



FOR OFFICIAL USE ONLY

**DEPARTMENT OF THE AIR FORCE**  
HEADQUARTERS AIR FORCE NETWORK INTEGRATION CENTER (AFNIC)  
SCOTT AIR FORCE BASE ILLINOIS 62225-5222

MEMORANDUM FOR AFNIC/EVSN

FROM: AFNIC/EV  
203 West Losey Street, Room 2100  
Scott AFB IL 62225-5222

SUBJECT: Software Certification for CerTest Version 5.x (Certification Termination Date [CTD]: 2 Nov 14)

1. CerTest Version 5.x is hereby certified in accordance with (IAW) AFI 33-210 for use on standard desktop systems connected to the AF-GIG and placed on the Air Force Evaluated/Approved Products List (AF E/APL). This certification and associated CTD does not apply to subsequent major application revisions. For example, version 6.x would not be grandfathered under this certification.
2. CerTest Version 5.x is a computer-based testing and management application. It utilizes data banks of test questions and generates specific tests and results which in-turn can be reported or exported to certifying and validating authorities.
3. My decision is based on the validation of test data reviewed and tested by AFNIC/EVSN, and documented in this certification. CerTest Version 5.x uses mobile code technology, which shall be implemented in compliance with DoDI 8552.01 and configured according to DISA's guidance at <https://powhatan.iie.disa.mil/mcp/mcpdocs.html>. Because CerTest Version 5.x produces sensitive data, users and/or the local Information Assurance Officer shall ensure all data is protected IAW AFSSI 8502. AFNIC/EVSN confirmed there are no high or medium risk vulnerabilities and the product presents a low risk to the AF-GIG.
4. This certification is for this version, installed IAW the manufacturer's installation instructions. In addition, all applicable Time Compliance Network Orders for this product shall be implemented according to AFI 33-138, *Enterprise Network Operations Notification and Tracking*. This certification is not an Approval to Operate (ATO). Before this software can be used on a system or enclave, the system or enclave ATO shall be updated to include this software version. For questions or to obtain test data, my Information Assurance CA representative POC is AFNIC/EVSC Customer Service Team, (618) 229-6294 (DSN 779-6294) or e-mail: [afnic.ev-ca-ct@us.af.mil](mailto:afnic.ev-ca-ct@us.af.mil).

JOSEPH G. CRONIN, GS-15, DAF  
Air Force Certifying Authority

FOR OFFICIAL USE ONLY

**Vulnerabilities for CerTest Version 5.3.0.0:**

<b>Vulnerability #:</b>	None
<b>Note:</b>	
<b>Severity Category:</b>	
<b>Mitigating Factors:</b>	

**CerTest Version 5.3.0.0 Testing Checklist:**

<b>1. Desktop Review</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
1.1 Will the requested application be deployed on a SDC machine?	X			
1.2 Does the application process, produce, or store sensitive data (e.g., Classified, Privacy Act, HIPAA, etc.)?	X			Users and/or the local Information Assurance Officer shall ensure all sensitive information is protected IAW AFSSI 8502.
1.3 Is the application developed/controlled by a foreign country?		X		PowerTrain Inc. 8201 Corporate Drive, Suite 580 Landover, MD 20785 (301) 731-0091
1.4 Is the application vendor listed under the "Excluded Parties List"?		X		
1.5 Are there any known vulnerabilities for the application (NVD and Security Focus check)?		X		
1.6 Is the request for an older version of the product?		X		
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.)? (Current buying standards: <a href="https://cs.eis.af.mil/a6/itrm/Lists/Computer%20Configurations/AllItems.aspx">https://cs.eis.af.mil/a6/itrm/Lists/Computer%20Configurations/AllItems.aspx</a> )		X		
1.8 Does it use the network during operation (e. g., auto-updates, help files, interface with other systems, etc.)?		X		
1.9 Are administrator rights required to install the application?	X			
1.10 Does the application require administrator rights during operation?		X		

