

ECC Enterprise Compliance Auditing & Reporting for the Gramm Leach Bliley Act

Windows Server Platform
Microsoft Operations Manager
ECAR™ Technical Reference

Copyright: © Enterprise Certified Corporation 2000-2006 ALL RIGHTS RESERVED

Applies To: Microsoft® Operations Manager 2005, Microsoft® SQL Reporting Services and Microsoft© Windows Server Platform

Document Version: ECC ECAR™ 4.1

Acknowledgement: FISMA recommendations derived directly from the National Institute of Science and Technology NIST Special Publication 800-53 and 800-66. We also acknowledge the contributions of the Federal Financial Institution Examination Council related publications and final rules.



Table of Contents

CHAPTER 1: OVERVIEW	3
INTRODUCTION	3
BACKGROUND: SECURITY CONTROLS	4
WHO BENEFITS FROM ECAR	4
SECURITY CONTROL BASELINES	5
TAILORING THE INITIAL BASELINE	5
REVISIONS AND EXTENSIONS	5
TECHNOLOGY OVERVIEW	6
System Recommended Requirements	7
INSTALLATION	9
Basic Configuration	10
Basic Installation and Configuration of ECAR	10
CHAPTER TWO: Administrative and Operating Console Events.....	13
Understanding Event Interface	13
Administrative Console View	13
Operator Console Interface	14
DEFAULT TECHNICAL EVENTS	15
AC: ACCESS CONTROLS.....	15
AU: AUDIT AND ACCOUNTABILITY.....	29
CP: Contingency Planning	35
IA: Identification and Authentication Print.....	37
SC: System and Communication Protection	43
SI: System and Information Integrity	54
EVENT VIEWS	55
AC: Access Control	55
AU: Audit and Accountability	56
(Operational) CP: Contingency Planning.....	57
IA: Identification and Authentication	57
(Operational) SI: System and Information Integrity	58
SC: System and Communication Protection	58
CHAPTER THREE: ECAR REPORTS	60
Standard ECAR Reports.....	60
APPENDIX A: IT Security Events	65
APPENDIX B: REFERENCES.....	69
APPENDIX C: ACRONYMS	72

CHAPTER 1: OVERVIEW

INTRODUCTION

The Gramm Leach Bliley Act (GLBA) requires financial institutions to establish consistent and comprehensive controls over non-public information. The Federal Financial Institutions Examination Council's (FFIEC) is an interagency body empowered to prescribe uniform principles, standards, and reports for the examinations by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions. They have published a number of related guidelines including Tier I and Tier II examination objectives and procedures. While extremely well described, these FFIEC guidelines are still subject to interpretation.

The FFIEC and its partner agencies are also subject to the Federal Information Security Management Act. A logical assumption regarding IT security controls is to baseline GLBA compliance against the same regulations the FFIEC must abide.

The Federal Information Security Management Act (FISMA) was enacted to protect critical data infrastructures and promote best practice standards. The National Institute of Science and Technology (NIST) assumed responsibility for interpreting the legislation and translating the goals into understandable and achievable guidelines. As it relates to FISMA, NIST Special Publication 800-53 seeks to assist government agencies and commercial contracting organizations to understand and achieve compliance. [NIST SP 800-59 and related documents identifies issues impacting national security systems.]

Failure to comply with GLBA may result in very significant administrative sanctions against public companies. Beyond punitive actions, the NIST recommendations should be regarded as positive IT security guidance. In developing ECAR, Enterprise Certified Corporation embraced the baseline NIST/FFIEC recommendations as solidly grounded and consistent the best of international IT security best practice standards.

The FFIEC has published guidelines for examiners of financial institution compliance. Tier I Objectives provide eight general purpose requirements:

1. Determine the appropriate scope for the examination;
2. Determine the complexity of the institution's information security environment;
3. Determine the adequacy of the risk assessment process;
4. Evaluate the adequacy of security policies relative to the risk to the institution;
5. Evaluate the security-related controls embedded in vendor management;
6. Determine the adequacy of security testing;
7. Evaluate the effectiveness of enterprise-wide security administration;
8. Discuss corrective action and communicate findings.

Tier I Examination Objectives are reasonably but highly subjective. The Tier II Objectives and Procedures are significantly more directed at specific IT practices. While still process oriented, when coupled with NIST SP 800-53 recommendations, it is possible to quantify many areas of IT security compliance.

A major challenge for IT professionals is to measure GLBA 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 SOX 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 SOX 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 SOX 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 federal 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). Commercial companies producing information technology products and systems, creating

information security-related technologies, and providing information security services can also benefit.

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.

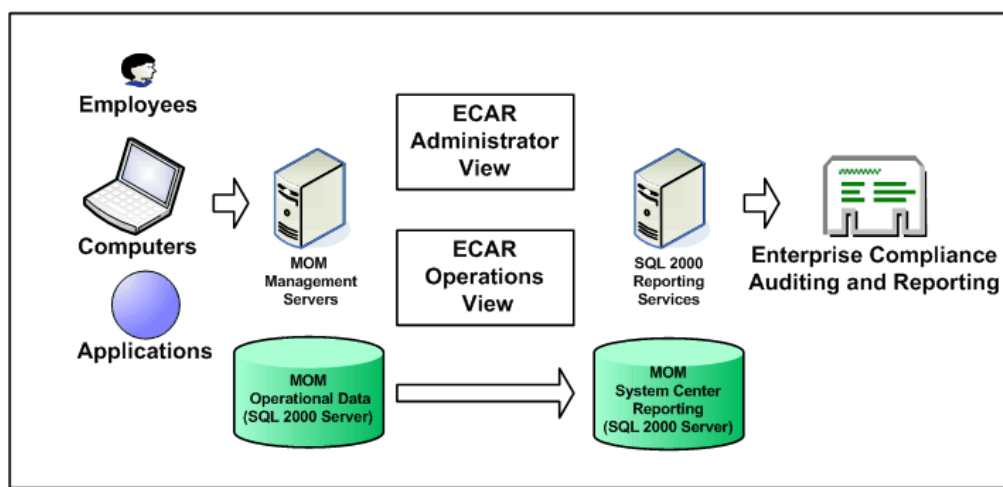
NIST has defined minimum security controls as having the low, moderate, and high baseline levels of impact. It is anticipated that these will also change over time as well. Therefore, ECAR permits the movement of IT security events between the recommended controls. ECAR, together with MOM, facilitates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

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.

TECHNOLOGY OVERVIEW

Enterprise Compliance Auditing and Reporting monitors and collects events generated by employee access to information systems. As employees access electronic information and perform activities for their job functions, ECAR monitors, audits, and reports control activity in order to validate corporate compliance with regulatory governance. IT professionals must first configure the corporation's internal IT structure to log activity pertinent to regulatory requirements. ECAR provides a framework to organize and guide control selection for reporting on control activity as it applies to the regulation.

The ECAR Administrator View organizes controls in regards to a particular regulation. ECAR supports GLBA, FISMA, HIPAA and SOX respectively. Using the MOM Administrator's console the IT Administrator can evaluate and select controls for monitoring. Once monitoring has been configured, real time event collection and monitoring can be observed with the ECAR operation views in the MOM Operations console. ECAR views are targeted at specific regulatory control areas, and focus the operator to pertinent control categories.



Event and monitoring data is centralized in the MOM Reporting Server for longer term auditing and reporting. ECAR reporting maps and categorizes collected data to the control areas and format required by the regulation. Using ECAR reports in conjunction with SQL 2000 Reporting Services data may be sorted by Domain, Computer, Date, Control area, or User. Reports may be filtered and selected for specific audit requirements by external agencies or for internal compliance purposes. Reports can be exported to a variety of file formats including PDF, XML, and Excel formats.

System Recommended Requirements

ECAR utilizes standard Microsoft server platform components. The key components to implement the ECAR Compliance Auditing system include:

- ECC Compliance Auditing & Reporting component files
- Microsoft Operations Manager 2005
- SQL Server 2000
- SQL 2000 Reporting Services

It is recommended that the user reference the server installation instructions provided by Microsoft Corporation. A typical software configuration for an individual server requirement includes the above components.

All of these components can be loaded onto one server. Server roles for large installations maybe distributed on multiple servers. A single server with the following software configuration will support a single MOM 2005 Management Server, Admin and Operational views, Reporting Services and host the MOM 2005 operational and reporting databases:

Single ECAR Server – Single server with all monitoring and reporting roles.

