DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

MEMORANDUM FOR DEFENSE HEALTH AGENCY AUTHORIZING OFFICIAL

SUBJECT: Software Certification for ***Spirola version 3.x***

1. ***Spirola version 3.x*** is hereby certified in accordance with DoDI 8510.01 for use on ***standard desktop*** systems ***'for NIPR use only use'*** and placed on the DHA Evaluated/Approved Products List (DHA E/APL). 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 2.x or version 4.x would not be grandfathered under this certification.

2. Spirola version 3.x is an application to assist the provider in monitoring and interpreting computerized longitudinal spirometry data for individuals and groups.

3. My decision is based on the validation of test data reviewed by DHA Cyber Security Division and documented in this certification. Because Spirola version 3.x stores/produces/processes sensitive data, users and/or the local Information Assurance Officer shall ensure all Spirola version 3.x controlled unclassified information is protected IAW CJCSI 6510.01. 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. DHA Cyber Security Division discovered high risk vulnerability with this application that shall be mitigated prior to use. Once the administrator implements the mitigation actions described below, the vulnerability will be mitigated and the application will present a low risk to the system or enclave.

   a. Spirola version 3.x can pull data from Database Connections. By default, the 'Encrypt Connection" is set to "No (Default)". If database connections are used 'Encrypt Connection' must be set to Yes.

4. All applicable Time Compliance Network Orders for this product shall be implemented according to DoDI 8410.03, Network Management and all other applicable Department of Defense Instructions (DoDI)

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) must 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 SCA representative POC is DHA Cybersecurity, e-mail: DHA NCR IT Mailbox CSD Assmnt and Authorization@mail.mil.

REBERKENNY.CLARISSA.M.1228628847

Digitally signed by REBERKENNY.CLARISSA.M.1228628847
Date: 2017.07.10 16:14:15 -04'00'

Jeffrey A. Eyink
Security Control Assessor
Defense Health Agency

Vulnerabilities for Spirola version 3.0.3:

Vulnerability:	Spirola version 3.x can pull data from Database Connections. By default, the 'Encrypt Connection" is set to "No (Default)".
CVE Affected:	N/A
Note:	N/A
Severity Category:	High
Mitigating Factors:	If database connections are used 'Encrypt connection' must be set to Yes.

Spirola version 3.0.3 Testing Checklist:

1. Desktop Review	**Yes**	**No**	**N/A**	**Comments**
1.1 Will the requested application be deployed on a DHA standard imaged machine?	X			
1.2 Does the application process, produce, or store sensitive data (e.g., Classified, Privacy Act, HIPAA, etc.)?	X			Unclassified, HIPAA
1.3 Is the application developed/controlled by a foreign country?		X		NIOSH cdc.gov 1600 Clifton Rd Atlanta, GA, 30329-4018
1.4 Is the application vendor listed as an exclusion on System for Award Management (SAM)?		X		
1.5 Are there any known vulnerabilities for the application?		X		
1.6 Is the request for an older version of the product?		X		

1. Desktop Review	Yes	No	N/A	Comments
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: https://info.health.mil/hit/infosec/assessor/ApprovedProductsTrans/Lists/EPL/AllItems.aspx)		X		
1.8 Are administrator rights required to install the application?	X			
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.)?		X		
1.10 Is this an IA or IA-enabled product?		X		
1.11 Are there specific bandwidth requirements?		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 Does the documentation provide clear guidance for installing and configuring the application?	X			

2. Testing Documentation Review	Yes	No	N/A	Comments
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 system's application menu?	X			
3.3 Does the application provide an 'Uninstall'?	X			
3.4 Were installation issues found?		X		

4. Testing Application Operation	Yes	No	N/A	Comments
4.1 Are there required input files (e.g., .dot, .ini, .config, manifest, etc.)?		X		
4.2 Does the application produce any files?	X			*.csv, *.xml, *.mdb, *.pdf
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 (data at rest)?		X		
4.5 Does the application provide automatic updates/user configurable updates?		X		

4. Testing Application Operation	Yes	No	N/A	Comments
4.6 Does the application include a Software Improvement Program which automatically sends various types of information back to the Vendor?		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 Was data transmitted being protected?		X		'Encrypt connection' must be set to Yes for any Database Connections.
5.4 Were exceptions added into the firewall policy?		X		
5.5 If firewall exceptions were added, will reconfiguring them impact the application?			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			

Table 5.6.1 Connection Table

Description and Purpose	Port/ Protocol/ Data Service	Origin Domain Name	Destination Domain Name	Bandwidth	Local Service Only?
Application Help Link (Spirola Home)	80/tcp/http 443/tcp/https	DISA Win7 Secure Host Baseline	www.cdc.gov	Low	No
Database Connection	1433/tcp/mssql	DISA Win7 Secure	User provided IP address	Medium	No

Description and Purpose	Port/ Protocol/ Data Service	Origin Domain Name	Destination Domain Name	Bandwidth	Local Service Only?
(MSSQL)		Host Baseline			

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 Did the application place application files within acceptable locations?	X			
6.4 Did the application install any additional software (e.g., browser plug-ins, toolbars, SQL servers, etc.)?		X		
6.5 Does the additional software have any known vulnerabilities?		X		
6.6 What process name does the application execute under?	X			Spirola.exe
6.7 Did the application remove, modify, or install a service?	X			Installed: - None Modified: - AppMgmt - msiserver - osppsvc - TrustedInstaller - WdiSystemHost - WinHttpAutoProxySvc Removed: - None
6.7.1 If a service is installed, does setup include automatic start?		X		
6.7.2 Describe any network operations with which the service is associated.			X	
6.7.3 Describe the function of any service installed.			X	

6. Testing Analyzing Configurations	Yes	No	N/A	Comments
6.8 Were there any other items of note (e.g., violations of security policy)?		X		