

**Software Product Security Evaluation
Version 2.00**

**Centers for Disease Control and Prevention
National Center for Chronic Disease Prevention and Health Promotion
Division of Cancer Prevention and Control
National Program of Cancer Registries**

November 12, 2009

Software Product Security Evaluation

About the Requestor

Requesting Office:

Date: February 2, 2009

Requestor Name:

Phone:

User ID:

Title:

About the Software

Software Name:

Software Version Number:

Manufacturer Name:

Manufacturer Address:

Manufacturer Phone:

Manufacturer Web Site:

Software Type:

Other (specify):

Application Use:

Other (specify):

Operating Environment (check all that apply):

- Windows XP
- Windows 2000
- Windows (prior versions)
- UNIX/Linux
- Other (specify):

Provide a comprehensive description of the software below:

Thoroughly explain how this software will be used and why it is necessary to accomplish your job duties below:

Have you checked to see if approved software meets your needs?

Does the registry offer alternate or similar software?

If the registry offers alternate or similar software, thoroughly explain why it does not meet your business needs below:

Is this software currently in use, or has it been used previously in this group?

If yes, indicate the starting, and if applicable, the ending dates of its use:

Starting Date:

Ending Date:

Is this request for a version upgrade?

If yes, indicate the current and proposed versions. Attach the vendor's list of changes and improvements, preferably from the vendor.

Current Version:

New Version:

Define the extent to which the software will be distributed and where. Indicate if users will be external to the cancer registry, and if so, describe where.

Provide the cancer registry workstation names for each location where the software will be installed. Attach a separate page if necessary.

Does the software require elevated user privileges (e.g. Power User level, Administrator level) on user workstation(s):

For initial installation?

For operation after initial installation?

If this software requires elevated user privileges for operation after initial installation, what privilege level is required?

If elevated privileges are required for operation, explain why they are needed below:

Note: Approval of the software does not imply approval of elevated user privilege. Requests for elevated user privilege must be submitted formally to the cancer registry.

Will the software be used to process *sensitive but unclassified* (SBU) information and/or *Information in Identifiable Form* (IIF)?

If yes, describe the SBU information and/or IIF that will be processed below:

Note: The “sensitive but unclassified” designation is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The term “IIF” includes any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means (such as names, Social Security numbers, and medical records numbers).

During normal operation, does this software require access to Internet resources (such as data from the vendor or external databases)?

If yes, indicate the URL to which it will connect and frequency of connection below:

Location of external database:

IP Address:

Will the vendor ever initiate or push patches, updates, upgrades, or anything else to the workstation or system without user consent or notification?

Describe the mechanism and frequency for the vendor to provide updates, such as patches, to this software (such as a direct connection to the vendor’s server, updates can be downloaded from a Web page, etc.) below:

Indicate whether this software has been evaluated successfully under either of the following programs:

(a) National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) (<http://www.niap-ccevs.org/cc-scheme/>)

If yes, describe:

Common Criteria Scheme:

Evaluation Assurance Level (EAL) Rating:

(b) National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) [Cryptographic Module Validation Program](http://csrc.nist.gov/cryptval/140-1/1401val.htm) (<http://csrc.nist.gov/cryptval/140-1/1401val.htm>)

If yes, describe:

Certificate Number:

FIPS 140 Validation:

Vulnerability Database Check

Check the databases at these locations for vulnerabilities in the requested software. Be specific for the version requested.

Vulnerabilities found in National Vulnerability Database (<http://nvd.nist.gov/nvd.cfm>)?

If yes, please list:

Vulnerabilities found in Security Focus Database (<http://www.securityfocus.com>)?

If yes, please list:

Vulnerabilities found in Open Source Vulnerability Database (<http://www.osvdb.org>)?

If yes, please list:

Please provide any additional comments or pertinent information below, or attach additional pages and documentation.