



2021-2022
FISMA Compliance Assessment

**Federal Information Security Modernization Act of 2014*
Reviewed July 30, 2021

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 Cancer Research Network Statistics and Data Management Center (SDMC) information systems and constituent system-level components located at Cancer Research And Biostatistics (CRAB) and within the purview of FISMA 2014 and the NIST Risk Management Framework (v. 1.1), including the Rave® Electronic Data Capture (EDC) system hosted at Medidata, meet compliance requirements. 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 a 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 renewal period, 3rd quarter of 2022, as long as any potential vulnerability reported during continuous monitoring processes do not result in unacceptable risk.

<p>DocuSigned by: Lisa R. Upshaw</p> <p> Signer Name: Lisa R. Upshaw Signing Reason: I approve this document Signing Time: 09 August 2021 3:33:28 PM PDT 452DEF8D0C954257B90DD3445D962AC9</p>	<p>09 August 2021 3:33:33 PM PDT</p>
<p>DocuSigned by: <i>Curt Malloy</i></p> <p> Signer Name: Curt Malloy Signing Reason: I approve this document Signing Time: 09 August 2021 3:40:22 PM PDT 46BFFF29F6C04E87A27F5519396D7D61</p>	<p>09 August 2021 3:40:26 PM PDT</p>
<p>DocuSigned by: <i>Keith Goodman</i></p> <p> Signer Name: Keith Goodman Signing Reason: I approve this document Signing Time: 10 August 2021 6:11:05 AM PDT 2E21E07796C94FCB558751D9B657B19</p>	<p>10 August 2021 6:11:23 AM PDT</p>

Lisa Upshaw, Director of Quality Compliance

Curt Malloy, Vice President, Chief Operations Officer

Keith Goodman, Vice President, Chief Technology Officer



July 30, 2021

The complete 2021-2022 FISMA Compliance Assessment is available to SWOG member institutions upon request.



Certification based upon NIST Risk Management Framework, including in part:

Special Publications

800-52 Rev. 2 (August 2019)

800-53 Rev. 5 (Dec 2020) Security and Privacy Controls for Information Systems and Organizations

800-53B (Oct 2020) Control Baselines for Information Systems and Organizations

800-60, Rev. 1 (Aug. 2008) Guide for Mapping Security Controls

FIPS Publications

140-2 (Dec 2002) Security Requirements for Cryptographic Modules

199 (Feb. 2004) Standards for Security Categorization of Federal Information and Information Systems

200 (March 2006) Minimum Security Requirements for Federal Information and Information Systems

Other NIST Publications and Security Analysis Tools

SUMMARY OF RECOMMENDATIONS

1. Media Use (MP-7): SDMC staff agree to policies and procedures that limit the use of portable media and mobile devices. An acceptable use agreement is under revision with an increased emphasis on media protection and will be implemented prior to the next compliance assessment.
2. Information Security Architecture (PL-8): Current Standard Operating Procedures (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.
3. Supply Chain Risk Management Plan (SR-2): SDMC staff are developing a Supply Chain Risk Management Plan that assesses dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, that present an increasing level of risk to an organization. The Supply Chain Risk Management Plan will be implemented prior to the next compliance assessment.
4. Supply Chain Controls and Processes (SR-3): SDMC staff are developing Supply Chain Controls and Processes that include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply Chain Controls and Processes will be implemented prior to the next compliance assessment.