

Supporting
DHS HIPAA
Final Security
Rules



Health Insurance Portability and Accountability Act
Enterprise Compliance Auditing & Reporting
ECAR™ for HIPAA
Technical Product Overview Whitepaper

ECAR™ for HIPAA Product Abstract

ECC Enterprise Compliance Auditing and Reporting (ECAR) is a framework for tracking IT security-related events against regulatory requirements and recommended best practices. The Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191) Final Security Rules are defined in the Federal Registry 45 CFR Part 160, 162 and 164. The Security Rules suggests "what" needs to be enforced. The National Institute of Science and Technology (NIST), the organization responsible of interpreting "how" to implement sound computing practices, has set forth specific recommendations for agencies impacted by HIPAA in NIST Special Publication 800-66. That document establishes the standard recommendation for the Federal Information Security Management Act (FISMA) as a benchmark as defined in NIST Special Publication 800-53.

The ECC Enterprise Compliance Auditing and Reporting (ECAR) system maps over 175 Microsoft Windows IT security events to the technical and operational specifications defined by NIST SP 800-53. Utilizing Microsoft Operations Manager (MOM) server, events are tracked and a variety of auditing reports are generated.

ECAR™ HIPAA FEATURES

Over 175 Windows Server IT Security Events
Events mapped to NIST Standards Recommended Controls

Access Control Management

Audit and Accountability

Contingency Planning

Identification and Authentication

System and Information Integrity

System and Communication Protection

Collective and Individual Event Views

Over 75 Management Audit Reports and Trails

Fully Customizable and Extensible

ECC Enterprise Compliance Auditing and Reporting (ECAR) Health Insurance Portability & Accountability Act (HIPAA) Windows IT Security Controls Using Microsoft Operations Manager

INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (also known as the Kennedy - Kassebaum Bill) affects all organizations throughout the healthcare industry: Patients, Healthcare Providers, Third Party Service Providers, Insurance Payers and Employers. The bill was intended to simplify the portability of healthcare coverage for people changing employers and streamline the processing of health related data. Title 45 of the Code of Federal Regulations imposes specific requirements for privacy and security of Protected Health Information (PHI).

ECC Enterprise Compliance Auditing and Reporting (ECAR) is a framework for tracking IT security-related events against regulatory requirements and recommended best practices. The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191) Final Security Rules are defined in the Federal Registry 45 CFR Part 160, 162 and 164. The rules are divided into primary categories administrative, physical and technical safeguards. While many of the rules are procedural in nature, a very significant number are quantifiable through the analysis and reporting of IT computing events.

The HIPAA Security Rules suggest "what" needs to be enforced. The National Institute of Science and Technology (NIST), the organization responsible of interpreting "how" to implement sound computing practices, has set forth specific recommendations for agencies impacted by HIPAA in NIST Special Publication 800-66. That document concludes that the HIPAA Security Rules are similar to those of the Federal Information Security Management Act (FISMA) that was enacted to protect critical data infrastructures and promote best practice standards. Whether the impacted party is government or private, a sound compliance plan would embrace both the Security Rules and NIST

recommendations associated with FISMA. As it relates to FISMA, NIST Special Publication 800-53 seeks to assist government agencies and commercial contracting organizations to understand and achieve compliance. ECC Enterprise Compliance Auditing and Reporting (ECC ECAR) for HIPAA aligns the HIPAA Security Rules to the NIST recommendations for FISMA and tracks Windows Server IT security events to produce consistent and repeatable audits and reports.

The ECC Enterprise Compliance Auditing and Reporting (ECAR) solution for maps over 175 Microsoft Windows security events to key technical and operational NIST Special Publication 800-53 and 800-66 guidelines. The framework for compliance on FISMA is used in order to align recommended practices to the HIPAA Security Rules. ECAR leverages information gathered and organized using Microsoft Operations Manager (MOM) monitoring and event collection capabilities. The IT administrator can examine these events from a variety of views and output reports based on such criteria as time periods, computer groups, users, domains and event IDs.

ECC ECAR provides three primary interfaces. The Administrative Console provides authorized users the ability to enable/disable rules, rules groups and event, plus edit knowledgebase information. The Operator Console permits the viewing of recent events and the establishment of alerts and state views. ECC ECAR management reports are web based and available through SQL Server Reporting Services. Users should refer to the ECC ECAR documentation on specific configuration questions. It should be noted that the defined recommendations in the NIST Special Publications utilized as the standards base sometimes do not map precisely to all Windows IT security controls. Therefore, ECC ECAR provides the framework for

further refining the mapping process to individual organizational situations. The Knowledgebase provides NIST based information for each control family and sub-family to assist in further analysis and interpretation of compliance.

