http://intranet.cdc.gov/ociso/canda/

Security Certification & Accreditation (C&A)

The CDC Certification & Accreditation (C&A) process ensures that information systems are operating with appropriate management review, that ongoing security control monitoring occurs, and that reaccreditations take place periodically or there is a significant change to an information system or its environment.

**Legal Basis and Requirements**

Based on the legislation identified below, the Office of Management and Budget (OMB) requires federal government agencies to: (1) plan for security; (2) ensure that security responsibilities are assigned; (3) periodically review information system security controls; and (4) authorize system processing prior to operations and periodically, thereafter.

* Public Law 100-235, the Computer Security Act of 1987, requires a risk-based security approach policy to ensure for cost-effective Information Technology (IT) security.
* The E-Government Act (Public Law 107-347), signed into law in December 2002, recognizes information security' importance to United States economic and national security interests. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program.
* FISMA, along with the Paperwork Reduction Act of 1995 and the 1996 Clinger-Cohen Act, explicitly emphasize a risk-based policy for cost-effective security.

**Systems Requiring Certification**

All computers, down to the individual PC, must be provided adequate security or security equal with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. Personal computers in many cases receive blanket C&A due to common system characteristics. Server-based computers hosting applications require more analysis and generally require individual C&A. System environment analysis is often necessary to define system specific C&A requirements.

**Security Certification**

Security Certification is a comprehensive evaluation of CDC management, operational, and technical security controls for an information system. This evaluation documents the effectiveness of existing security controls in a particular operational environment and includes recommendations to implement additional controls to mitigate outstanding system vulnerabilities. Security certification results are used to assess risks to the system and update the system's security plan.

**Security Accreditation**

Security Accreditation is the official CDC management decision to authorize an information system to operate. By accrediting an information system, a CDC official is explicitly acknowledging his or her responsibility for adverse impacts to the CDC resulting from the documented risk levels for the system. The C&A documents provide the factual basis for a CDC authorizing official to render a security accreditation decision. It is essential that CDC officials have the most complete, accurate, and trustworthy information possible to make credible, risk-based decisions on whether to authorize system operation.

**Page Last Updated: January 19, 2012**