1. Windows Server 2003 Standard Edition or Enterprise Edition
2. Service pack 1
3. SQL Server
4. From the Services snap-in ensure the SQL Server Agent is configured to start automatically
5. SQL Server pack 3a
6. Configure your server as an application server using the Configure Your Server administrative tool - enable ASP.NET. (NOTE: if you plan to perform custom report development then install Visual Studio 2003. Otherwise it is NOT required.)
7. SQL Reporting services – User the Enterprise Edition for production environments
8. SP1
9. MOM 2005

10. MOM 2005 Reporting

The following roles maybe be distributed across different servers in the following configurations:

Microsoft Operation Manager (MOM) 2005 Management Server

1. Windows Server 2003 Standard Edition
2. Service pack 1
3. Microsoft Data Access Components (MDAC) version 2.8.1022.0 or later
4. Microsoft .NET Framework version 1.1
5. MOM 2005

MOM 2005 Administrator Console and Operator Console

1. Microsoft .NET Framework version 1.1
2. IE 6 SP1 or IE 5.5 SP2
3. MOM 2005 Admin and Operational Console

MOM 2005 Reporting and SQL Server

1. Windows Server 2003 Standard Edition
2. Service pack 1
3. WMI Windows Installer Provider and ASP.NET Windows components (This can be accomplished by loading Microsoft Visual Studio® .NET 2003
4. SQL Server
5. SQL Server pack 3a
6. SQL Reporting services
7. SP1
8. MOM 2005 Reporting

Please see SUPCONFIG.HTM on MOM CD for further information.

System Requirements:

Install all MOM components on One Computer baseline requirements:

Pentium-compatible 550 MHz dual-processor or higher

- 1 GB of RAM (4 GB or higher recommended)
- 1 GB of available hard disk space (For Reporting, much more drive space might be needed)
- CD-ROM drive (if installing MOM from this computer)
- Network adapter

To use the MOM 2005 Management Server, the baseline system includes:

- Pentium-compatible 550 MHz processor or higher (dual Pentium-compatible 450 MHz processors or higher recommended)
- 512 MB of RAM (1 GB or higher recommended)
- 5 GB of available hard disk space
- CD-ROM drive (if installing MOM from this computer)
- Network adapter

To Use the MOM 2005 Database, the baseline system includes:

- Pentium-compatible 550 MHz processor or higher (dual Pentium-compatible 450 MHz processors or higher recommended)
- 512 MB of RAM (1 GB or higher recommended)
- 5 GB of available hard disk space
- Network adapter

To Use the MOM 2005 Reporting Server, the baseline system includes:

- Pentium-compatible 550 MHz processor or higher (dual Pentium-compatible 450 MHz processors or higher recommended)
- 512 MB of RAM (1 GB or higher recommended)
- 200 GB of available hard disk space
- Network adapter

INSTALLATION

ECAR configures Microsoft Operations Manager (MOM) 2005 to collect events required for regulatory governance. MOM's primary configuration involves a management server collecting information from various computers within the IT infrastructure. Please refer to MOM installation and instruction guides in regards to MOM server and agent deployment and configuration. It is assumed that before performing ECAR management and reporting installation, that MOM 2005 has been installed and configured according to Microsoft guidance.

In general we suggest that all systems are agent monitored for a number of reasons. First it ensures compatibility with the client side .dll and provider interfaces as the managed server will be updated with current agent code. Second, it allows the MOM server to maximize the number of systems it can manage as a MOM management server should only monitor a maximum of 10 agentless systems, while it can handle around 2000 agent monitored servers. Lastly, agent managed systems have control over the application provider source so that future enhancements to ECAR can easily be added to track additional control areas.

Basic Configuration

The MOM database components of concern are the OnePoint database and the SystemCenterReporting database. The OnePoint database contains configuration and current operational information and is associated with each MOM Management server. The configuration information includes event rules and view information established by management packs installed on the server, as well as service and computer attribute settings. The Operations data is information collected from event rules, alerts, and scripts that are configured on the Management server. As information is collected from the event logs and providers on managed systems the data is consolidated into the OnePoint database.

Before ECAR can be installed onto MOM Management Server, MOM reporting must be installed. This creates the SystemCenterReporting database that has a default size of 1000 MB. The reporting database may be installed on a different server than the MOM Management server for optimal performance. Please refer to MOM documentation for guidance.

Operational data from the OnePoint database is periodically moved to the SystemCenterReporting database for long term storage and obviously reporting purposes. A scheduled task with a default time of 1:00AM performs this task daily. For testing purposes and to update reporting with up to the day or hour data, this task maybe manually instigated with the following steps on the MOM Reporting server:

1. Select the **Start → Control Panel → Scheduled Tasks**
2. Right click the **SystemCenterDTSPackageTask** and select **Run**.

This will transfer data from the OnePoint database to the SystemCenterReporting database.

Basic Installation and Configuration of ECAR

Install ECAR Rules, Views and Reports:

1. Open the MOM Administrator Console and right click on the Management Packs Node.
2. Select Import/Export Management Pack... and follow the wizard instructions for installing both the ECAR.akm management pack and the ECAR.xml reporting pack.
3. Once you have installed the ECAR management AKM add systems to the ECAR Computer groups for monitoring and event collection.

Configure ECAR Reporting:

1. Configure the SQL 2000 Reporting Server by going to the root reporting directory found by using a browser and entering the URL: <http://localhost/reports>.
2. Select the Microsoft Operations Manager Reporting directory. Then select the Enterprise Compliance Audit Report directory and then select the ECCDS data source.
3. Configure the data source to target the MOM management server containing the SystemCenterReporting database. This can be done using Windows Authentication, storing credentials on the report server, or using credentials of the user as they access the report server. Window's Authentication is the preferred method here, but please refer to SQL 2000 Reporting Services documentation for further information.

Configure ECAR Computer Groups

1. From the MOM Administrative Console, open **Management Packs** → Open Computer Groups → right click **ECC ECAR** → select Properties
2. Select the **Search for Computers Tab** → Select **Search for Computers by the Criteria specified below** → initiate the computer search [**NOTE:** The administrator should select only those groups of computers that will be subject to the regulatory audit. It is recommended that the administrator pre-define the systems and/or domains prior to initiating the search.]
3. Select the **Included Computers** tab → from the list, Add those specific systems to be included in the regulatory audits
4. (Optional) Select the **Excluded Computers** tab → from the list, Add those specific systems to excluded in the regulatory audits

[**NOTE:** All systems included in this group will be audited in accordance with all Enabled Rules Groups. In some instances, an administrator may want to audit a system or a group of systems based on a selective set of Rules Groups. For example, a special monitoring of Domain Controller for Access Control Rules may be desired. To create a sub-audit computer group, right click on **Computer Groups** and select **Create a Computer Group**. Use the wizard to complete the Computer Group creation. To associate the new Computer Group with a Rule Group, open the **Management Packs** node and find the **Rules Groups** node. Open the **ECC ECAR Rules Group** and drill down to the desired Rules Group. Right click on the desired ECC ECAR Rules Group, select **Associate with Computer Group**, select the **Add** button, select the new Computer Group, select **OK** to complete the activity. Repeat this ECC ECAR Rules Group association for each rule to be included with the new Computer Group sub

audit. All sub-Rules Groups will inherit the association of the Parent Rules Group. Therefore, in the example of Access Control, it is only necessary to associate the Parent ECC ECAR Access Control to automatically associate all the Enabled sub-Rules Groups with the Computer Group.]

Configure Events and Event Rule Groups – Enable/Disable

[**NOTE:** Not all ECAR Event Groups are enabled by default. In most cases where the Event Rules are disabled, the rule in question is regarded as generally procedural. However, the administrator may enable a rules group by selecting its Properties and checking the Enabled button located by the General tab. Security Events can then be copied from other ECC ECAR rules groups.]

[**NOTE:** All Event Rules found in Enable Rules Groups are Enabled by default. Due to the volume of information that will be gathered by all of these Event Rules, the administrator may want to Disable some of the Event Rules on a periodic basis. This is accomplished by right clicking on the Event Rule, select Properties, uncheck the box entitled This Rule is Enabled found on the General Tab, confirm by pressing OK. If an Event Rules Group is Disabled, all Event Rules found in that group are automatically Disabled.]

CHAPTER TWO: Administrative and Operating Console Events

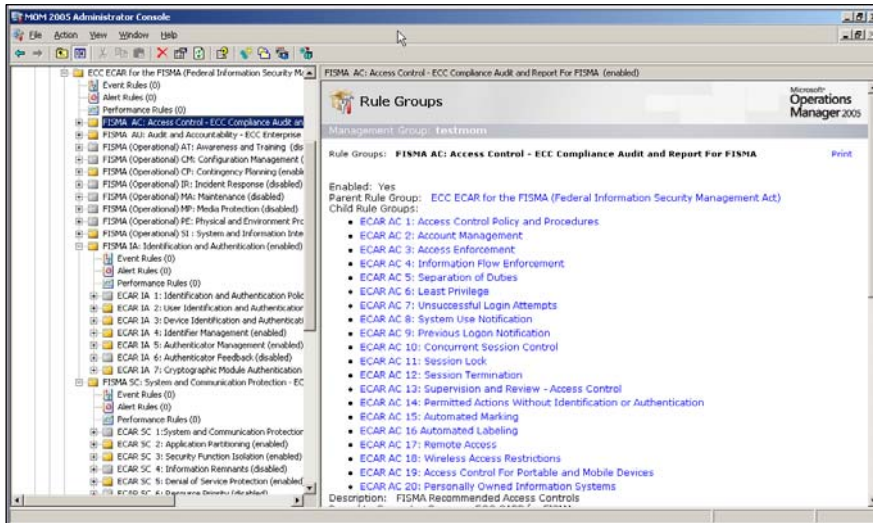
Understanding Event Interface

ECC ECAR breaks down the tracking of security events in accordance with the mapping provided by NIST Special Publication 800-53. ECC ECAR organizes the recommendations of NIST SP 800-53 into Rules Groups using the same naming conventions. Knowledgebase information relative to each Rules Group is derived directly from NIST SP 800-53 in order to provide the administrator greater clarity as to why a particular audit function is being performed.