A major challenge for IT professionals is to measure HIPAA compliance with repeatable audits and processes that produce meaningful and accurate reports. The Microsoft Windows server platform provides information on individual security events generated as accounts access electronic data and perform activities that can be manually reviewed via log files. However, this process is time consuming and ad hoc. The ECC Enterprise Compliance Auditing and Reporting solution for HIPAA maps over 175 Microsoft Windows security events to key technical and operational NIST SP800-53 guidelines. ECAR leverages information gathered and organized using the Microsoft Operations Manager (MOM). The IT administrator can examine these events from a variety of views and output reports based on such criteria as time periods, computer groups, users, domains and event ID.

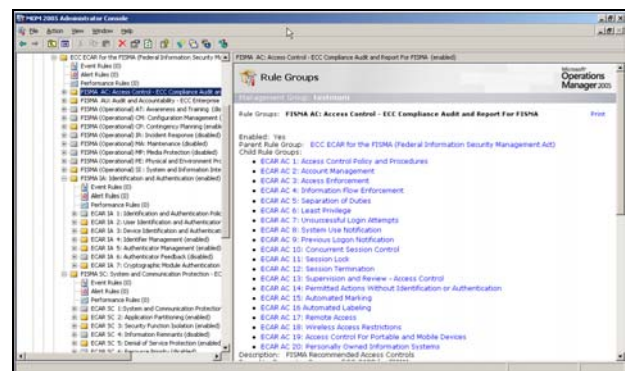
BACKGROUND: SECURITY CONTROLS

The selection and employment of appropriate security controls for an information system is fundamental. NIST breaks down security controls into three safeguard families: management, operational, and technical. The purpose is to protect the confidentiality, integrity, and availability of systems and information. While certain NIST guidelines are procedural, many of the technical and operational recommendations are IT event driven and lend themselves to ECAR's automated compliance auditing and reporting.

ECAR is designed to assist organizations subject to HIPAA to collect and report on Microsoft Windows server platform IT events. The goal is to facilitate a more consistent, comparable, and repeatable approach that is consistent with recommended minimum security controls for information systems as categorized by Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Through the use of the MOM infrastructure, ECAR promotes a dynamic, extensible catalog of security controls for information systems.

WHO BENEFITS FROM ECAR

ECAR is intended to serve a diverse audience of information system and security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and project managers); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Public company financial officers concerned with implementing appropriate controls relative to information security systems can also benefit.



ECAR FOR HIPAA ADMINISTRATIVE CONSOLE

SECURITY CONTROL BASELINES

Organizations must employ security controls to meet security requirements defined by laws, executive orders, directives, policies, or regulations (e.g., Federal Information Security Management Act, OMB Circular A-130, Appendix III) 15. The challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would comply with the stated security requirements. Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task.

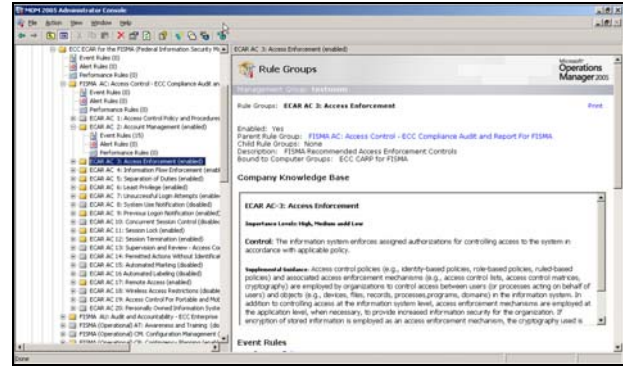
TAILORING THE INITIAL BASELINE

After the appropriate security controls are selected, three additional steps are needed to tailor the baseline for a specific organizational information system: (i) the application of *scoping guidance* to the initial baseline; (ii) the specification of *organization-defined parameters* in the security controls, where appropriate; and (iii) the specification of *compensating security controls*, if needed. By default, ECC ECAR provides the initial framework, reports, and regulatory knowledge. However, organizational line tuning will still be required. To ensure a cost-effective, risk-based approach to achieving adequate information security organization-wide, tailoring activities should be coordinated with appropriate officials (e.g., senior agency information security officers, authorizing officials). The resulting set of security controls should be documented in the security plan for the information system and integrated with the ECAR system.

