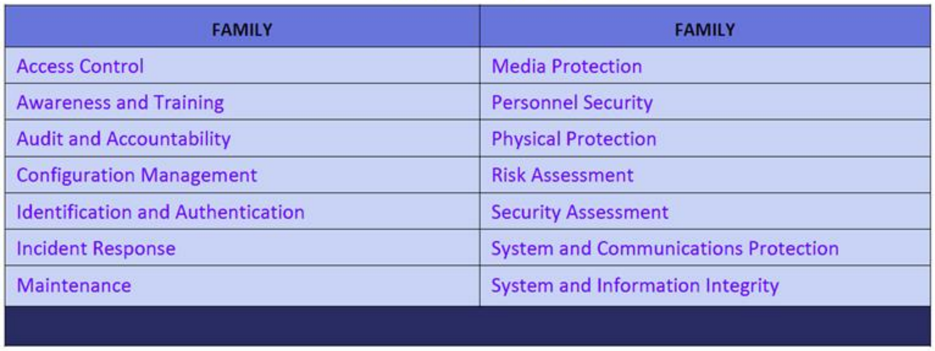
GAITS Security Overview

The Guidance and Impact Tracking System (GAITS) platform is a secure, web-based project and portfolio management platform designed to assist the commercialization of healthcare innovations by helping teams with innovative healthcare ideas, and the portfolio managers that support them, learn from the experiences of others to more efficiently speed innovative solutions to patient care.

The Consortia for Improving Medicine with Innovation & Technology (CIMIT) developed and operates GAITS on secure AWS servers. CIMIT recognizes the imperative to protect the intellectual property of teams that use GAITS. To do so, it maintains a System Security Plan (SSP) for GAITS based on the National Institutes of Standards and Technology (NIST) 800-171 Revision 2, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations for both systems.* The security requirements for protecting the confidentiality of data processed by the system are based on requirements derived from NIST 800-53 controls. The recommended security requirements for protecting the confidentiality of CUI requires 110 controls across fourteen (14) control families.

TABLE 1: SECURITY REQUIREMENT FAMILIES



FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

An Authorization to Operate (ATO) package (SSP, Security Assessment Report (SAR) and Plan of Actions and Milestones (POA&M) have been developed to ensure that the system security posture is maintained. Penetration testing, security control assessment by an independent third party, and regular vulnerability assessments of the underlying platform are conducted. Risk management through POA&M tracks and mitigates any risks identified.

The GAITS platform leverages features such as In-transit and at-rest encryption (256 bit AES) to protect data confidentiality and integrity, and 99.9% Service Level Agreement (SLA) guarantees data availability. Granular Permission control and Identity as well as access management addresses the mission-critical need to ensure appropriate access to enterprise resources while also meeting rigorous compliance standards.

Rev 1
December 5, 2021