The MOM Administrative and Operator Console provide different perspectives of the events and rules group for ECC ECAR.

Administrative Console View

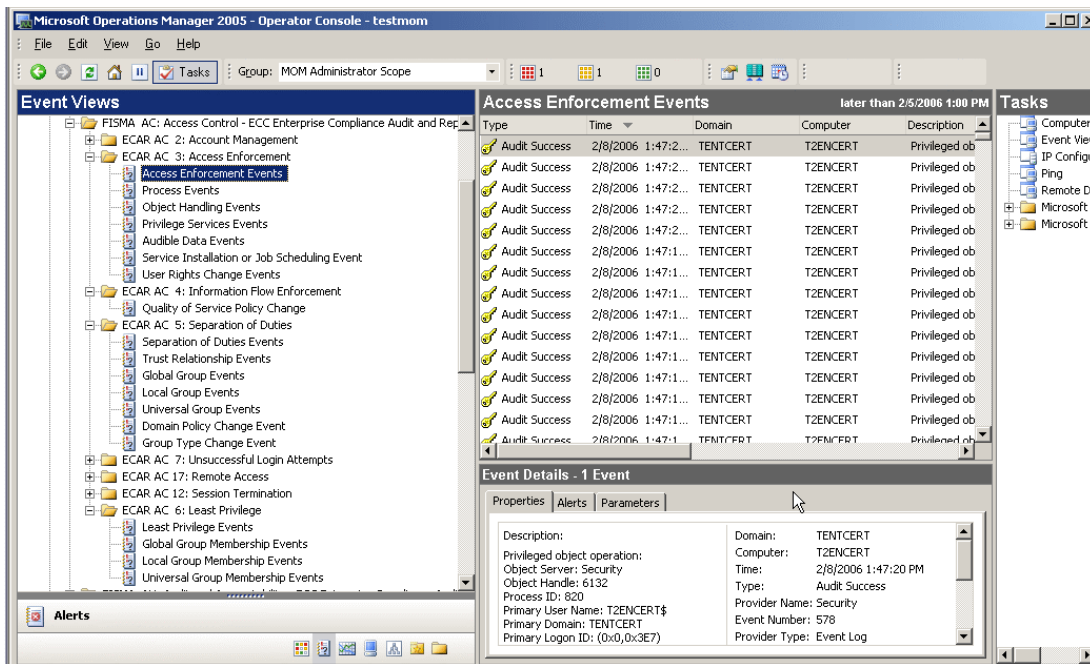
ECC ECAR utilizes the standard MOM Administrative Console interface. After launching the MOM Administrative Console, the user should open the Management Pack tree and select Rules Group. The ECC ECAR Rules Group will become visible. By selecting the parent ECC ECAR Rules group, the first level tree is revealed. According, sub-Rules groups are revealed by selecting the desired item. Rules Groups that are shown with a yellow file folder are Enabled by default. All Enabled Rules Groups contain one or more Windows IT Security Event. Rules Groups contain knowledgebase explanations that are derived directly from NIST SP 800-53. All individual IT Security Events are Enabled by default. Depending on the specific information desired for a given audit cycle, the administrator may select to Enable or Disable a Rules Group or a specific IT Security Event by selecting the desired action from the Properties General tab.



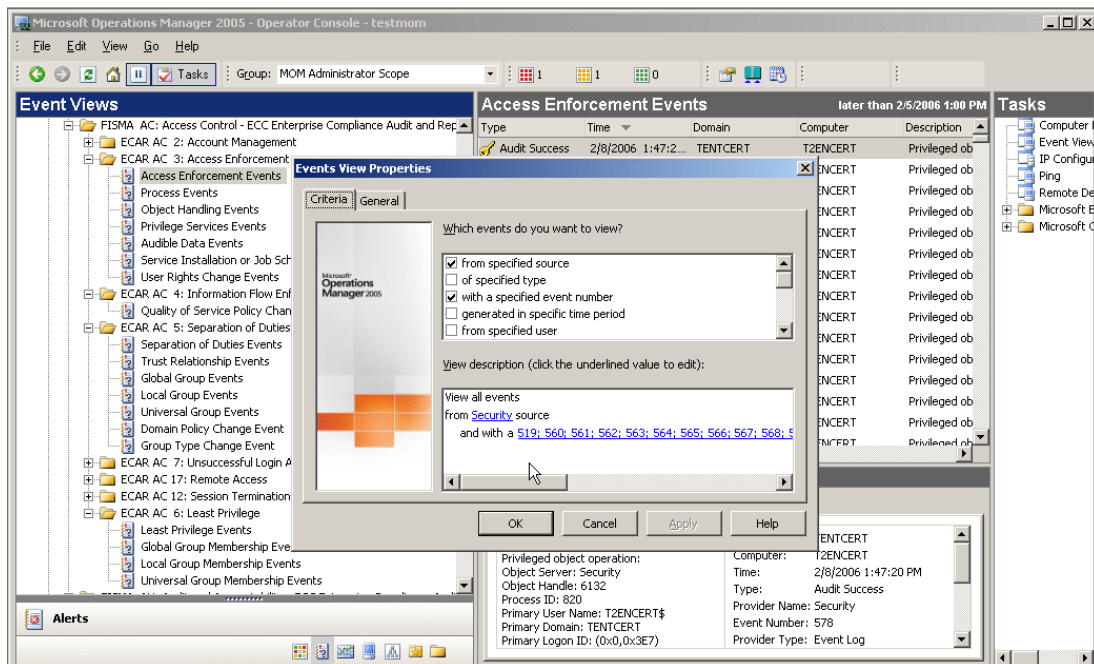
ECC ECAR ADMINISTRATIVE CONSOLE

Operator Console Interface

ECC ECAR utilizes the standard MOM Operator Console interface. A set of predefined Event Views are shipped with ECC ECAR. For Enabled Rules Groups, the Event Views are provided for all associated IT Security Events. In many cases, Event Views are also provided for sub-categories of an Event Rule in order to provide a more defined perspective.



An administrator may also create or modify the Event Views. To create a new Event View Group, right click on desired category and select New Folder and provide it an appropriate name. To create a new Event View, right click on the desired folder and select New Event View. Follow Wizard to define a new Event View.



Enabled: Yes

Parent Rule Group: ECC ECAR

Child Rule Groups:

ECAR AC 1: Access Control Policy and Procedures

ECAR AC 2: Account Management

ECAR AC 3: Access Enforcement

ECAR AC 4: Information Flow Enforcement

ECAR AC 5: Separation of Duties

ECAR AC 6: Least Privilege

ECAR AC 7: Unsuccessful Login Attempts

ECAR AC 8: System Use Notification

ECAR AC 9: Previous Logon Notification

ECAR AC 10: Concurrent Session Control

ECAR AC 11: Session Lock

ECAR AC 12: Session Termination

ECAR AC 13: Supervision and Review - Access Control

ECAR AC 14: Permitted Actions Without Identification or Authentication

ECAR AC 15: Automated Marking

ECAR AC 16 Automated Labeling

ECAR AC 17: Remote Access

ECAR AC 18: Wireless Access Restrictions

ECAR AC 19: Access Control For Portable and Mobile Devices

ECAR AC 20: Personally Owned Information Systems

ECC CAR AC-1: ACCESS CONTROL AND PROCEDURES

Enabled: No

Control Level: High, Medium and Low

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for

the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

NIST Special Publication 800-53

ECC CAR AC-2: Account Management

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended Controls for Account Management

Importance Levels: High, Medium and Low

NOTE: PROCEDURAL RECOMMENDATION. Users should review the following recommendations and added those reporting rules as deemed appropriate.

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency].

Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes.

Control Enhancements:

- (1) The organization employs automated mechanisms to support the management of information system accounts.
- (2) The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].
- (3) The information system automatically disables inactive accounts after [Assignment: organization defined time period].
- (4) The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.