REVISIONS AND EXTENSIONS

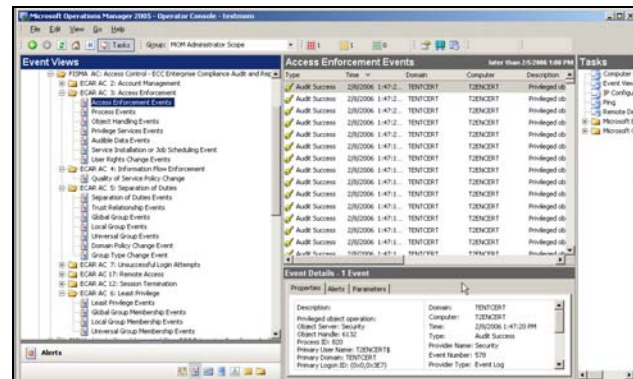
The set of security controls listed in the control catalog and the ECAR associated Windows server platform IT events represents a baseline of safeguards and countermeasures for information systems. ECAR is designed to facilitate revision and extensions to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within organizations; and (iii) new security technologies that may be available. The events and controls populating the various families will change over time, as operating systems and applications are added and updated. ECAR is designed to also accommodate governmental regulatory additions, deletions, or modifications to the catalog of security controls.

NIST has defined minimum security controls as having the low, moderate, and high baseline levels of impact. It is anticipated that these will also change over time as well. Therefore, ECAR permits the movement of IT security events between the recommended controls. ECAR together with MOM facilitates dynamic and flexible technical auditing and reporting on a rigorous set of security controls in a cost-effective manner.



ECAR HIPAA/NIST SOURCED KNOWLEDGE BASE

Security controls containing configurable parameters give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, directives, executive orders, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk. ECAR permits organizations to map IT security events to a variety of views in order to facilitate granular and targeted security audits.



ECAR EVENT VIEWS

ECAR SUPPORTED SECURITY CONTROLS

By default, ECAR supports the HIPAA Security Rules utilizing the following NIST SP800-53 security controls framework. The ECAR infrastructure also allows the user to add, delete and modify the default events that are associated with other recommended controls.

NIST FAMILY: ACCESS CONTROL
CLASS: TECHNICAL

HIPAA SECURITY RULE - ACCESS: The HIPAA Security Rules includes explicit requirements on access management and control. Under its Administrative Safeguards, Section 164.308(a)(4)(1) requires organizations to establish policies and procedure relating to authorized use of electronic protected health information. Section 164.308(a)(5) establishes guidance relative to awareness, training, and response. The HIPAA Security Rules Technical Safeguards provide requirements that lend themselves to event auditing and reporting. Section 164.312(a)(1) defines access control technical implementation that specifically states that organizations must maintain electronic health information to allow access only to those persons or software applications that have been granted access rights as specified in 164.308(a)(4). [Source NIST Special Publication 800-66] ECC ECAR takes into account the broad basis of these requirements and has applied the standards framework set forth in NIST Special Publication 800-53 to gather related IT security events for the purpose of auditing and reporting.

AC-2 ACCOUNT MANAGEMENT - The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

AC-3 ACCESS ENFORCEMENT - The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

AC-4 INFORMATION FLOW ENFORCEMENT - The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

AC-5 SEPARATION OF DUTIES - The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

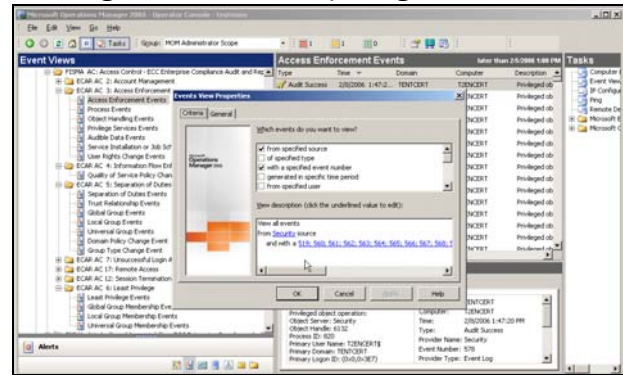
AC-6 LEAST PRIVILEGE - The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS - The information system enforces a limit on consecutive invalid access attempts by a user during a time period.

AC-12 SESSION TERMINATION - The information system automatically terminates a session.

AC-17 REMOTE ACCESS - The organization documents, monitors, and controls all methods of remote access

(e.g., dial-up, Internet) to the information system including remote access for privileged functions.



