DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR COMBAT COMMAND
JOINT BASE LANGLEY-EUSTIS VA

MEMORANDUM FOR HQ CCC/CZZE

FROM: HQ ACC A6/A6I
300 Exploration Way
Hampton, VA 23666

SUBJECT: Software Certification for Air Conformity Applicability Model (ACAM) Version 5.x

1. ACAM version 5.x is hereby certified in accordance with (IAW) AFI 17-101 for use on standard desktop systems connected to the AF Network (AFNET) and AF SIPRNet and placed on the AF Evaluated Products List (AF 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 6.x would not be grandfathered under this certification.

2. ACAM version 5.x is an existing GOTS standalone product/application that is the AF's standardized method for performing modeling of air emission for General Conformity Applicability Analysis to meet legally mandated regulatory air requirements.

3. My decision is based on the validation of test data reviewed by HQ CCC/CZZE tested by AFCEC/CZTQ and documented in this certification. *Because ACAM version 5.x stores/produces/processes sensitive data*, users and/or the local Cybersecurity Liaison shall ensure all ACAM version 5.x controlled unclassified information is protected IAW CJCSI 6510.01. HQ CCC confirmed there are no high or medium risk vulnerabilities, and the product presents a low risk to the system or enclave.

4. Software versions earlier than ACAM 5.0.18a version 5.0.18 were not assessed and may contain vulnerabilities; therefore, administrators should install this version or later. In addition, all applicable Time Compliance Network Orders for this product shall be implemented according to AFI 17-201, *Command and Control (C2) for Cyberspace Operations* and AF Methods and Procedures Technical Order (MPTO) Air Force Information Network (AFIN) Vulnerability Management, TO 00-33A-1109.

5. This certification is not an Approval to Operate (ATO). 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. IAW AFI 17-101, once this software is included in the system/enclave's ATO this software is considered certified and approved for use under the active ATO and does not necessarily need to be removed even after this certification expired. For questions or to obtain supporting documentation, the Information Assurance SCA representative POC is HQ CCC/CZZE, (618) 229-6862 (DSN 779-6862) or e-mail: ccc.saca@us.af.mil.

HAM.JASON.B.1083649220

Digitally signed by HAM.JASON.B.1083649220
Date: 2022.11.04 12:19:08 -05'00'

PAMELA K. PIAZZA, GS-15, DAF
Air Force Security Control Assessor

Vulnerabilities for ACAM 5.0.18a version 5.0.18:

Vulnerability One:	None
CVE Affected:	
Note:	
Severity Category:	
Mitigating Factors:	

ACAM 5.0.18a version 5.0.18 Testing Checklist:

1. Desktop Review	**Yes**	**No**	**N/A**	**Comments**
1.1 Will the requested application be deployed on a SDC machine?	X			
1.2 Does the application process, produce, or store classified data?		X		Since this application stores/produces/processes sensitive data, users and/or the local Cybersecurity Liaison shall ensure all controlled unclassified information is protected IAW CJCSI 6510.01.
1.3 Is the application developed/controlled by a foreign country?		X		AFCEC 2261 Hughes Ave. Ste 155 Lackland AFB, TX 78236-9853
1.4 Is the application vendor listed as an exclusion on System for Award Management (SAM)?		X		
1.5 If this is a GOTS product, do we have a signed Configuration Management Plan (CMP) on file?	X			
1.6 Are there any known vulnerabilities for the application?		X		
1.7 Is the request for an older version of the product?		X		
1.8 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: https://go.usa.gov/xQ3Cc)		X		

1. Desktop Review	Yes	No	N/A	Comments
1.9 Are administrator rights required to install the application?	X			
1.10 Does the application require extra configuration steps or permissions to execute (e.g., manually creating directories or files, setting up another application to run, etc.)?		X		
1.11 Is this an IA or IA-enabled product?		X		

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?			X	
2.2 Is documentation required to install and configure the application?		X		GUI installation was self-explanatory.
2.3 Are dedicated personnel required to operate and/or maintain (vs. simply using the product in process/analyze/transfer data, etc.)?		X		

3. Testing Application Installation	Yes	No	N/A	Comments
3.1 Was malicious code detected in the installation files?		X		
3.2 Does the application add itself to the system's application menu?	X			
3.3 Does the application add an 'Uninstall' option to the system's application menu?		X		
3.4 Were installation issues found?		X		

4. Testing Application Operation	Yes	No	N/A	Comments
4.1 Are there configuration files required to execute the application (e.g., .dot, .ini, .config, manifest, .lic, etc.)?		X		
4.2 Are there credentials associated with the application?		X		
4.2.1 Are these credentials configurable?			X	

4. Testing Application Operation	Yes	No	N/A	Comments
4.2.2 How are these credentials protected?			X	
4.3 Does the application provide encryption of data (data at rest)?		X		
4.4 Does the application include a Software Improvement Program which automatically sends various types of information back to the Vendor?		X		
4.5 Does the application use cloud services?		X		
4.6 Does the application provide automatic updates/user configurable updates?		X		
4.7 Is the application compatible with a standard user account?	X			

5. Testing/Analyzing Network	Yes	No	N/A	Comments
5.1 Was application related network traffic detected during installation?		X		
5.2 Was application related network traffic detected during operation?		X		
5.3 Were exceptions added into the firewall policy?		X		
5.4 If firewall exceptions were added, will reconfiguring them impact the application?			X	
5.5 Are all of the ports, protocols, and services (PPS) identified below being used according to DoDI 8551.01 and per the vulnerability assessment report for each PPS? This applies regardless of whether or not the PPS in use crosses any type of network boundary.			X	

Table 5.5.1 Connection Table

Description and Purpose	Port/ Protocol/ Data Service	Source Device(s) or Server Name	Destination Device(s) or Server Name (Listens for Connection)	Local Service Only?

6. Testing/Analyzing Configurations	Yes	No	N/A	Comments
6.1 Were system .dll's overwritten with older versions?		X		
6.2 Does the application employ use of mobile code technology?		X		
6.3 Does the software application incorporate Open Source Software, either as a direct OSS product or through the use of other OSS products?		X		
6.4 Did the application place application files within acceptable locations?	X			
6.5 Did the application install any additional software (e.g., browser plug-ins, toolbars, SQL servers, etc.)?		X		
6.6 Does the additional software have any known vulnerabilities?			X	
6.7 What process name does the application execute under?	X			ACAMWPF_SEI_5018a.exe
6.8 Did the application install, modify, or remove a service?	X			Modified: - gpsvc - NgcSvc - TrustedInstaller - WaaSMedicSvc - WdiSystemHost
6.8.1 If a service is installed, does setup include automatic start?		X		
6.8.2 Describe any network operations with which the service is associated.			X	
6.8.3 Describe the function of any service installed.			X	
6.9 Were there any other items of note (e.g., violations of security policy)?		X		