

FISMA Cybersecurity Certification and Authorization to Operate

To

CISO, The Emmes Company, LLC

Date: Jul/27/2026

401 N. Washington Street Suite 700, Rockville, MARYLAND 20850, USA.

From: Lead Assessor, ISIT Consultants, Pvt. Ltd.

Subject: Authority to Operate (ATO) for Emmes Company Advantage eClinical Suite

Introduction

This letter formally authorizes the operation of the Emmes Advantage eClinical Suite for data collection and associated enterprise infrastructure, which is a collection of integrated and web-enabled application subsystems, support utilities, software and hardware that have specifically been designed, developed and deployed to support secure data entry and reporting for the projects and scientific studies that Emmes supports.

System Description

The Advantage eClinical Suite contains internal productivity tools for the design, validation, and deployment of project-specific content that is consistent with the operational rules of the Advantage platform. The platform is workflow, component, and service driven. Core development and client-specific configuration and customization are defined by the Emmes Advantage eClinical (ADV) SOPs, Validation (VAL) SOPs, and the Master Software Verification and Validation Plan (VMP). The standard or default workflow is frequently modified by projects to utilize available Advantage subsystems or to plug in unique project-specific functional components. All components, services, and project-specific functions require user authentication. All use and activity is logged.

The primary data handling components of the Advantage eClinical Suite are EDC (Electronic Data Capture), Epro (electronic Patient Reported Outcomes), Global Trace, and TED (Transform, Extract & Download). These components are supported by semi-automated adverse event (MedDRA) and medication (WHODRUG) coding systems. New components and enhancements to existing components are added to the Advantage eClinical Suite and made available to projects as they are developed, validated, and deployed.

Emmes makes significant project-specific enhancements to meet the needs of our clients. It is common to have these project-specific enhancements refined and added as standard features to future releases of the Advantage eClinical Suite.

System Environment

Network

The Emmes system network environment consists of:

- AWS Components (S3, ECS, Lambda, CMS etc)
- AWS DB(DynamoDB)
- AWS Security components (VPC, SES, SGS, SNS, ACM etc)
- AWS monitoring tools (Cloudwatch, inspector, GuardDuty, Security hub, Cloud trail etc)

Remote Access

Emmes staff can also remotely access the Advantage eClinical Suite network via VPC environment. User access requires multifactor authentication with the same token authentication as internal access. Additional security features that protect the network while remote VPN or UAG users are connected include Cache Cleaner and Advanced Endpoint Protection.

Data Safety

Emmes systems are hosted on AWS cloud Infra. The redundancy is built using the DR service from AWS.

Computing and Processing

The Advantage eClinical Cloud (AEC) runs on a Node.js runtime environment (Version 22). The application utilizes Amazon DynamoDB, Amazon S3, and a relational database management system (RDBMS) for data storage.

System Characterization

INFORMATION SYSTEM CATEGORIZATION	- MODERATE
INFORMATION SYSTEM OPERATIONAL STATUS	- OPERATIONAL
INFORMATION SYSTEM TYPE	- MAJOR APPLICATION

Security Controls Assessment Summary

Different applicable controls from following control families have been assessed. Details of each control and their assessment status have been described in the **FISMA Implementation -Assessment Workbook**.

Control Family	Total controls	Total controls (Applicable)	Total controls (Not Applicable)	Evidence Available	Missing Evidences	Compliance percentage %	Controls marked as satisfied	Risk identified	% Complete	Implementation Compliance percentage %
Access Control(AC)	147	67	80	67	0	100%	67	0	67/67	100%
Awareness and Training (AT)	17	12	5	12	0	100%	12	0	12/12	100%
Audit and Accountability (AU)	69	35	34	35	0	100%	35	0	35/35	100%
Assessment,Authorization and monitoring(CA)	32	18	14	18	0	100%	18	0	18/18	100%
Configuration Management (CM)	66	37	29	37	0	100%	37	0	37/37	100%
Contingency Planning (CP)	56	42	14	42	0	100%	42	0	42/42	100%
Identification and Authentication (IA)	70	23	47	23	0	100%	23	0	23/23	100%
Incident Response (IR)	42	29	13	29	0	100%	29	0	29/29	100%
Maintenance (MA)	30	8	22	8	0	100%	8	0	8/8	100%
Media Protection (MP)	30	11	19	11	0	100%	11	0	11/11	100%
Physical and Environmental Protection (PE)	59	29	30	29	0	100%	29	0	29/29	100%
Planning (PL)	17	11	6	11	0	100%	11	0	11/11	100%
Program Management (PM)	37	25	12	25	0	100%	25	0	25/25	100%
Personnel Security (PS)	18	17	1	17	0	100%	17	0	17/17	100%
Personally Identifiable Information Processing and Transparency (PT)	21	16	5	16	0	100%	16	0	16/16	100%
Risk Assessment (RA)	26	21	5	21	0	100%	21	0	21/21	100%
System and Services Acquisition (SA)	145	55	90	55	0	100%	55	0	55/55	100%
System and Communications Protection (SC)	162	31	131	31	0	100%	31	0	31/31	100%
System and Information Integrity (SI)	118	55	63	55	0	100%	55	0	55/55	100%
Supply chain Risk management(SR)	27	15	12	15	0	100%	15	0	15/15	100%
Total	1189	557	632	557	0	100%	557	0	557/557	100%

Risk Assessment Summary

Total number of Risks Identified - 2

High Risks – 0, Medium Risk – 0, Low Risks - 2

All the Risk details, remediation plan has been documented in the **Emmes FISMA - POAM** document.

Summary and Plan of Action and Milestones

All applicable controls under the NIST 800-53 release 5, Moderate baseline were evaluated. Minor findings addressed in POA&M.

Details of findings and Plan of actions documented in **Emmes FISMA - POAM** document.

Continuous Monitoring Strategy

Annually: Vulnerability scans and remediation of vulnerabilities, Full Security Controls Assessment, Security Awareness Training.

Quarterly: Configuration audits, patch validation

Monthly: SIEM alerts review

Authorization Decision

Authorization Type: ATO (Authority to Operate)

Date Issued: Jul 27, 2026

Expiration Date: Jul 26, 2027

Signed By:

Gobinda
Chandra Patra

Digitally signed by
Gobinda Chandra Patra
Date: 2026.08.03
16:38:57 +05'30'

Gobinda Chandra Patra, CISA, CISM, CRISC

Lead Assessor

ISIT Consultants Pvt. Ltd.