p>

**Table 5.6.1 Connection Table**

Description and Purpose	Port/ Protocol/ Data Service	Origin Domain Name	Destination Domain Name	Bandwidth	Local Service Only?
What function does this conversation provide? Help, licensing, updates? Be as specific as possible. Place each conversation in its own row.	Only list Port/ Protocol/Data Service Note: format 80/tcp/http 443/tcp/https	SDC Client  Don't give the IP address of your test computer	Where? www.???.com? Don't give IP address	[Low, Medium, High] What is the sustained bandwidth? (Low < 1MB; 1 MB > Medium < 10 MB; High > 10MB)	Yes/No

6. Testing Analyzing Configurations	Yes	No	N/A	Comments
6.1 Were system .dll's overwritten with older versions?				<p>If yes, give details and research, because this situation is considered high risk. (FS Check – mkrntest) Older dll's may have known vulnerabilities</p>

6. Testing Analyzing Configurations	Yes	No	N/A	Comments
6.2 Does the application employ use of mobile code technology?				<p>If 'Yes' then include the appropriate blue wording in paragraph 3 and then use the following: Use of mobile code shall comply with the requirements of the Application Security and Development STIG and DISA's implementation guidance at <a href="https://powhatan.iiee.disa.mil/mcp/mcpdocs.html">https://powhatan.iiee.disa.mil/mcp/mcpdocs.html</a> before installation.</p> <p>NOTE: If there are added OCX's, Java/javaw/javaws executables in in Fsccheck this will be a 'Yes'</p>
6.3 Did the application place application files within acceptable locations?				<p>Acceptable location is Program Files Folder. Installing off the root of c:\ is not acceptable. (FS Check – mkruntest) This is a High vulnerability</p>
6.4 Did the application install any additional software (e.g., browser plug-ins, toolbars, SQL servers, etc.)?				<p>List additional software and version numbers installed. To obtain this information, look in three different places.</p> <ol style="list-style-type: none"> <li>1. The reinstalls of mkruntest results</li> <li>2. The install screens.</li> <li>3. The manufacturer's installation guide.</li> </ol> <p>Additional applications/products require a vulnerability check.</p>
6.5 Does the additional software have any known vulnerabilities?				<p>If 'Yes', fill-in Vulnerability table. All additional installed software shall be checked with NVD and/or Security Focus and highs and mediums shall be mitigated...also include appropriate wording in paragraph 3 and vulnerability tables</p>

6. Testing Analyzing Configurations	Yes	No	N/A	Comments
6.6 What process name does the application execute under?				Found in the difference between tasklist before and tasklist after. Note the application 'shall' be running for tasklist to capture the process name in the post-installation capture. (tasklist – mkruntest) Unclear on which process? Remember Google is your friend.
6.7 Did the application remove, modify, or install a service?				List any/all services removed modified or installed. (sc – services – mkruntest) Format: (don't list 'none'; only list the categories where there is data) Installed: - Modified: - Removed: -
6.7.1 If a service is installed, does setup include automatic start?				(sc – services – mkruntest) Note: This is for installed services only. List which service is set for automatic start. Automatic start uses admin rights and is a concern
6.7.2 Describe any network operations with which the service is associated.				If the service listens on a network port, a deeper analysis may be required to determine how it operates.(sc – services – mkruntest) This is for installed services only with network traffic. If the service is listed here then we should see a conversation in Table 5.6.1. List the service 'then' what the service does.

6. Testing Analyzing Configurations	Yes	No	N/A	Comments
6.7.3 Describe the function of any service installed.				<p>Installation of persistent services can be considered a risk. (sc – services – mkruntime) This is for <i>installed</i> services only.</p> <p>If the service is listed in 6.7.2 there is no need to include the function here.</p> <p>List the service 'then' what the service does.</p>
6.8 Were there any other items of note (e.g., violations of security policy)?				<p>Any issue that was not covered elsewhere in this memo (e.g. violations of security policy, forbidden file extensions in registry file report, etc) Yes this is the catch all question if nothing else applies.</p>

## Attachment 4

### SOFTWARE CERTIFICATION PROCESS NARRATIVE

Block 1: Start the process

Block 2: User completes the ARW located at

Block 3: User emails the completed ARW to [AFRL.SWEval@us.af.mil](mailto:AFRL.SWEval@us.af.mil)