Source: NIST SP 800-53

Event#	Description	Status
624	User Account was created	Enabled
625	User Account type was changed	Enabled
626	User Account was enabled	Enabled
627	User Account password was changed	Enabled
628	User Account password was set	Enabled
629	User Account was disabled	Enabled
630	User Account was deleted	Enabled
640	General account database was changed	Enabled
642	User Account was changed	Enabled
644	User Account was locked	Enabled
645	Computer Account was created	Enabled
646	Computer Account was changed	Enabled
647	Computer Account was deleted	Enabled
685	Name of an account was changed	Enabled
697	Password Policy Checking API Called	Enabled

ECC CAR AC-3: Access Enforcement

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended Access Enforcement Controls

Importance Levels: High, Medium and Low

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes ,programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 compliant.

Source: NIST SP 800-53

Event#	Description	Status
519	Process is using an invalid located procedure call (LPC) port to impersonate a client and reply or read from or write to a client address space	Enabled

560	Access was granted to an already existing object	Enabled
562	Handle to an object was closed	Enabled
563	Attempt to open an object with the intent to delete it was made	Enabled
564	A protect object was deleted	Enabled
565	Access was granted to an already existing object type	Enabled
566	A generic object operation took place	Enabled
567	Permission associated with a handled was used	Enabled
568	Attempt to create a hard link to a file being audited was made	Enabled
569	Resource Manager of Authorization Manager attempted to create a client context	Enabled
570	The client attempted to access an object	Enabled
571	The client context was deleted by the Authorization Manager	Enabled
572	Administrator Manager initialized the application	Enabled
577	Privilege Service Called	Enabled
578	Privileges were used on an already open handle to a protected object	Enabled
592	New Process was created	Enabled
593	Process Exit	Enabled
594	Object handle was duplicated	Enabled
595	Object was indirectly accessed	Enabled
598	Audible Data was protected	Enabled
599	Audible Data was unprotected	Enabled
600	Primary Token was assigned to an object	Enabled
601	User attempted to install a service	Enabled
602	Schedule job was created	Enabled
608	User right was assigned	Enabled
609	User right was removed	Enabled
621	System access was granted	Enabled
622	System access was removed	Enabled

ECC CAR AC-4: Information Flow Enforcement

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Information Flow Enforcement Controls

Importance Level: High, Medium, Low

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Event#	Description	Status
619	Quality of Service Policy Changed	Enabled

ECC CAR AC-5: Separation of Duties

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommendation for Separation of Duties Controls

Supplemental Guidance: Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within information systems and between interconnected systems based on the characteristics of the information. Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).

Source: NIST 800-53

Event#	Description	Status
610	Trust Relationship with another domain was created	Enabled
611	Trust Relationship with another domain was removed	Enabled
620	Trust Relationship with another domain is changed	Enabled
631	Global Group was created	Enabled
631	Global Group was created	Enabled
632	Global Group member was added	Enabled
633	Global Group member was removed	Enabled
634	Global Group was deleted	Enabled
635	Local Group was created	Enabled
636	Local Group member was added	Enabled
637	Local Group member was deleted	Enabled
638	Local group was deleted	Enabled
639	Local group account was changed	Enabled
641	Global Group was changed	Enabled
643	Domain Policy was changed	Enabled
648	Local Security Group with Security Disabled was Created	Enabled
649	Local Security Group with Security Disabled was Changed	Enabled
650	Local Security Group Member Added	Enabled
651	Security Disabled Local Group Member Removed	Enabled
652	Security disabled local group was deleted	Enabled
653	Security-disabled Global Group was created	Enabled
654	Security-disabled Global Group was changed	Enabled
655	Member of a Security-disabled Global Group was added	Enabled
656	Member of Global Security-disabled Group was removed	Enabled

657	Security-disable Global Group was deleted	Enabled
658	Universal Group was created	Enabled
659	Universal Group was changed	Enabled
660	Member of a Universal Group security-enabled was added	Enabled
661	Member of Universal Group security-enabled was removed	Enabled
662	Universal Group was delete	Enabled
663	Universal Security-disabled group was created	Enabled
664	Universal Security-disabled group was changed	Enabled
665	Member of Universal Security-disabled group was added	Enabled
666	Member of Universal Security-disabled group was removed	Enabled
667	Member of Universal Security-disabled group was deleted	Enabled
668	Group type was changed	Enabled
684	Set the security redirector for administrative groups	Enabled
769	Trusted forest information was added	Enabled
770	Trusted forest information was deleted	Enabled
771	Trusted forest information was modified	Enabled
801	Role separation enabled	Enabled

ECC CAR AC-6: Least Privilege

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommendations for Least Privilege Control

Importance Level: High and Medium

Control: 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.

Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Source: NIST SP 800-53

Event#	Description	Status
632	Global Group member was added	Enabled
633	Global Group member was removed	Enabled
636	Local Security Group Member Added	Enabled
655	Member of a Security-disabled Global Group was added	Enabled
656	Member of Global Security-disabled Group was removed	Enabled
660	Member of a Universal Group security-enabled was added	Enabled

661	Member of Universal Group security-enabled was removed	Enabled
665	Member of Universal Security-disabled group was added	Enabled
666	Member of Universal Security-disabled group was removed	Enabled
667	Member of Universal Security-disabled group was deleted	Enabled
637	Local Security Group Member Deleted	Enabled

ECC CAR AC-7: Unsuccessful Login Attempts

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended Unsuccessful Login Attempts Control

Importance Levels: High, Medium and Low

Control: The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Source: NIST SP 800-53

Event#	Description	Status
529	Logon failure from unknown user name or bad password	Enabled
530	Logon failed by user outside allocated time	Enabled
531	Logon to disabled account failed	Enabled
532	Logon to expired account failed	Enabled
534	Logon by non-allowed type failed	Enabled
535	Logon due to expired password failed	Enabled
536	Logon failed due to inactive logon service	Enabled
537	Logon for other reasons failed	Enabled
539	Logon during account lock-out failed	Enabled
548	Logon failure due to SID difference with trusted domain and account domain	Enabled
549	Logon from untrusted forest namespace failed	Enabled
533	Logon by unauthorized computer user failed	Enabled

ECC CAR AC-8: System Use Notification

Enabled: NO

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended for System Use Notification Control

Importance Levels: High, Medium and Low

Control: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: Privacy and security policies are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. For publicly accessible systems: (i) the system use information is available as opposed to displaying the information before granting access; (ii) there are no references to monitoring, recording, or auditing since privacy accommodations for such systems generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Source: NIST SP 800-53

ECC CAR AC-9: Previous Logon Notification

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended Previous Login Notification Control

Importance Level: None Set

Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance: None.

Source: NIST SP 800-53

ECC CAR AC-10: Concurrent Session Control

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended Concurrent Session Control

Importance Level: None Set

Control: The information system limits the number of concurrent sessions for any user to organization defined number of sessions.

SOURCE: NIST SP 800-53

ECC CAR AC-11: Session Lock

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Session Lock Control

Importance Level: High and Medium

Control: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.

SOURCE: NIST SP 800-53

ECC CAR AC-12: Session Termination

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended Session Termination Control

Importance Level: High and Moderate

Control: The information system automatically terminates a session after [Assignment: organization-defined time period] of inactivity.

SOURCE: NIST SP 800-53

Event#	Description	Status
682	User reconnected to a disconnected terminal server connection	Enabled
683	User disconnected terminal services connection without logging off	Enabled

ECC CAR AC-13: Supervision and Review - Access Control

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Supervision and Review - Access Control

Importance Level: High, Moderate and Low

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently, the activities of users with significant information system roles and responsibilities.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

SOURCE: NIST SP 800-53

ECC CAR AC-14: Permitted Actions Without Identification or Authentication

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended ECC ECAR AC-14: Permitted Actions Without Identification or Authentication Control

Importance Level: High, Moderate and Low

Control: The organization identifies specific user actions that can be performed on the information system without identification or authentication.

Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

SOURCE: NIST SP 800-53

ECC CAR AC-15: Automated Marking

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended ECC ECAR AC-15: Automated Marking Control

Importance Level: High

Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Supplemental Guidance: None.

SOURCE: NIST SP 800-53

ECC CAR AC-16 Automated Labeling

Enabled: No

Parent Rule Group AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Automated Labeling Control

Importance Level: None Set

Control: The information system appropriately labels information in storage, in process, and in transmission.

Supplemental Guidance: Information labeling is accomplished in accordance with special dissemination, handling, or distribution instructions, or as otherwise required to enforce information system security policy.

SOURCE: NIST SP 800-53

ECC CAR AC-17: Remote Access

Enabled: Yes

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: NIST Recommended Remote Access Control

Importance Level: High, Moderate and Low

Control: 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.

Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Supplemental Guidance: Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or

subversion of authorized connections (e.g., using virtual private network technology). The organization permits remote access for privileged functions only for compelling operational needs. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements:

- (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.
- (2) The organization uses encryption to protect the confidentiality of remote access sessions.
- (3) The organization controls all remote accesses through a managed access control point.

