Clinical and Laboratory Standards Institute®

October 2006

AUTO11-A

IT Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard

This document provides a framework for communication of IT security issues between the IVD system vendor and the healthcare organization.

A standard for global application developed through the Clinical and Laboratory Standards Institute consensus process.

Clinical and Laboratory Standards Institute

Setting the standard for quality in clinical laboratory testing around the world.

The Clinical and Laboratory Standards Institute (CLSI) is a not-for-profit membership organization that brings together the varied perspectives and expertise of the worldwide laboratory community for the advancement of a common cause: to foster excellence in laboratory medicine by developing and implementing clinical laboratory standards and guidelines that help laboratories fulfill their responsibilities with efficiency, effectiveness, and global applicability.

Consensus Process

Consensus—the substantial agreement by materially affected, competent, and interested parties—is core to the development of all CLSI documents. It does not always connote unanimous agreement, but does mean that the participants in the development of a consensus document have considered and resolved all relevant objections and accept the resulting agreement.

Commenting on Documents

CLSI documents undergo periodic evaluation and modification to keep pace with advancements in technologies, procedures, methods, and protocols affecting the laboratory or health care.

CLSI's consensus process depends on experts who volunteer to serve as contributing authors and/or as participants in the reviewing and commenting process. At the end of each comment period, the committee that developed the document is obligated to review all comments, respond in writing to all substantive comments, and revise the draft document as appropriate.

Comments on published CLSI documents are equally essential, and may be submitted by anyone, at any time, on any document. All comments are addressed according to the consensus process by a committee of experts.

Appeals Process

If it is believed that an objection has not been adequately addressed, the process for appeals is documented in the CLSI Standards Development Policies and Process document.

All comments and responses submitted on draft and published documents are retained on file at CLSI and are available upon request.

Get Involved—Volunteer!

Do you use CLSI documents in your workplace? Do you see room for improvement? Would you like to get involved in the revision process? Or maybe you see a need to develop a new document for an emerging technology? CLSI wants to hear from you. We are always looking for volunteers. By donating your time and talents to improve the standards that affect your own work, you will play an active role in improving public health across the globe.

For further information on committee participation or to submit comments, contact CLSI.

Clinical and Laboratory Standards Institute
950 West Valley Road, Suite 2500
Wayne, PA 19087 USA
P: 610.688.0100
F: 610.688.0700
www.clsi.org
standard@clsi.org

AUTO11-A
Vol. 26 No. 33
ISBN 1-56238-621-2
Replaces AUTO11-P
ISSN 0273-3099
Vol. 26 No. 5

IT Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard

Volume 26 Number 33

Andrzej J. Knafel, PhD
David Chou, MD
Bryan Crocker
Randy R. Davis
Eric Olson
Douglas O. Wood
Edwin O. Heierman, PhD

Abstract

Clinical and Laboratory Standards Institute document AUTO11-A—*IT Security of* In Vitro *Diagnostic Instruments and Software Systems; Approved Standard* specifies technical and operational requirements, as well as technical implementation procedures related to security of IVD systems (devices, analytical instruments, data management systems, etc.) installed at a healthcare organization. The intended users for this standard are vendors (IVD system manufacturers), users (e.g., laboratory personnel), and IT management of the healthcare organizations.

Clinical and Laboratory Standards Institute (CLSI). *IT Security of* In Vitro *Diagnostic Instruments and Software Systems; Approved Standard*. CLSI document AUTO11-A (ISBN 1-56238-621-2). Clinical and Laboratory Standards Institute, 950 West Valley Road, Suite 2500, Wayne, Pennsylvania 19087 USA, 2006.

CLINICAL AND
LABORATORY
STANDARDS
INSTITUTE®

Suggested Citation

CLSI. *IT Security of* In Vitro *Diagnostic Instruments and Software Systems; Approved Standard.* CLSI document AUTO11-A. Wayne, PA: Clinical and Laboratory Standards Institute; 2006.

Proposed Standard
January 2006

Approved Standard
October 2006

ISBN 1-56238-621-2
ISSN 0273-3099

Committee Membership

Area Committee on Automation and Informatics

Paul J. Mountain, MSc, MT(ASCP)
Chairholder
Flamborough, Ontario, Canada

David Chou, MD
Vice-Chairholder
Univ. of Washington Medical Center
Seattle, Washington

James V. Callaghan, MT(ASCP)
FDA Center for Devices and Radiological Health
Rockville, Maryland

Randy R. Davis
Dade Behring Inc.
Newark, Delaware

Charles D. Hawker, PhD, MBA, FACB
ARUP Laboratories, Inc.
Salt Lake City, Utah

Andrzej J. Knafel, PhD
Roche Instrument Center AG
Rotkreuz, Switzerland

Gary W. Kramer, PhD
National Institute of Standards and Technology
Gaithersburg, Maryland

Richard S. Seaberg, MT(ASCP)
North Shore University Hospital
Manhasset, New York

Advisors

Michael G. Bissell, MD, PhD, MPH
Ohio State University
Columbus, Ohio

Suzanne H. Butch, MA, MT(ASCP), SB
The University of Michigan
Ann Arbor, Michigan