Block 4 (Decision): AFRL/RCC Cybersecurity Office reviews the ARW to verify the ARW is complete – if yes, go to Block 5, if not, go to Block 6

Block 5: AFRL/RCC Cybersecurity Office enters the ARW onto the SharePoint site located at [https://cs1.eis.af.mil/sites/rdte/Lists/DREN\\_EPL/EPL.aspx](https://cs1.eis.af.mil/sites/rdte/Lists/DREN_EPL/EPL.aspx) and assigns AFRL/RCC Cybersecurity POC and proceed to block 7

Block 6: AFRL/RCC Cybersecurity Office returns the ARW with feedback to the submitter return to Block 2 in flowchart

Block 7: AFRL/RCC Cybersecurity POC assigns and notifies a TD to test

Block 8: TD completes testing

Block 9: TD uploads test results to ARMEDEC located at <https://safe.armedec.army.mil/safe>

Block 10: AFRL/RCC Cybersecurity POC downloads test results package to include certification memo and other associated documentation

Block 11: AFRL/RCC Cybersecurity POC reviews test results package to include certification memo and other associated documentation

Block 12 (Decision): AFRL/RCC Cybersecurity POC reviews results to verify appropriate test result package was provided, if yes, go to Block 13, if no, go to Block 7

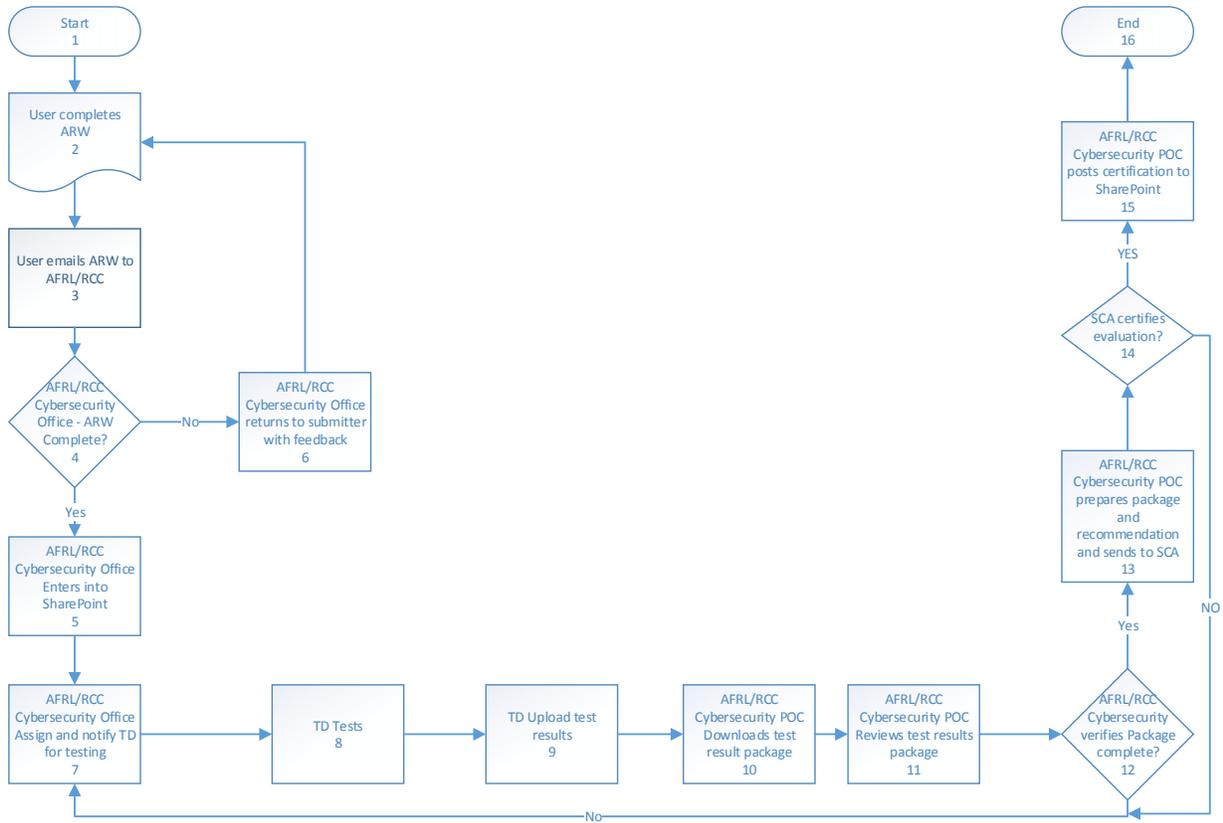
Block 13: AFRL/RCC Cybersecurity POC prepares package and provides recommendation to SCA