SOURCE: NIST SP 800-53

Event#	Description	Status
682	User reconnected to a disconnected terminal server connection	Enabled
683	User disconnected terminal services connection without logging off	Enabled

ECC CAR AC-18: Wireless Access Restrictions

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Wireless Access Restrictions Control

Importance Level: High and Moderate

Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.

Supplemental Guidance: NIST Special Publication 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards.

Control Enhancements:

- (1) The organization uses authentication and encryption to protect wireless access to the information system.

SOURCE: NIST SP 800-53

ECC CAR AC-19: Access Control For Portable and Mobile Devices

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Access Control For Portable and Mobile Devices Control

Importance Level: High and Moderate

Control: The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to organizational networks without first meeting organizational security policies and procedures. Security policies and procedures might include such activities as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).

Control Enhancements:

(1) The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.

SOURCE: NIST SP 800-53

ECC CAR AC-20: Personally Owned Information Systems

Enabled: No

Parent Rule Group: AC: Access Control - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Personally Owned Information Systems Control

Importance Level: High, Moderate and Low

Control: The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.

Supplemental Guidance: The organization establishes strict terms and conditions for the use of personally owned information systems. The terms and conditions should address, at a minimum:

(i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, spyware definitions).

Control Enhancements: None.

SOURCE: NIST SP 800-53

AU: AUDIT AND ACCOUNTABILITY

ECAR AU: AUDIT AND ACCOUNTABILITY

FAMILY: Audit and Accountability

CLASS: Technical

Enabled: Yes

Parent Rule Group: ECC ECAR

Child Rule Groups:

ECAR AU 1: Audit and Accountability Policy and Procedures

ECAR AU 2: Auditable Events

ECAR AU 3: Content of Audit Reports

ECAR AU 4: Audit Storage Capacity

ECAR AU 5: Audit Processing

ECAR AU 6: Audit Monitoring, Analysis and Reporting

ECAR AU 7: Audit Reduction and Report Generation

ECAR AU 8: Time Stamps

ECAR AU 9: Protection of Audit Information

ECAR AU 10: Non-Repudiation

ECAR AU 11: Audit Retention

Description: NIST Recommended Audit and Accountability Control

ECAR AU-1: Audit and Accountability Policy and Procedures

Enabled: No

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Audit and Accountability Policy and Procedures Control

Importance Level: High, Moderate and Low

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the

implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

SOURCE: NIST SP 800-53

ECC CAR AU-2: Auditable Events

Enabled: No

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Auditable Events Control

Importance Levels: High, Moderate and Low

Control: The information system generates audit records for the following events:
[Assignment: organization-defined auditable events].

Supplemental Guidance: The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. The checklists and configuration guides at <http://csrc.nist.gov/pcig/cig.html> provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents.

Control Enhancements:

- (1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.
- (2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

SOURCE: NIST SP 800-53

ECC CAR AU-3: Content of Audit Reports

Enabled: Yes

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Content of Audit Reports

Importance Level: High, Moderate and Low

Control: 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.

Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.

Control Enhancements:

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

SOURCE: NIST SP 800-53

Event#	Description	Status
623	Auditing policy was set on a per-user basis	Enabled
625	Per User Audit Policy was changed	Enabled
612	Audit policy was changed	Enabled
805	Event log service read the security log configuration for a session	Enabled

ECC CAR AU-4: Audit Storage Capacity

Enabled: Yes

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Audit Storage Capacity

Importance Level: High, Moderate and Low

Control: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

SOURCE: NIST SP 800-53

Event#	Description	Status
516	Audit Log was exhausted	Enabled
517	Event Log was cleared	Enabled
521	Security log auditing failed	Enabled
523	Audit Log Capacity	Enabled

ECC CAR AU-5: Audit Processing

Enabled: Yes

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Audit Processing Control

Importance Level: High, Moderate and Low

Control: 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: [Assignment: organization-defined actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)].

Supplemental Guidance: None.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches

[Assignment: organization-defined percentage of maximum audit record storage capacity].

SOURCE: NIST SP 800-53

Event#	Description	Status
516	Audit Log was exhausted	Enabled
517	Event Log was cleared	Enabled
521	Security log auditing failed	Enabled
523	Audit Log Capacity	Enabled
522	Audit Collection failed	Enabled

ECC CAR AU-6: Audit Monitoring, Analysis and Reporting

Enabled: Yes

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Audit Monitoring, Analysis and Reporting Control

Importance Level: High and Moderate

Control: 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.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.

SOURCE: NIST SP 800-53

Event#	Description	Status
612	Audit policy was changed	Enabled
805	Event log service read the security log configuration for a session	Enabled

ECC CAR AU-7: Audit Reduction and Report Generation

Enabled: No

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended FISM Audit Reduction and Report Generation

Importance Level: High and Moderate

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

SOURCE: NIST SP 800-53

ECC CAR AU-8: Time Stamps

Enabled: Yes

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Time Stamp Control

Importance Level: High and Moderate

Control: The information system provides time stamps for use in audit record generation.

Supplemental Guidance: Time stamps of audit records are generated using internal system clocks that are synchronized system wide.

SOURCE: NIST SP 800-53

Event#	Description	Status
520	The system time was change	Enabled

ECC CAR AU-9: Protection of Audit Information

Enabled: No

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Protection of Audit Information

Importance Level: High, Moderate and Low

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: None.

Control Enhancements:

(1) The information system produces audit information on hardware-enforced, write-once media.

SOURCE: NIST SP 800-53

ECC CAR AU-10: Non-Repudiation

Enabled: No

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended FISA Non-Repudiation Control

Importance Level: None Set

Control: The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).

Supplemental Guidance: Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-

repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

SOURCE: NIST SP 800-53

ECC CAR AU-11: Audit Retention

Enabled: No

Parent Rule Group: AU: AUDIT AND ACCOUNTABILITY - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Audit Retention

Importance Level: High, Moderation and Low

Control: The organization retains audit logs for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: NIST Special Publication 800-61 provides guidance on computer security incident handling and audit log retention.

SOURCE: NIST SP 800-53

CP: Contingency Planning

Recommended Operational Contingency Planning

FAMILY: Contingency Planning

CLASSIFICATION: Operational

Enabled: Yes

Parent Rule Group: ECC ECAR Child Rule Groups:

ECAR CP 9: Information System Backup

ECAR CP 10: Information Recovery and Reconstruction

Description: Recommended Operational Contingency Planning

ECAR CP 9: Information System Backup

Enabled: Yes

Parent Rule Group: (Operational) CP: Contingency Planning

Child Rule Groups: None

Importance Level: High, Medium and Low

Control: 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.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control Enhancements:

(1) The organization tests backup information [Assignment: organization-defined frequency] to ensure media reliability and information integrity.

(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.

(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

SOURCE: NST SP 800-53

Event#	Description	Status
596	Data Protection Master Key was backed up	Enabled
597	Data Protection Master Key was recovered from a recovery server	Enabled
780	Certificate Services backup started	Enabled
781	Certificate Services backup completed	Enabled
783	Certificate Services restore completed	Enabled
797	Certificate Services archived a log	Enabled
798	Certificate Services imported and archived a key	Enabled
799	Certification services published the certificate authority (CA) certificate to AD	Enabled

ECAR CP 10: Information Recovery and Reconstruction Print

Enabled: Yes

Parent Rule Group: (Operational) CP: Contingency Planning

Child Rule Groups: None

Importance Level: High, Medium and Low

Control: 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.

Supplemental Guidance: Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished,

system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested.

Control Enhancements:

(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

SOURCE: NIST SP 800-53

Event#	Description	Status
596	Data Protection Master Key was backed up	Enabled
597	Data Protection Master Key was recovered from a recovery server	Enabled
780	Certificate Services backup started	Enabled
781	Certificate Services backup completed	Enabled
783	Certificate Services restore completed	Enabled
797	Certificate Services archived a log	Enabled
798	Certificate Services imported and archived a key	Enabled
799	Certification services published the certificate authority (CA) certificate to AD	Enabled

IA: Identification and Authentication Print

ACT IA: Identification and Authentication

FAMILY: Identification and Authentication

CLASS: Technical

Enabled: Yes

Parent Rule Group: ECC CAR

Child Rule Groups:

ECAR IA 1: Identification and Authentication Policy and Procedures

ECAR IA 2: User Identification and Authentication

ECAR IA 3: Device Identification and Authentication

ECAR IA 4: Identifier Management

ECAR IA 5: Authenticator Management

ECAR IA 6: Authenticator Feedback

ECAR IA 7: Cryptographic Module Authentication

Description: Recommended Identification and Authentication Control

ECC CAR IA-1: Identification and Authentication Policy and Procedures

Enabled: No

Parent Rule Group: IA: Identification and Authentication

Child Rule Groups: None

Description: Recommended Identification and Authentication Policy and Procedures

Bound to Computer Groups: None

Importance Level: High, Moderate and Low

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73 and 800-76; and (ii) other applicable federal laws, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

SOURCE: NIST SP 800-53

ECC CAR IA-2: User Identification and Authentication

Enabled: Yes

Parent Rule Group: IA: Identification and Authentication

Child Rule Groups: None

Description: Recommended User Identification and Authentication

Importance Level: High, Moderate and Low

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Supplemental Guidance: Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63

provides guidance on remote electronic authentication. For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter which is considered to offer sufficient protection, NIST Special Publication 800-63 guidance should be applied as follows: (i) for low impact information systems, tokens that meet Level 1, 2, 3, or 4 requirements are acceptable; (ii) for moderate-impact information systems, tokens that meet Level 2, 3, or 4 requirements are acceptable; and (iii) for high-impact information systems, tokens that meet Level 3 or 4 requirements are acceptable. In addition to identifying and authenticating users at the information system level, identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

Control Enhancements:

(1) The information system employs multifactor authentication.

