Security Overview for Registry Plus Software Programs for Cancer Registries

July 19 , 2012

Topics

[Overview 1](#_Toc330466572)

[NIST Spreadsheet 1](#_Toc330466573)

[Web Plus 2](#_Toc330466574)

[NPCR Web Site for an Introduction to Data Security 2](#_Toc330466575)

[Other Registry Plus Documents that Specifically Address Security 3](#_Toc330466576)

[Application Scans of Web Plus 3](#_Toc330466577)

[Other Data Security Related Links 4](#_Toc330466580)

[Helpful Sites 4](#_Toc330466581)

[Reference Documents 4](#_Toc330466582)

# Program Director Overview

CDC's National Program of Cancer Registries (NPCR) has successfully gone through the Health and Human Services (HHS) Certification and Accreditation (C&A) review process for Registry Plus Web Plus module and Level III certification on all the other Registry Plus modules. Through this process all the HHS /C&A National Institute of Standards and Technology (NIST) controls have been addressed in Web Plus.

All Registry Plus modules not assessable outside institution’s firewall have completed the Level III review for software and networking products after addressing the issues of support, infrastructure impact, lifecycle maintenance and security requirements. These products must be demonstrated as compatible with CDC's IT strict infrastructure and IT Security standards. All Level III products must undergo and pass the Offices Office of the Chief Information Security Officer (OCISO) Level III Security Risk Assessment process.

It is highly recommended that all Central Cancer Registries (NPCR) develop a security policy that is specific to the needs of the registry and the organization in which the registry operates.

The following information will to help cancer registries to work with its organization's technical support staff for making cancer registry data secure to develop or audit their current security policy. The security policy of the organization in which the registry operates must meet or be modified to accommodate the specific concerns of the cancer registry.

# NIST Spreadsheet

National Institute of Standards and Technology (NIST) controls have been addressed in Web Plus. The Registry Plus Development Team has completed the Web Plus CDC NIST Controls and have the details available in a comprehensive spreadsheet. This spreadsheet is ready for state central cancer registries using Web Plus requiring security details on the National Institute of Standards and Technology (NIST) security controls. This spreadsheet will be updated as new information is published by NIST. It can be used to address security requirements by your agency security steward(s), local/federal U.S. Department of Veterans Affairs security officers, or other organizations requiring security documentation.

These controls are included in a spreadsheet that is posted at the following CDC ftp site: <ftp://ftp.cdc.gov/pub/Software/RegistryPlus/Security> Excel file name ([CDC\_ NISTControls\_WEBPLUS\_04202012\_VERSION\_01.01.xlsx](ftp://ftp.cdc.gov/pub/Software/RegistryPlus/Security/CDC_%20NISTControls_WEBPLUS_04202012_VERSION_01.01.xlsx)) Questions or concerns regarding this document can be sent to Joseph Rogers [jdr0@cdc.gov](mailto:jdr0@cdc.gov).

# Web Plus

From a security perspective, the most vulnerable module of Registry Plus is the Web Plus application. It is the only module accessible outside the institution’s firewall and the registries “demilitarized zone”. Some controls need to be addressed by the security officer at the institution using Web Plus to address NIST requirements. These controls are included in the detailed spreadsheet. This document can be used to address security requirements by your agency security steward(s), local/federal U.S. Department of Veterans Affairs security officers, or other organizations requiring security documentation.

General information regarding Web Plus security can be found on the following links:

* Web Plus Security Features: <http://www.cdc.gov/cancer/npcr/tools/registryplus/wp_security.htm>
* Maximizing Data Security in Web Plus: <http://www.cdc.gov/cancer/npcr/tools/registryplus/wp_security2.htm>
* Registry Plus Central Registry Tools Systems and IT Personnel Requirements:

<http://www.cdc.gov/cancer/npcr/pdf/registryplus/registry_plus_requirements.pdf>

In addition, the Web Plus application has gone through different levels of scans before deployment to ensure security. The Web Plus application was thoroughly tested through IBM AppScan tool for possible SQL injection and Cross-Site scripting vulnerabilities. Any recommendations by the AppScan tool were fixed in the current release of the Web Plus application and were retested using AppScan. CDC-NPCR will provide institutions planning to use or using Web Plus with vulnerability and source code security scan logs utilizing the IBM Apps Scan tool (external or source code) with each major release of Web Plus. These logs will be available on both the current and the eventual production version of the software.   If you decide to run your own vulnerability scan, we will address all critical issues relating to institutional security requirements, i.e. state, university, VA, or DOD. This applies to all the CDC-NPCR applications.

# NPCR Web Site for an Introduction to Data Security

All registries that submit data to NPCR should have a security policy that is specific to the needs of the registry and the organization in which the registry operates. This includes registries that are a part of a larger public health department, a university, or an institution that provides information technology support for several programs. The security policy of the organization in which the registry operates must meet or be modified to accommodate the specific concerns of the cancer registry.

