**Security Overview for Registry Plus Software Programs for Cancer Registries**

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”. 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>

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. These controls are included in a spreadsheet that can be requested from the registry plus staff (Joseph Rogers jdr0@cdc.gov) . Some controls need to be addressed by the security officer at the institution using Web Plus. These controls are included in the detailed spreadsheet.

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.

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.

Please let us know if you require any additional issues that are required to be addressed and we will try to meet these requests.