SOURCE: NIST SP 800-53

Event#	Description	Status
528	Logon was successful	Enabled
529	Logon failure from unknown user name or bad password	Enabled
530	Logon failed by user outside allocated time	Enabled
531	Logon to disabled account failed	Enabled
532	Logon to expired account failed	Enabled
534	Logon by non-allowed type failed	Enabled
535	Logon due to expired password failed	Enabled
536	Logon failed due to inactive logon service	Enabled
537	Logon for other reasons failed	Enabled
538	Logoff by user was completed	Enabled
539	Logon during account lock-out failed	Enabled
540	Logon to network was successful	Enabled
548	Logon failure due to SID difference with trusted domain and account domain	Enabled
549	Logon from untrusted forest namespace failed	Enabled
551	User log off process was initiated	Enabled
552	User logon with explicit credentials while logged on as different user	Enabled
672	Authentication Service (AS) ticket was issued and validate	Enabled
673	Ticket Granting Service (TGS) ticket was issued	Enabled
674	Security Principal was renewed as AS or TGS Ticket	Enabled
675	Preauthorization failed	Enabled
676	Authorization ticket failed	Enabled
677	TGS ticket was not granted	Enabled
678	An account was successfully mapped to a domain account	Enabled
680	NTLM Successfully Authenticates User	Enabled
681	NTLM failed when login attempt to domain ... not W2k3 or XP	Enabled

ECC CAR IA-3: Device Identification and Authentication

Enabled: Yes

Parent Rule Group: IA: Identification and Authentication

Child Rule Groups: None

Description: Recommended Device Identification and Authentication

Importance Level: High and Moderate

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.

SOURCE: NIST SP 800-53

Event#	Description	Status
533	Logon by unauthorized computer user failed	Enabled
541	Main Mode IKE Connection to peer was complete	Enabled
542	Data channel was terminated	Enabled
543	Main mode was terminated	Enabled
544	Main mode failed due to peer invalid certificate or signature	Enabled
545	Main mode failed due to Kerberos failure or invalid password	Enabled
546	IKE security establishment failed due to invalid peer proposal	Enabled
547	IKE handshake failed	Enabled

ECC CAR IA-4: Identifier Management

Enabled: Yes

Parent Rule Group: IA: Identification and Authentication

Child Rule Groups: None

Description: Recommended Identifier Management

Importance Level: High, Moderate and Low

Control: 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.

Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors.

SOURCE: NIST SP 800-53

Event#	Description	Status
624	User Account was created	Enabled
625	User Account type was changed	Enabled
626	User Account was enabled	Enabled
627	User Account password was changed	Enabled
628	User Account password was set	Enabled
629	User Account was disabled	Enabled
630	User Account was deleted	Enabled
640	General account database was changed	Enabled
642	User Account was changed	Enabled
644	User Account was locked	Enabled
645	Computer Account was created	Enabled
646	Computer Account was changed	Enabled
647	Computer Account was deleted	Enabled
685	Name of an account was changed	Enabled
697	Password Policy Checking API Called	Enabled

ECC CAR IA-5: Authenticator Management

Enabled: Yes

Parent Rule Group: IA: Identification and Authentication

Child Rule Groups: None

Description: Recommended Authentication

Importance Level: High, Moderate and Low

Control: 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.

Supplemental Guidance: Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates

by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

SOURCE: NIST SP 800-53

Event#	Description	Status
514	Authentication package was located by the Local Security Agent (LSA)	Enabled
515	Trusted Logon Process was registered by the Local Security Agent	Enabled
518	Notification package was loaded on the Security Accounts Manager	Enabled
615	IPSec Policy was changed	Enabled
616	IPSec Policy agent encountered a potentially serious failure	Enabled
617	Kerberos policy was changed	Enabled
618	Encrypted Data Policy was changed	Enabled
772	Certificate Manager denied a pending certificate request	Enabled
773	Certificate Services received a resubmitted certificate request	Enabled
774	Certificate Services revoked a certificate	Enabled
775	Certificate Services received a request to publish the certificated revocation list (CRL)	Enabled
776	Certificate Services publish the CRL	Enabled
777	A certificate request extension was made	Enabled
778	One or more certificate request attributes changed	Enabled
786	The security permissions for Certificate Services changed	Enabled
787	Certificate Services retrieved an archival file	Enabled
788	Certificate Services imported a certificate into the database	Enabled
789	The audit filter for Certificate Services changed	Enabled
790	Certificate Services received a certificate request	Enabled
791	Certificate Services approved a certificate request	Enabled
792	Certificate Services denied a certificate request	Enabled
793	Certificate Services set the status of a certificate request to pending	Enabled
794	The certificate manager settings for Certificate Services change	Enabled
795	A Configuration entry changed in Certificate Services	Enabled
796	A property of Certification Services change	Enabled
800	One or more rows have been deleted from certificate database	Enabled

ECC CAR IA-6: Authenticator Feedback

Enabled: No

Parent Rule Group: IA: Identification and Authentication

Child Rule Groups: None

Description: Recommended Authentication Feedback

Importance Level: High, Moderate and Low

Control: The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.

Supplemental Guidance: The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).

SOURCE: NIST SP 800-53

ECC CAR IA-7: Cryptographic Module Authentication

Enabled: Yes

Parent Rule Group: IA: Identification and Authentication

Child Rule Groups: None

Description: Recommended Cryptographic Module Authentication

Importance Level: High, Moderate and Low

Control: For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.

SOURCE: NIST SP 800-53

EVENT #	DESCRIPTION	STATUS
596	Data Protection Master Key was backed up	Enabled
597	Data Protection Master Key was recovered from a recovery server	Enabled

SC: System and Communication Protection

FAMILY SC: System and Communication Protection

FAMILY: System and Communication Protection

CLASSIFICATION: Technical

Enabled: Yes

Parent Rule Group: ECC ECAR

Child Rule Groups:

ECAR SC 1: System and Communication Protection Policy and Procedures

ECAR SC 2: Application Partitioning

ECAR SC 3: Security Function Isolation

ECAR SC 4: Information Remnants

ECAR SC 5: Denial of Service Protection

ECAR SC 6: Resource Priority

ECAR SC 7: Boundary Protection

ECAR SC 8: Transmission Integrity

ECAR SC 9: Transmission Confidentiality

ECAR SC 10: Network Disconnect

ECAR SC 11: Trusted Path

ECAR SC 12: Cryptographic Key Establishment and Management

ECAR SC 13: Use of Validated Cryptography

ECAR SC 14: Public Access Protection

ECAR SC 15: Collaborative Computing

ECAR SC 16: Transmission of Security Parameters

ECAR SC 17: Public Key Infrastructure Certificates

ECAR SC 18: Mobile Code

ECAR SC 19: Voice Over Internet Protocol

Description: Recommended System and Communication Control

ECC CAR SC-1: System and Communication Protection Policy and Procedures

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended System and Communication Protection Policy and Procedures

Importance Level: High, Moderate and Low

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

SOURCE: NIST SP 800-53

ECC CAR SC-2: Application Partitioning

Enabled: Yes

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Application Partitioning

Importance Level: High and Moderate

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

SOURCE: NIST SP 800-53

Event#	Description	Status
768	Collision detected between a namespace element in one forest and namespace element in another forest	Enabled

ECC CAR SC-3: Security Function Isolation

Enabled: Yes

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Security Function Isolation

Importance Level: High

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Control Enhancements:

- (1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.
- (2) The information system further divides the security functions with the functions enforcing access and information flow control isolated and protected from both nonsecurity functions and from other security functions.
- (3) The information system minimizes the amount of nonsecurity functions included within the isolation boundary containing security functions.
- (4) The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.
- (5) The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.