This data security web site provides general security information specifically tailored for central cancer registries. This site provides information on the following topics in Data Security:

* Introduction <http://www.cdc.gov/cancer/npcr/tools/security/>
* Guidelines for Cancer Registries: <http://www.cdc.gov/cancer/npcr/tools/security/requirements.htm>
* Planning: <http://www.cdc.gov/cancer/npcr/tools/security/planning.htm>
* CDC Certification and Accreditation (C&A) Process: <http://www.cdc.gov/cancer/npcr/tools/security/cdcca.htm>
* Security Features in Web Plus: <http://www.cdc.gov/cancer/npcr/tools/security/wp_security.htm>
* Maximizing Data Security in Web Plus: <http://www.cdc.gov/cancer/npcr/tools/security/wp_security2.htm>
* Introduction to Data Encryption: <http://www.cdc.gov/cancer/npcr/tools/security/encryption.htm>
* Details about Data Encryption: <http://www.cdc.gov/cancer/npcr/tools/security/encryption2.htm>
* Data Breach Response: <http://www.cdc.gov/cancer/npcr/tools/security/breach.htm>
* Vulnerability Management Life Cycle: <http://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm>
* Frequently Asked Questions about Data Security: <http://www.cdc.gov/cancer/npcr/tools/security/faq.htm>
* Technical Support: <http://www.cdc.gov/cancer/npcr/tools/security/support.htm>
* Data Security Related Links: <http://www.cdc.gov/cancer/npcr/tools/security/links.htm>

# Other Registry Plus Documents that Specifically Address Security

* Review of top security principle questions for Web Plus from the Pennsylvania Department of Health. The document is named PA-Security Principles for Web Plus(Web Plus CA² Certification Follow-up.pdf and can be found at the following link. <ftp://ftp.cdc.gov/pub/Software/RegistryPlus/Security/Web%20Plus%20Security%20Memos/>
* The Web Plus Security Assessment notice from 2007 can be found at: <ftp://ftp.cdc.gov/pub/Software/RegistryPlus/Security/Web%20Plus%20Security%20Memos/>
* The completed Department of Defense JTF CapMed Software Test Request Worksheets for the CRS Plus, Prep Plus and Web Plus applications can be found at: <ftp://ftp.cdc.gov/pub/Software/RegistryPlus/Security/DOD/>

# Application Scans of Web Plus

In an effort to address high level application-security and risk-management we are using the most complete portfolio solution available by the market leader in this type of tool to test the Web Plus product. This tool is used both at the CDC as well as central cancer registries active in managing application risk in their systems. With advanced security testing and a platform managing application risk, this portfolio solution delivers the security expertise to application management that allowed us to identify potential vulnerabilities, and reduce overall application risk before these liabilities could be exploited. These technologies keep up with the latest threats and provide actionable results.

All potential vulnerabilities and application risk identified with the portfolio solution are addressed and the application rescanned. This new software version is then scanned again by central cancer registries to ensure the results are duplicated. The scan results will be available to Registry Plus users in PDF document.

Here are some of the highlights of the settings for the scans:

1. Scans for vulnerabilities will be conducted each and every page.
2. We scan Web Plus using privilege escalation feature. The privilege escalation is very important since Web Plus has different types of users and each user is limited to certain functionalities.
3. CDC uses the edition of the tool that has all features including privilege escalation.
4. CDC does use SSL option during the scans.
5. CDC can provide detailed scan report in PDF file format. The detailed PDF is very important for Registry Plus development team to review the issues and mitigate. The scan results will be available to Registry Plus users in PDF document for each major release of the application.

# Other Data Security Related Links

# Helpful Sites

* National Institute of Standards and Technology (NIST) FIPS 140-2 Standard [Cryptographic Module Validation Program (CMVP)](http://csrc.nist.gov/groups/STM/cmvp/)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html)
* U.S. Department of Health and Human Services (HHS) [Encryption Standard for Mobile Devices and Portable Media](http://www.hhs.gov/ocio/policy/20070001001s.html)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html) (2007-0001.001S)
* [CDC Unified Process](http://www2a.cdc.gov/cdcup/)
* [Microsoft® Security Central](http://www.microsoft.com/security/)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html)

# Reference Documents

* CDC's [Registry Plus™ Security Features Adobe PDF file [PDF-35KB]](http://www.cdc.gov/cancer/npcr/tools/security/RP_Security_Feature.pdf)
* [Software Product Security Evaluation Adobe PDF file [PDF-176KB]](http://www.cdc.gov/cancer/npcr/pdf/Product_Security_Evaluation_Form.pdf) to request permission to install software on CDC's network
* [Moderate NIST Control Document Adobe PDF file [PDF-400KB]](http://www.cdc.gov/cancer/npcr/pdf/NIST_Security_Controls_Moderate.pdf) outlines security reviews prior to the installation of software applications on CDC's network
* [NIST checklist for protection of remote information Adobe PDF file [PDF-118KB]](http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html)
* [*Standards for Cancer Registries Volume III: Standards for Completeness, Quality, Analysis, Management, Security and Confidentiality of Data,*](http://www.naaccr.org/StandardsandRegistryOperations/VolumeIII.aspx)*[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html)* especially Chapter 6, "Security and Confidentiality"
* U.S. General Services Administration [SmartBUY Program Overview](http://www.gsa.gov/portal/content/105119)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html) and [Data at Rest (DAR) Encryption Fact Sheet Microsoft Word file [DOC-56KB]](http://contacts.gsa.gov/graphics/insite/fas/DAR_Fact_Sheet_7-8-08.doc)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html)
* U.S. Department of Health and Human Services [Laptop Encryption Policy Microsoft Word file [DOC-38KB]](http://www.hhs.gov/ocio/policy/policydocs/20070001001s.doc)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html)
* Memo [M-06-16 Adobe PDF file [PDF-118KB]](http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html) “Protection of Sensitive Agency Information” from the Executive Office of the President, OMB
* Memo [M-07-16 Adobe PDF file [PDF-227KB]](http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf)[External Web Site Icon](http://www.cdc.gov/Other/disclaimer.html) “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” from the Executive Office of the President, OMB