Block 14 (Decision): AF S&T SCA certifies, if yes, go to Block 15, if no, go to Block 7

Block 15: AFRL/RCC Cybersecurity POC post signed memorandum on SharePoint

Block 16: End Process

### SOFTWARE CERTIFICATION PROCESS FLOWCHART



**TRUSTED SOURCES LISTING  
FOR RECIPROCITY**

**1. AF Evaluated/Approved Products Listing**

**Description:** The AF E/APL is the definitive source for standard desktop, web, and mobile applications formally approved to operate on the AF DODiN NIPR and SIPR environments. THE AFNIC/NTS office at Scott AFB manages the process and the SCA for the EPL is at HQ AFSPC/A2/3/6 at Peterson AFB

**LINK:** <https://cs3.eis.af.mil/sites/afao/Lists/COTSGOTS%20Software/EPL.aspx>

**2. NSA NIAP/Common Criteria Evaluated Products Lists**

**Description:** NSA manages the National Information Assurance Partnership (NIAP), a US government program originated to meet the security testing needs of both consumers and producers of information technology. Through the NIAP's Common Criteria Evaluation and Validation Scheme (CCEVS), approved Common Criteria Testing Laboratories (CCTLs) evaluate Commercial Off-The-Shelf (COTS) Products. The CCEVS Validation Body: provides technical guidance to CCTLs, validates the results of IT security evaluations for conformance to the International Common Criteria for IT Security Evaluation, and serves as an interface to other nations for the recognition of such evaluations.

**LINK:** [https://www.niap-ccevs.org/CCEVS\\_Products/pcl.cfm](https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm)

**LINK to Common Criteria products list:** <http://www.commoncriteriaportal.org/products/>

**3. DoD Unified Capabilities Approval Products List**

**Description:** The DoD Unified Capabilities (UC) APL is established in accordance with the UC Requirements (UCR 2013) document and mandated by the DoD Instruction (DoDI) 8100.04. Its purpose is to maintain a single consolidated list of products that have completed Interoperability (IO) and Information Assurance (IA) certification. Use of the DoD UC APL allows DoD components to purchase and operate UC systems over all DoD network infrastructures. The APLITS site incorporates JITC testing.

**LINK:** <https://aplits.disa.mil/processAPList.action>

**4. AF Intelligence Community Approved Products List (APL)**

**Description:** The 25 AF/A6S Agency Software Evaluation site is the software evaluation site for the 25<sup>th</sup> AF/A6S, which is the Authorizing Official (AO) for all AF Sensitive Compartmented Information systems and Collateral (Top Secret and below) Intelligence Surveillance and Reconnaissance (ISR) mission systems. Evaluated products that the AO has permitted to be used by the ISR community are placed on the AF Intelligence Community (IC) APL.

**LINK:** <https://intelshare.intelink.gov/sites/afisra-a6s/a6sc/Lists/APL>

**5. Army Networkiness SharePoint Portal**

**Description:** The Army Networkiness (NW) program was created out of an Army need to address compliance and mitigate risks. Its purpose is to ensure that all applications, systems, devices, Web services, and hardware purchases support Federal, Department of Defense (DoD), and Army guidelines, regulations, and requirements. In effect, the program is to determine whether an application or system is worthy to go on the Army's Enterprise network (LandWarNet). The NW program assesses interoperability and supports the Army's goal for a standard baseline, utilizing Enterprise License Agreements to maximize the reach of our IT dollars. NW was developed in a proactive way to preclude drive-by fielding of systems, serve as a safety-net prior to anything connecting to the LWN, prevent

products from causing damage or interoperability issues, and to mitigate the risks posed to the LWN from numerous threat vectors.

**LINK:** <https://army.deps.mil/NETCOM/sites/nw/CoNApproval/Lists/Networthiness%20Data/>