SOURCE: NIST SP 800-53

ECC CAR SC-4: Information Remnants

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Information Remnants

Importance Level: High and Moderate

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

SOURCE: NIST SP 800-53

ECC CAR SC-5: Denial of Service Protection

Enabled: Yes

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Denial of Service Protection

Importance Level: High, Moderate and Low

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization- defined list of types of denial of service attacks or reference to source for current list].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

SOURCE: NIST SP 800-53

Event#	Description	Status
550	Notification of possible denial of service attack was sent	Enabled

ECC CAR SC-6: Resource Priority

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Resource Priority

Importance Level: High and Moderate

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

SOURCE: NIST SP 800-53

ECC CAR SC-7: Boundary Protection

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Boundary Protection

Importance: High and Moderate

Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Supplemental Guidance: Any connections to the Internet, or other external networks or information systems, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate sub networks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.

SOURCE: NIST SP 800-53

ECC CAR SC-8: Transmission Integrity

Enabled: Yes

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Transmission Integrity

Importance Level: High and Moderate

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

SOURCE: NIST SP 800-53

Event#	Description	Status
619	Quality of Service Policy Changed	Enabled
618	Encrypted Data Policy was changed	Enabled
541	Main Mode IKE Connection to peer was complete	Enabled
542	Data channel was terminated	Enabled
543	Main mode was terminated	Enabled
544	Main mode failed due to peer invalid certificate or signature	Enabled
545	Main mode failed due to Kerberos failure or invalid password	Enabled
546	IKE security establishment failed due to invalid peer proposal	Enabled
547	IKE handshake failed	Enabled

ECC CAR SC-9: Transmission Confidentiality

Enabled: Yes

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Transmission Confidentiality

Importance Level: High and Moderate

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: The FIPS 199 security category (for confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

SOURCE: NIST SP 800-53

Event#	Description	Status
618	Encrypted Data Policy was changed	Enabled
541	Main Mode IKE Connection to peer was complete	Enabled
542	Data channel was terminated	Enabled
543	Main mode was terminated	Enabled
544	Main mode failed due to peer invalid certificate or signature	Enabled
545	Main mode failed due to Kerberos failure or invalid password	Enabled
546	IKE security establishment failed due to invalid peer proposal	Enabled
547	IKE handshake failed	Enabled

ECC CAR SC-10: Network Disconnect

Enabled: Yes

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Network Disconnect

Importance Level: High and Moderate

Control: The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.

SOURCE: NIST SP 800-53

Event#	Description	Status
542	Data channel was terminated	Enabled
683	User disconnected terminal services without logging off	Enabled

ECC CAR SC 11 –Trusted Path

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Trust Path Control

Importance Level: None Set

Control: The information system establishes a trusted communications path between the user and the security functionality of the system.

SOURCE: NIST SP 800-53

ECC CAR SC-12: Cryptographic Key Establishment and Management

Enabled: Yes

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Cryptographic Key Establishment and Management

Importance Level: High and Moderate

Control: The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.

SOURCE: NIST SP 800-53

Event#	Description	Status
615	IPSec Policy was changed	Enabled
617	Kerberos policy was changed	Enabled
618	Encrypted Data Policy was changed	Enabled
772	Certificate Manager denied a pending certificate request	Enabled
773	Certificate Services received a resubmitted certificate request	Enabled
774	Certificate Services revoked a certificate	Enabled
775	Certificate Services received a request to publish the certificated revocation list (CRL)	Enabled
776	Certificate Services publish the CRL	Enabled
777	A certificate request extension was made	Enabled
778	One or more certificate request attributes changed	Enabled
786	The security permissions for Certificate Services changed	Enabled
788	Certificate Services imported a certificate into the database	Enabled
790	Certificate Services received a certificate request	Enabled
791	Certificate Services approved a certificate request	Enabled
792	Certificate Services denied a certificate request	Enabled
793	Certificate Services set the status of a certificate request to pending	Enabled
794	The certificate manager settings for Certificate Services change	Enabled
795	A Configuration entry changed in Certificate Services	Enabled
796	A property of Certification Services change	Enabled

ECC CAR SC-13: Use of Validated Cryptography

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Use of Validated Cryptography

Importance Level: High, Moderate and Low

Control: When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.

SOURCE: NIST SP 800-53

ECC CAR SC-14: Public Access Protection

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Public Access Protection

Importance Level: High, Moderate and Low

Control: For publicly available systems, the information system protects the integrity of the information and applications.

SOURCE: NIST SP 800-53

ECC CAR SC-15: Collaborative Computing

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Collaborative Computing Control

Importance Level: High and Moderate

Control: The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).

SOURCE: NIST SP 800-53

ECC CAR SC-16: Transmission of Security Parameters

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Transmission of Security Parameters

Importance Level: Not Set

Control: The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.

Supplemental Guidance: Security parameters may be explicitly or implicitly associated with the information contained within the information system

SOURCE: NIST SP 800-53

ECC CAR SC-17: Public Key Infrastructure Certificates

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Public Key Infrastructure Certificates

Importance Level: High and Moderate

Control: The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.

Supplemental Guidance: Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

SOURCE: NIST SP 800-53

ECC CAR SC-18: Mobile Code

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Mobile Code Control

Importance Level: High and Moderate

Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.

Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at: <http://iase.disa.mil/mcp/index.html>.

SOURCE: NIST SP 800-53

ECC CAR SC-19: Voice Over Internet Protocol

Enabled: No

Parent Rule Group: SC: System and Communication Protection - ECC Compliance Audit and Report Pack

Child Rule Groups: None

Description: Recommended Voice Over Internet Protocol Control

Importance Level: High and Moderate

Control: The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP. Supplemental Guidance: NIST Special Publication 800-58 provides guidance on security considerations for VOIP technologies employed in information systems.

SOURCE: NIST SP 800-53

SI: System and Information Integrity

SI: System and Information Integrity

CLASS: Operational

ECAR SI 6: Security Verification Functionality Print

Enabled: Yes

Parent Rule Group: Act

Child Rule Groups: None

Importance Level: High and Moderate

Control: The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.

Supplemental Guidance: None.

Control Enhancements:

- (1) The organization employs automated mechanisms to provide notification of failed security tests.
- (2) The organization employs automated mechanisms to support management of distributed security testing.

SOURCE: NIST SP 800-53

Event#	Description	Status
512	Server Startup	Enabled
513	Server Shutdown	Enabled
613	IPSec Policy Agent was started	Enabled
614	IPSec Policy Agent was disabled	Enabled
779	Certificate Services received a request to shutdown	Enabled
782	Certificate Services restore started	Enabled
784	Certificate Services started	Enabled
785	Certificate Services stopped	Enabled

EVENT VIEWS

Event Views provide a means to quickly see related activity associated with one or a defined collection of IT security events. Views are accessible through the MOM Operations Console. The user can customize the views by creating, adding or modifying those Event Views for ECAR™ that are shipped by default and identified in the following pages. Refer to the MOM Operations Console Event View documentation to customize the ECAR™ views.

AC: Access Control

ECAR AC 2: Account Management

Account Management Event

Event #: 624; 625; 626; 626; 627; 628; 629; 630; 640; 642; 642; 644; 645; 646; 647; 685; 697

Computer Account Events

Event #: 645; 646; 647

General Database Account Change

Event #: 640

User Account Events

Event #: 624; 625; 626; 627; 628; 629; 630; 642; 644; 671

ECAR AC 3: Access Enforcement

Access Enforcement Events

Event #: 519; 560; 561; 562; 563; 564; 565; 566; 567; 568; 569; 570; 571; 572; 573;
577; 578; 592; 593; 594; 595; 598; 599; 600; 601; 602; 608; 609; 621; 622; 669; 670

ECAR AC 4: Information Flow Enforcement

Quality of Service Events

Event #: 619

ECAR AC 5: Separation of Duties

Separation of Duties Events

Event #: 610; 611; 620; 631; 632; 633; 634; 635; 636; 637; 638; 639; 641; 643; 648;
649; 650; 651; 652; 653; 654; 655; 656; 657; 658; 659; 660; 661; 662; 663; 664; 665;
666; 667; 668; 684; 769; 770; 771; 801

ECAR AC 7: Unsuccessful Login Attempts

Unsuccessful Login Attempts Events

Event #: 529; 530; 531; 532; 534; 535; 536; 537; 539; 548; 549; 533

ECAR AC 17: Remote Access

Remote Access Events

Event #: 682; 683

AU: Audit and Accountability

ECAR AU 3: Content of Audit Reports

Content of Audit Reports Events

Event #: 623; 625; 612; 805

ECAR AU 4: Audit Storage Capacity

Audit Storage Capacity Events

Event #: 516; 517; 521; 523

ECAR AU 5: Audit Processing

Audit Processing Events

Event #: 516; 517; 521; 522; 523

ECAR AU 6: Audit Monitoring, Analysis and Reporting

Audit Monitoring, Analysis and Reporting Events

Event #: 612; 805

ECAR AU 8: Time Stamps

Time Stamps Events

Event #: 520

(Operational) CP: Contingency Planning

ECAR CP 9: Information System Backup

Information System Backup Events

Event #: 596; 597; 780; 781; 783; 797; 798; 799

ECAR CP 10: Information Recovery and Reconstruction

Information Recovery and Reconstruction Events

Event #: 596; 597; 780; 781; 783; 797; 798; 799

IA: Identification and Authentication

ECAR IA 2: User Identification and Authentication

User Identification and Authentication Events

Event #: 528; 529; 530; 531; 532; 534; 535; 536; 537; 538; 539; 540; 548; 549; 551; 552; 672; 673; 674; 675; 676; 677; 678; 680; 681