ECAR/MOM Custom Event Views

HIPAA SECURITY RULE-AUDITING: The HIPAA Security Rules includes explicit requirements on auditing IT security relating to access to non public information. Under its Administrative Safeguards, Section 164.308(a)(1)(a)(D) requires organizations to establish policies and procedure regularly review records of information activity such as audit logs, access reports and security incident tracking reports. The HIPAA Security Rules Technical Safeguards provide requirements that lend themselves to event auditing and reporting. Specifically, Section 164.312(b) defines audit controls technical implementation requiring organizations record and examines activities that contain or use electronic protected health information. [Source NIST Special Publication 800-66] ECC ECAR takes into account the broad basis of these requirements and has applied the standards framework set forth in NIST Special Publication 800-53 to gather related IT security events for the purpose of auditing and reporting.

NIST FAMILY: AUDIT AND ACCOUNTABILITY CLASS: TECHNICAL

AU-3 CONTENT OF AUDIT RECORDS - The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.

AU-4 AUDIT STORAGE CAPACITY - The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

AU-5 AUDIT PROCESSING - In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING - The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual

activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

AU-8 TIME STAMPS - The information system provides time stamps for use in audit record generation.



ECAR DEFAULT REPORTS

HIPAA SECURITY RULE CONTINGENCY PLANNING:

The HIPAA Security Rules includes explicit requirements for contingency planning. Under its Administrative Safeguards, Section 164.308(a)(7)(i) requires organizations to establish policies and procedure for responding to an emergency or other occurrence that damages systems containing protected electronic health information. Section 164.308(a)(7)(ii)(A) stipulates the requirement for Data Backup and subsection (B) establishes guidance for a Disaster Recovery Plan. [Source NIST Special Publication 800-66] NIST Special Publication 800-53 sets forth standards recommendations for Contingency Planning under sections CP 9 Information Backup and CP 10 Information Recovery, respectively. ECC ECAR takes into account the broad basis of these requirements and has applied the standards framework set forth in NIST Special Publication 8000-53 to gather related IT security events for the purpose of auditing and reporting.

NIST FAMILY: CONTINGENCY PLANNING CLASS: OPERATIONAL

CP-9 INFORMATION SYSTEM BACKUP - The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and stores backup information at an appropriately secured location.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION - The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

HIPAA SECURITY RULE: AUTHENTICATION

The HIPAA Security Rules includes explicit requirements for identification and authentication of users of systems containing protected electronic health information. Under its Administrative Safeguards, Section 164.308(a)(8)(A-C) requires organizations to establish policies and procedures for authorization and/or supervision, clearance, and appropriate termination of workforce members. Further, Section 164.308(a)(4)(ii)(B) requires the implementation of policies and procedures for granting access to protected information through access to workstations, transactions, program, process or other mechanisms. As part of the HIPAA Security Rule Technical Safeguard, 164.312(d) dictates implementation of process to verify that a person or entity seeking access to protected data is the one claimed. Additionally, 163.312(e)(2) mandates integrity controls and encryption requirements. [Source NIST Special Publication 800-66] NIST Special Publication 800-53 sets forth standards recommendations for Identification and Authentication. ECC ECAR takes into account the broad basis of these requirements and has applied the standards framework set forth in NIST Special Publication 8000-53 to gather related IT security events for the purpose of auditing and reporting.

NIST FAMILY: IDENTIFICATION AND AUTHENTICATION CLASS: TECHNICAL

IA-2 USER IDENTIFICATION AND AUTHENTICATION - The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

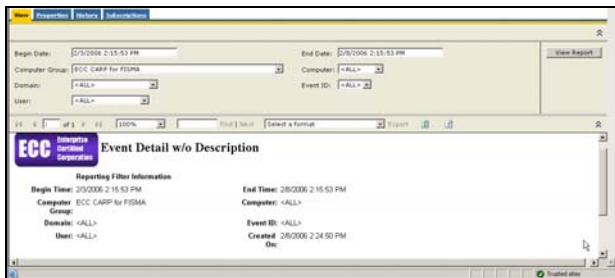
IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION - The information system identifies and authenticates specific devices before establishing a connection.

IA-4 IDENTIFIER MANAGEMENT - The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.

IA-5 AUTHENTICATOR MANAGEMENT - The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or

damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION -For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.



