

FISMA Cybersecurity Certification and Authorization to Operate

To

CISO, The Emmes Company, LLC

Date: 05/02/2026

401 N. Washington Street Suite 700, Rockville, MARYLAND 21703, 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 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:

- Juniper Networks Internet router configured with redundant connectivity and border gateway protocol (BGP) routing.
- Palo Alto Networks next generation firewall
- Kemp Technologies Load Master virtual and hardware-based load balancers
- Juniper Networks redundant core Gb Ethernet switches
- Arista Networks 10 Gb Ethernet switches
- Hewlett Packard workgroup switches (connected via Gb fiber in the risers and redundant copper links)
- Duo Security multifactor authentication (for internal and VPN access)

Wireless Access

Emmes uses a separate "walled garden" for guests. The wireless network is configured with

Wi-Fi Protected Access 2 (WPA2) security encryption.

Remote Access

Emmes staff can also remotely access the corporate network via Palo Alto' Global Protect VPN or Unified Access Gateway (UAG) to the Virtual Desktop Interface (VDI) environment. Remote VPN or UAG user access requires the same multifactor authentication with the same token authentication as internal access. Additional security features that protect the corporate network while remote VPN or UAG users are connected include Cache Cleaner and Advanced Endpoint Protection.

Data Safety

Emmes systems are hosted on rack mounted redundant Hewlett Packard server hardware housed in Emmes' secure corporate data center. Redundant emergency power is provided

by Uninterruptible Power Supplies (UPS), rooftop natural gas emergency generator, and ground level building diesel generator. To improve redundancy, Emmes has deployed multiple Nimble storage area network (SAN) devices in the corporate data center and a remote facility. Emmes replicates production data and other essential services data to an off-site hosting facility located in Ashburn, VA.

Computing and Processing

Our Java 2 Platform, Enterprise Edition (J2EE) applications execute from Microsoft Windows 2012R2 application and web servers. Data are stored on Windows 2012R2 servers running Microsoft SQL Server 2014 64-bit software.

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 status have been described in the **FISMA Implementation -Assessment Work Book**.

Control Family	Total controls	Total controls (Applicable)	Document Review completed for the controls	Implementation Review completed for the controls
Access Control(AC)	45	38	38	38
Awareness and Training (AT)	7	6	6	6
Audit and Accountability (AU)	20	16	16	16
Assessment,Authorization and monitoring(CA)	11	10	10	10
Configuration Management (CM)	26	23	23	23
Contingency Planning (CP)	26	23	23	23
Identification and Authentication (IA)	26	20	20	20

Incident Response (IR)	14	13	13	13
Maintenance (MA)	10	9	9	9
Media Protection (MP)	8	7	7	7
Physical and Environmental Protection (PE)	24	18	18	18
Planning (PL)	9	8	8	8
Program Management (PM)	32	32	32	32
Personnel Security (PS)	9	9	9	9
Personally Identifiable Information Processing and Transparency (PT)	8	3	3	3
Risk Assessment (RA)	12	10	10	10
System and Services Acquisition (SA)	22	16	16	16
System and Communications Protection (SC)	54	24	24	24
System and Information Integrity (SI)	29	18	18	18
Supply chain Risk management(SR)	16	13	13	13
Total	408	316	316	316

Risk Assessment Summary

Total number of Risks Identified - 2

High Risks – 1, Low Risks - 1

All the Risk details, remediation plan has been documented in the **FedRAMP-POAM-Emmes Fisma** 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 **FedRAMP-POAM-Emmes Fisma** 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: May 31, 2026

Expiration Date: May 31, 2027

Gobinda
Chandra
Patra

Digitally signed by
Gobinda Chandra
Patra
Date: 2026.05.08
21:46:12 +05'30'

Signed By:

Gobinda Chandra Patra, CISA, CISM, CRISC
Lead Assessor

ISIT Consultants Pvt. Ltd.