<b>1. Desktop Review</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
1.11 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.)?	X			All users of this application must have read/write privileges on subdirectory where it is installed, i.e., "<Windows System Drive>\Program Files\CerTest" or the user home folder.
1.12 Does the EULA specify limitations such as: a. Restriction for government use, b. User's permission to monitor and/or accept automatic updates, c. User's permission for the application to harvest system or personal information.		X		
1.13 Is this an IA or IA-enabled product?		X		
1.14 Does the application employ use of mobile code technology?	X			Use of mobile code shall comply with the requirements of DoDI 8552.01 and DISA's implementation guidance at <a href="https://powhatan.iie.disa.mil/mcp/mcpdocs.html">https://powhatan.iie.disa.mil/mcp/mcpdocs.html</a> .

**Table 1.5.1 Known Vulnerabilities:**

<b>CVE</b>	<b>CVSS</b>	<b>Version Affected</b>	<b>Summary</b>	<b>Mitigation</b>
None.				

<b>2. Testing Documentation Review</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	<b>Comments</b>
2.1 If testing a trial or unregistered version, does it have the same functionality as the full version?			X	
2.2 Does the documentation provide clear guidance for installing and configuring the application?	X			
2.3 Are dedicated personnel required to operate and/or maintain (vs. simply using the product in process/ analyze/transfer data, etc.)?		X		

<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?		X		
3.2 Does the application add itself to system's application menu?	X			
3.3 Does the application provide an 'Uninstall'?		X		
3.4 Were installation issues found?		X		

<b>4. Testing Application Operation</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>	
4.1 Are there required input files (e.g., doc, xls, pcap, high-risk (exe's), etc.)?	X			Database file types.
4.2 Does the application produce any files?	X			Text and report file types.
4.3 Are there credentials associated with the application?	X			
4.3.1 Are these credentials configurable?	X			
4.3.2 How are these credentials protected?				User ID/password in Microsoft Access Database.
4.4 Does the application provide encryption of data?		X		
4.5 Does the application provide automatic updates or user configurable updates?		X		
4.6 Is the application compatible with a standard user account?	X			
4.7 Were there any other items of note (e.g., violations of security policy)?		X		

<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?		X		
5.2 Was application related network traffic detected during operation?		X		
5.3 Was data transmitted being protected?			X	
5.4 Were exceptions added into the firewall policy?		X		
5.5 If firewall exceptions were added, are they configurable?			X	
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?			X	

5. Testing/Analyzing Network	Yes	No	N/A	Comments
5.7 Are there specific bandwidth requirements?		X		

**Table 5.6.1 Connection Table:**

Port/ Protocol	Source	Destination	Bandwidth	Function

6. Testing Analyzing Configurations	Yes	No	N/A	Comments
6.1 Were system .dll's overwritten with older versions?		X		
6.2 Did the application place application files within acceptable locations?		X		Redirect installation from the default location of "<Windows System Drive>\CerTest" to "<Windows System Drive>\Program Files\CerTest" or the user home folder.
6.3 Did the application install any additional software (e.g., browser plug-ins, toolbars, SQL servers, etc.)?		X		
6.4 Does the additional software have any known vulnerabilities?		X		
6.5 What process name does the application execute under?				certest.exe
6.6 Did the application remove, modify, or install a service?	X			The following pre-existing services stopped: <i>Windows Installer</i> <i>WinHTTP Web Proxy Auto-Discovery</i>
6.6.1 If a service is installed, does setup include automatic start?			X	
6.6.2 Describe any network operations with which the service is associated.			X	
6.6.3 Describe the function of any service installed.			X	
6.7 Are there high-risk Windows registry entries?		X		

**Table 6.7.1-High Risk Registry Entries:**

Registry Type	High Level Registry Entry	Specific Registry Entry	Is it Application Related	Risk Level