SWOG Statistics and Data Management Center

Supported at Cancer Research And Biostatistics

2019-2020
FISMA 2002*
Compliance Assessment

**Federal Information Security Management Act of 2002*

Reviewed March 25, 2019

Covering Security for Systems within the Scope of FISMA 2002 Requirements

Statement of Certification and Accreditation

The undersigned certify that to their knowledge that SWOG Statistics and Data Management Center (SDMC) information systems and constituent system-level components located at CRAB and within the purview of FISMA 2002, including the Rave® Electronic Data Capture (EDC) system hosted at Medidata, are in compliance. Based on security certifications of systems and supporting evidence provided in the associated security accreditation package (including current system security plan, security assessment report, and plan of action and milestones), the undersigned have determined that risk to information provided by public and private agencies is acceptable. This is formal declaration that security controls have been implemented in the information system and that security meets or surpasses levels of acceptable risk. A summary of recommendations for implementation of additional security controls is attached.

This certification and accreditation of the information system will remain in effect through the next annual renewal period, 1st quarter of 2020, as long as any potential vulnerability reported during continuous monitoring processes do not result in unacceptable risk.

28 MAR 2019

Lisa Upshaw, Director of Quality Compliance — Date

28 MAR 2019

Curt Malloy, Vice President, Chief Operations Officer — Date

28 MAR 2019

Keith Goodman, Vice President, Chief Technology Officer — Date

The complete 2017-18 FISMA Compliance Assessment is available to SWOG member institutions upon request.

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Certification based, in part, upon:

- **Special Publications 800-53 Rev. 4 (April 2013) & 800-53A Rev. 4 (Dec 2014)**
(Recommended Security Controls for Federal Information Systems)
- **FIPS Publications 140-2 (Dec 2002)**
(Security Requirements for Cryptographic Modules)
- **FIPS Publications 199 (Feb. 2004) & 200 (March 2006)**
(Standards for Security Categorization & Minimum Security Requirements for Federal Information and Information Systems)
- **Other NIST Publications and Security Analysis Tools**

SUMMARY OF RECOMMENDATIONS

1. Media Use: SDMC staff utilize iPhone and BlackBerry devices which have been deployed using best practices for security and privacy. Some recent modifications to the mobile device infrastructure support these devices. An SOP covering mobile support is under development and review. It is recommended that this SOP be completed prior to the next review.
2. Information Security Architecture: Current SOPs cover internal systems. We provide due diligence in review of external systems which are evaluated using the same criteria as internal systems. External systems used with federal data are reviewed by the NCI for security compliance. The SWOG SDMC reviews compliance reports for external systems as they are made available.