DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE NETWORK INTEGRATION CENTER (AFNIC)
SCOTT AIR FORCE BASE, ILLINOIS

MEMORANDUM FOR HQ AFNIC/EVSN

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

SUBJECT: Software Certification for WipeDrive Pro version 5.x
(Certification Termination Date [CTD]: 9 Sep 12)

1. WipeDrive Pro version 5.x is hereby certified IAW AFI 33-210 for use on systems not 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. WipeDrive Pro version 5.x erases entire hard drives permanently so that the original data cannot be recovered. WipeDrive Pro may not be used to sanitize classified hard drives. However, it may be used to overwrite hard drives involved in a classified message incident or classified information spillage.

3. My decision is based on the validation of test data reviewed by HQ AFNIC/EVSN as documented in this certification. HQ AFNIC/EVSN confirmed there is a high-risk finding and the product shall not be used on a system attached to the AF-GIG. In addition, AFSSI 8580 only authorizes Information Assurance Officers/Managers use of this type of product. Therefore, WipeDrive Pro disk(s) should be physically controlled at all times to prevent access by unauthorized users. WipeDrive Pro has not completed Common Criteria certification at the time of this memorandum. However, WipeDrive Pro version 5.x is undergoing testing at the SAIC Common Criteria Testing Laboratory in Columbia, Maryland.

4. This certification is for this version installed IAW the manufacturer's installation instructions. My Information Assurance validation OPR is HQ AFNIC/EVSN, 618-229-6484 (DSN 779-6484) or e-mail: afca.evsn.cots@us.af.mil. Test data may be obtained by contacting HQ AFNIC/EVSN.

CRONIN.JOSEPH.G.1231299714

Digitally signed by CRONIN.JOSEPH.G.1231299714
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USAF, cn=CRONIN.JOSEPH.G.1231299714
Date: 2009.09.09 17:32:14 -05'00'

JOSEPH G. CRONIN, YC-03, DAF
Air Force Certifying Authority

Findings for WipeDrive Pro version 5.1:

Finding:	WipeDrive Pro can be executed by anyone, not just an administrator, by hard-booting a computer with the WipeDrive disk in the disk drive provided the boot sequence is set to look at the disk drive first, thus eliminating any information on the targeted computer.
Note:	The software can be easily downloaded from the internet. The demo version will wipe the first 25% of the targeted storage space and the registered version will wipe the entire targeted area.
Severity Category:	High risk.
Mitigating Factors:	Physical security of the WipeDrive Pro disk(s) should be in place to limit access to authorized users only and precautions taken to prevent unauthorized users from downloading the software from the internet. Also, enforce system-level security by requiring authorized access to boot-disk operations (i.e., require a PROM password to limit the boot sequence).

WipeDrive Pro version 5.1 Testing Checklist:

1. Desktop Review	Yes	No	N/A	Comments
1.1 Will the requested application be deployed on a non-FDCC machine?			X	The application runs from a boot disk and is not dependent on an operating system to run.

1. Desktop Review	Yes	No	N/A	Comments
1.2 Does the application process, produce, or store sensitive data (classified, Privacy Act, HIPAA,…)?	X			This product will be used for cleaning and sanitizing sensitive unclassified media only. While it may also be used for **clearing** classified media, it will not be used for **sanitizing** classified media. However, under extenuating circumstances, it may be used for file/folder overwrite of hard drives involved in a Classified Message Incident (CMI) or classified information spillage. A decision to use this product to clean up the effects of a spillage must be based on operational necessity and mission criticality. It must not be used as a matter of convenience. Use AFSSI 8580, Attachments 2 and 3 for risk determination guidance. In addition, hard drives involved in a CMI or classified information spillage that are overwritten using this product and returned to service must be tracked, remain under organizational control, and destroyed at the end of organizational use.
1.3 Is the application developed/controlled by a foreign country?		X		
1.4 Is the application vendor listed under the “Excluded Parties List”?		X		
1.5 Is the request for an older version of the product?		X		
1.6 Are there software dependencies not provided by FDCC (e.g., Perl, SQL servers)?		X		
1.7 Does it require a network connection to operate (auto-updates, help files, interface with other systems)?		X		