Al DeStefano
Sysmex Corporation
Tucson, Arizona

Robert J. Dominici
Cholestech Corp.
Alamo, California

Jeffrey A. DuBois, PhD
NOVA Biomedical Corp.
Waltham, Massachusetts

Robert H. Engel, PhD
Engel Associates
Duxbury, Massachusetts

Arden W. Forrey, Jr., PhD, FACB
University of Washington
Seattle, Washington

Masayoshi Hayashi
Sysmex Corporation - Japan
Kobe, Japan

David A. Herold, MD, PhD
VA (San Diego) Medical Center
San Diego, California

Georg E. Hoffmann, MD
Trillium GmbH
Grafrath, Germany

Stephen Howlett
Beckman Coulter, Inc.
Miami, Florida

Brian Richard Jackson, MD
ARUP Laboratories
Salt Lake City, Utah

Rodney S. Markin, MD, PhD
Univ. of Nebraska Medical Center
Omaha, Nebraska

Michael D. McNeely, MD
MDS Metro Laboratory Services
Victoria, British Columbia, Canada

Richard A. McPherson, MD
Medical College of Virginia Hospital
Richmond, Virginia

David O'Bryan, PhD
Hibernia Consulting
Kennett Square, Pennsylvania

Paul J. Orsulak, PhD
VA North Texas Health Care System
Dallas, Texas

Jeff Quint, PhD
Beckman Coulter, Inc.
Brea, California

Hiroshi Sekiya
Olympus America Inc.
Irving, Texas

Russell H. Tomar, MD
John H. Stroger, Jr. Hospital of Cook County
Chicago, Illinois

Subcommittee on IT Security of IVD Instruments and Software Systems

Andrzej J. Knafel, PhD
Chairholder
Roche Instrument Center AG
Rotkreuz, Switzerland

Lynn Ballard
Beckman Coulter, Inc.
Fullerton, California

David Chou, MD
Univ. of Washington Medical Center
Seattle, Washington

Bryan Crocker
Capital Health
Halifax, Nova Scotia, Canada

Randy R. Davis
Dade Behring Inc.
Newark, Delaware

Eric Olson
DPC Instrument Systems Division
Flanders, New Jersey

Douglas O. Wood
FDA Center for Devices and Radiological Health
Rockville, Maryland

Advisors

Ed Heierman, PhD
Abbott Laboratories
Irving, Texas

Jeff Johnson, CISSP
Diagnostic Products Corporation
Los Angeles, California

Staff

Clinical and Laboratory Standards Institute
Wayne, Pennsylvania

John J. Zlockie, MBA
Vice President, Standards

David E. Sterry, MT(ASCP)
Staff Liaison

Donna M. Wilhelm
Editor

Melissa A. Lewis
Assistant Editor

Acknowledgement

CLSI and the Subcommittee on IT Security gratefully acknowledge Mr. Steven Lodin of Roche Diagnostics for his contributions to the development and completion of this document.

Contents

Foreword

The IT security requirements related to various laboratory systems (devices, analytical instruments, data management systems, etc.) are growing, mainly caused by 1) new international regulations applicable to healthcare organizations,[1] 2) an increase in the degree of integration of the IVD systems in the IT environment of healthcare institutions, and 3) attacks observed in healthcare organizations from a multitude of sources.

The real and potential threats for the systems and the organizations are also growing. Listed below are several examples illustrating how systems could be compromised by malicious software/people:

- changing processed/static data (e.g., test applications, calibration), resulting in the production of incorrect results;

- stealing patient electronic health records by querying the LIS/HIS from compromised laboratory systems (e.g., laboratory instrument with CLSI/NCCLS document LIS2—*Specification for Transferring Information Between Clinical Laboratory Instruments and Information Systems* [formerly ASTM E1394] query protocol);

- stealing or manipulating patient/sample results from the system;

- damaging the IVD system software, requiring reinstallation and resulting in down-time for the user and service costs for the vendor;

- misusing the IVD system as a means for compromising other systems in the healthcare organization's IT environment; and

- misusing the IVD system as a means for entering the vendor's corporate network.

This document provides a framework for communication of IT security issues between the IVD system vendor and the healthcare organization.

Key Words

Access control, authentication, authorization, encryption, hardening, IT security

IT Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard

1 Scope

This standard specifies technical and operational requirements, as well as technical implementation procedures related to IT security of IVD systems (devices, analytical instruments, data management systems, etc.) installed at a healthcare organization. This standard also provides guidance to meet and use existing technical standards for medical device IT security and recommendations for identifying the parties responsible for implementing these requirements.

The intended users for this standard are vendors (IVD system manufacturers), users (e.g., laboratory personnel), and IT management of healthcare organizations.

This standard is not intended for use as the final written policy for the healthcare organization. For example, local organizations will need to include in their own documentation the technical and process aspects of medical device security addressed by other standards organizations, such as ISO, IEEE, etc.

The suggested best practices contained in this document are based on the current state of technology at the time of publication. These best practices are distinguished from the requirements by a text box.

Some requirements, procedures, and guidelines specified by this standard may not be necessary or desired for IVD systems during clinical trials. The healthcare organization and vendor should clearly state in the corresponding contract how the standard would be applied during clinical trials.

2 Definitions

authentication – process of determining that an entity (someone or something) is the one claimed to be.

authorization – *In Automation and Informatics*, process of granting rights or access to systems, applications, or networks; **NOTE:** Authorization determines who is trusted for a given purpose.

device end user – end user in the HCO familiar with the medical device and its operation.

healthcare organization (HCO) – all components of an organization where the IVD is installed.

IT support – customer support staff familiar with computer hardware, operating system software, commercial off-the-shelf (COTS) software components, and networking environment.

validation – confirmation, through the provision of objective evidence, that requirements for a specific intended use or application have been fulfilled (ISO 9000).[2]

verification – confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (ISO 9000).[2]

2.1 Acronyms

BIOS	basic input/output system
COTS	commercial off-the-shelf
CRC	cyclical redundancy check
DBMS	database management system