ECAR REPORT SAMPLE

HIPAA SECURITY RULE SYSTEM AND COMMUNICATION PROTECTION

The HIPAA Security Rules includes explicit requirements for system and communications protection of computers containing protected electronic health information. Under its Administrative Safeguards, Section 164.308 requires organizations to establish policies and procedures for areas involving system and communication protection. As part of the HIPAA Security Rule Technical Safeguard, 164.312(c)(1) dictates implementation of process to protect subject health information from improper alterations and destruction. Section 164.312(e)(1) requires implementation of technical security measures to guard against unauthorized access to protected health information that is being transmitted over a communications network. Additionally, 164.312(e)(2) mandates integrity controls and encryption requirements.

NIST FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION CLASS: TECHNICAL

SC-2 APPLICATION PARTITIONING - The information system separates user functionality (including user interface services) from information system management functionality.

SC-3 SECURITY FUNCTION ISOLATION - The information system isolates security functions from non-security functions.

SC-5 DENIAL OF SERVICE PROTECTION - The information system protects against or limits the effects of the following types of denial of service attacks.

SC-8 TRANSMISSION INTEGRITY - The information system protects the integrity of transmitted information

SC-9 TRANSMISSION CONFIDENTIALITY - The information system protects the confidentiality of transmitted information.

SC-10 NETWORK DISCONNECT - The information system terminates a network connection at the end of a session or after inactivity

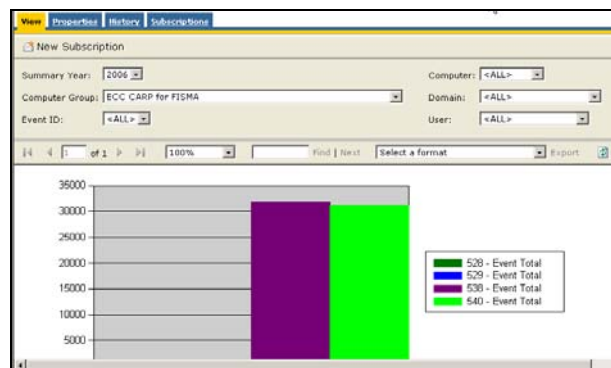
SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT - The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

HIPAA SECURITY RULE SYSTEM INTEGRITY

The HIPAA Security Rules includes explicit requirements for maintenance of system integrity of computers containing protected electronic health information. Under its Administrative Safeguards, Section 164.308 requires organizations to establish policies and procedures for areas involving system integrity. As part of the HIPAA Security Rule Technical Safeguard, 164.312(c)(1) dictates implementation of process to protect subject health information from improper alterations and destruction. Additionally, 164.312(e)(2) mandates integrity controls and encryption requirements. [Source NIST Special Publication 800-66]

NIST FAMILY: SYSTEM AND INFORMATION INTEGRITY CLASS: OPERATIONAL

SI-6 SECURITY FUNCTIONALITY VERIFICATION - The information system verifies the correct operation of security functions): upon system startup and restart.



ECAR Sample Graphical Report

ECAR, MICROSOFT AND NIST

The Microsoft Windows Server platform provides IT professionals about 200 security events that can be used for regulatory compliance auditing and reporting. The Microsoft Operation Manager facilitates the collection of events and manages the ability to customize views and reports. Building on this foundation ECC developed ECAR around NIST recommendations as a compliance auditing and reporting environment.

ECAR is used to identify security compliance issues for both assessment and mitigation purposes. As the proactive monitoring capacity of to react and adjust its risk posture.

ECC want to acknowledge the ground breaking efforts of NIST and in particular the team responsible for SP800-53.

SYSTEM REQUIREMENTS:

Microsoft Windows 2003 Server
Microsoft Operations Manager
SQL Server with Reporting Services



ABOUT ECC

Enterprise Certified Corporation is the publisher of risk management solutions focused on IT security regulatory compliance. The firm is comprised of world-class IT security and Windows experts including the authors of best selling books like the *Ultimate Windows 2003 Server System Administrator's Guide*. In addition, Microsoft has honored principals with four Most Value Professional (MVP) awards in the field of Windows Security. The company participates in many industry and trade organizations such as the Sarbanes Oxley executive roundtable and the Department of Homeland Security/FBI's Infragard.

For more information about ECC and its other solutions go to:

<http://www.enterprisecertified.com>

1-800-701-2785 Sales #4 Service #5

ECAR™ is a trademark of Enterprise Certified Corporation ALL RIGHTS RESERVED WORLD WIDE

ECC Enterprise Compliance Auditing and Reporting (ECAR)
Health Insurance Portability & Accountability Act (HIPAA)
Windows IT Security Controls Using Microsoft Operations Manager