Table 1.7.1 Port and Protocols Required to Operate:

Function	Port/ Protocol	Source	Destination	Data Type	Bandwidth
NONE					

1. Desktop Review	Yes	No	N/A	Comments
1.8 Are administrator rights required to install the application?			X	No installation is necessary to run the WipeDrive application. It can be run from a boot-disk.
1.9 Does the application require administrator rights to execute?		X		Anyone can hard-boot a computer with the boot disk in the disk drive and run the WipeDrive program as long as the system's boot sequence is set to look at the disk drive first.
1.10 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 that is needed is to hard-boot a computer with the boot disk in the disk drive and run the WipeDrive program (provided the system's boot sequence is set to look at the disk drive first).
1.11 Does the EULA specify limitations such as: 1. Restriction for government use, 2. User's permission to monitor and/or accept automatic updates, 3. User's permission for the application to harvest system or personal information.	X			U.S. GOVERNMENT RESTRICTED RIGHTS. If you are acquiring the Software on behalf of any unit or agency of the US Government the following provision applies: It is acknowledged that the Software and the Documentation were developed at private expense and that no part is in the public domain and that the SOFTWARE and Documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 52.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Contractor/Manufacturer is White Canyon, Inc.
1.12 Are there any known vulnerabilities for the application (NVD and Security Focus check)?		X		

Table 1.12.1 Known Vulnerabilities:

CVE	CVSS	Version Affected	Summary	Mitigation
NONE				

1. Desktop Review	Yes	No	N/A	Comments
1.13 Is this an IA or IA enabled product?	X			Has not been common criteria tested.
1.14 Is testing required?	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? (If not comment on the differences)		X		The Demo version of the application will wipe only the first 25% of the drive it is run against, as opposed to 100% with the registered version.
2.2 Does the documentation provide clear guidance for installing and configuring the application?	X			
2.3 Is the source code available for this application (open source)?		X		However, reference is made to the GNU General Public License. This indicates that open source code can be obtained for any open source component(s) that may exist.
2.4 Are dedicated personnel required to operate and/or maintain (vs. simply using the product in process/ analyze/transfer data, etc.)?		X		
2.5 Are there any hardware dependencies (e.g., special video, sound card, or microphone specifications)?		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 system's application menu?			X	
3.3 Does the application provide an 'Uninstall'?			X	
3.4 Were installation issues found? If so, document them in the comments section.			X	Application was run from a boot disk.

4. Testing Application Operation	Yes	No	N/A	
4.1 Are there required input files (e.g., doc, xls, pcap, high risk (exe's) etc)?		X		
4.2 Does the application produce any files?		X		
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?			X	
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		

5. Testing Analyzing Network	Yes	No	N/A	Comments
5.1 Review capture file from Section 3, was application related network traffic detected during installation?			X	
5.2 Review capture file from Section 4, was application related network traffic detected during execution?		X		
5.3 Was data transmitted being protected?		X		
5.4 Were exceptions added into the firewall policy?			X	
5.4.1 If exceptions were added, are they configurable?			X	
5.5 If crossing the enclave boundary are the ports allowed by the DoD PPS Matrix?			X	
5.6 Are there specific bandwidth requirements?			X	

Table 5.6.1 Connection Table:

Function	Port/ Protocol	Source	Destination	Data Type	Bandwidth
NONE					

6. Testing Analyzing Configurations	Yes	No	N/A	Comments
6.1 Were system .dlls overwritten with older versions?			X	
6.2 Did the application place application files within acceptable locations?			X	
6.3 Did the application install any additional software (e.g., browser plug-ins, toolbars, SQL)?			X	
6.3.1 Does the additional software have any known vulnerabilities?			X	
6.4 What process name does the application execute under?			X	
6.5 Did the application remove, modify, or install a service?			X	
6.5.1 If a service is installed is it set to automatically start?			X	
6.5.2 Describe any network operations with which the service is associated.			X	
6.5.3 Describe the function of any service installed			X	
6.6 Are there high risk Windows registry entries?			X	

Table 6.6.1-High Risk Registry Entries:

Registry Type	High Level Registry Entry	Specific Registry Entry	Is it Application Related	Risk Level
NONE				