ECAR IA 3: Device Identification and Authentication

Device Identification and Authentication Events

Event #: 533; 541; 542; 543; 544; 545; 546; 547

IKE Events

Event #: 541; 546; 547

Main Mode Events

Event #: 541; 542; 543; 544; 545

ECAR IA 4: Identifier Management

Computer Account Events

Event #: 645; 646; 647

General Database Account Change

Event #: 640

User Account Events

Event #: 624; 625; 626; 627; 628; 629; 630; 642; 644; 671

ECAR IA 5: Authenticator Management

Authenticator Management Events

Event #: 514; 515; 518; 615; 616; 617; 618; 772; 773; 774; 775; 776; 777; 778; 786;
787; 788; 789; 790; 791; 792; 793; 794; 795; 796; 800

IPSec Policy Change Event

Event #: 615; 616

Kerberos Policy Change Event

Event #: 617

(Operational) SI: System and Information Integrity

ECAR SI 6: Security Verification Functionality

Security Verification Functionality Events

Event #: 512; 513; 613; 614; 779; 782; 784; 785

SC: System and Communication Protection

ECAR SC 2: Application Partitioning

Application Partitioning Events

Event #: 768

ECAR SC 5: Denial of Service Protection

Denial of Service Protection Event

Event #: 550

ECAR SC 8: Transmission Integrity

Transmission Integrity Events

Event #: 619; 618; 541; 542; 543; 544; 545; 546; 547

IKE Events

Event #: 541; 546; 547

Main Mode Events

Event #: 541; 542; 543; 544; 545

Quality of Service Policy Change Events

Event #: 619

ECAR SC 9: Transmission Confidentiality

Transmission Confidentiality Events

Event #: 618; 541; 542; 543; 544; 545; 546; 547

Encrypted Data Policy Change

Event # 618

IKE Events

Event #: 541; 546; 547

Main Mode Events

Event #: 541; 542; 543; 544; 545

ECAR SC 12: Cryptographic Key Establishment and Management

Certificate Services Events

Event #: 772; 773; 774; 775; 776; 777; 778; 786; 788; 790; 791; 792; 798; 799

IPSec Policy Change Event

Event #: 615; 616

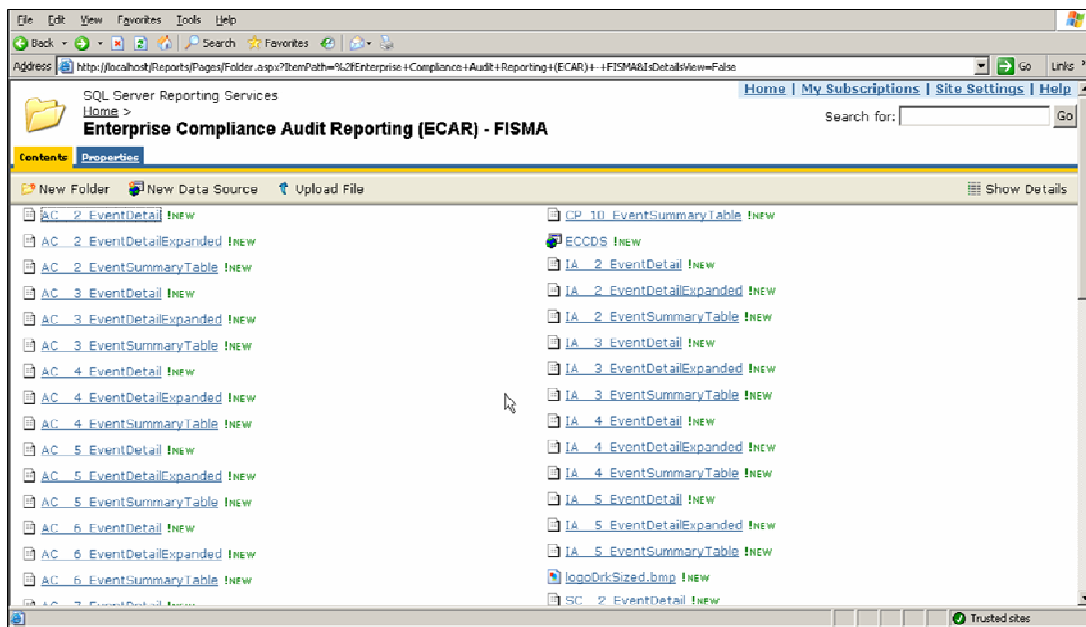
Kerberos Policy Change Event

Event #: 617

CHAPTER THREE: ECAR REPORTS

Standard ECAR Reports

ECAR reporting intends to meet the requirements of external compliance auditors, internal compliance auditors, and enhance the general security practices for internal IT Staff. ECAR ships with over 90 pre-designed reports that map directly to enable NIST SP 800-53 recommended controls. Once Deployed from the MOM Server, the reports are available from SQL 2000 Reporting Services Server. Using Internet Explorer browser, type in the URL for the Reporting Server: <http://ServerName/ReportServer>.



The naming conventions of each report map directly to the ECAR Rules Group and NIST recommendations. Therefore report AC_2_EventDetail maps to Access Control Rule Group 2 with an Event Detail output form.

Each ECAR NIST enabled recommendation is supported by three report types:

Event Detail - The basic report format and control group is the Even Detail Report. The event detail reports display high level event information including the date and time of occurrence, event ID and type plus domain, computer and user information. An example of the Event Detail report type is shown in the next figure.

Address: http://localhost/Reports/Pages/Report.aspx?ItemPath=%2fEnterprise+Compliance+Audit+Reporting+(ECAR)+FISMA%2fAC_3

1 of 9 | 100% | Find | Next | Select a format | Export

Domain: <ALL> Event ID: <ALL>
User: <ALL> Created 2/16/2006 3:22:07 PM
On:

Event ID	Date Time	Type	Domain	Computer	User
593	2/11/2006 3:38:00 PM	Audit Success	TENTCERT	T2ENCERT	LOCAL SERVICE
600	2/11/2006 3:40:02 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
592	2/11/2006 3:40:02 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
593	2/11/2006 4:07:13 PM	Audit Success	TENTCERT	T2ENCERT	LOCAL SERVICE
600	2/11/2006 4:10:19 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
592	2/11/2006 4:10:19 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
593	2/11/2006 4:37:03 PM	Audit Success	TENTCERT	T2ENCERT	LOCAL SERVICE
592	2/11/2006 4:40:24 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
600	2/11/2006 4:40:24 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
593	2/11/2006 5:07:02 PM	Audit Success	TENTCERT	T2ENCERT	LOCAL SERVICE
600	2/11/2006 5:10:02 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
592	2/11/2006 5:10:02 PM	Audit Success	TENTCERT	T2ENCERT	SYSTEM
593	2/11/2006 6:07:02 PM	Audit Success	TENTCERT	T2ENCERT	LOCAL SERVICE

Done Trusted sites

Event Detail Expanded - Provides an expanded set of information on the select Event Rule Group as shown below.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address: http://localhost/Reports/Pages/Report.aspx?ItemPath=%2fEnterprise+Compliance+Audit+Reporting+(ECAR)+FISMA%2fAC_3_EventDetail

1 of 18 | 150% | Find | Next | Select a format | Export

Event ID	Date Time	Type	Domain	Computer
593	2/11/2006 3:38:00 PM	Audit Success	TENTCERT	T2ENCERT
Description:		A process has exited: Process ID: 2192 Image File Name: C:\WINDOWS\system32\wbem\wmiprvse.exe User Name: LOCAL SERVICE Domain: NT AUTHORITY Logon ID: (0x0,0x3E5)		
600	2/11/2006 3:40:02 PM	Audit Success	TENTCERT	T2ENCERT
Description:		A process was assigned a primary token.		

Event Summary Report – This report type provides audit information of events grouped for quarterly summary reports.

Report Manager - Microsoft Internet Explorer

Address: http://localhost/Reports/Pages/Report.aspx?ItemPath=%2fEnterprise+Compliance+Audit+Reporting+(ECAR)+--+F15MA%2fIA_2_EventSummary

Summary Year: 2005
 Computer Group: ECC ECAR - GLBA
 Event ID: <ALL>
 Computer: <ALL>
 Domain: <ALL>
 User: <ALL>

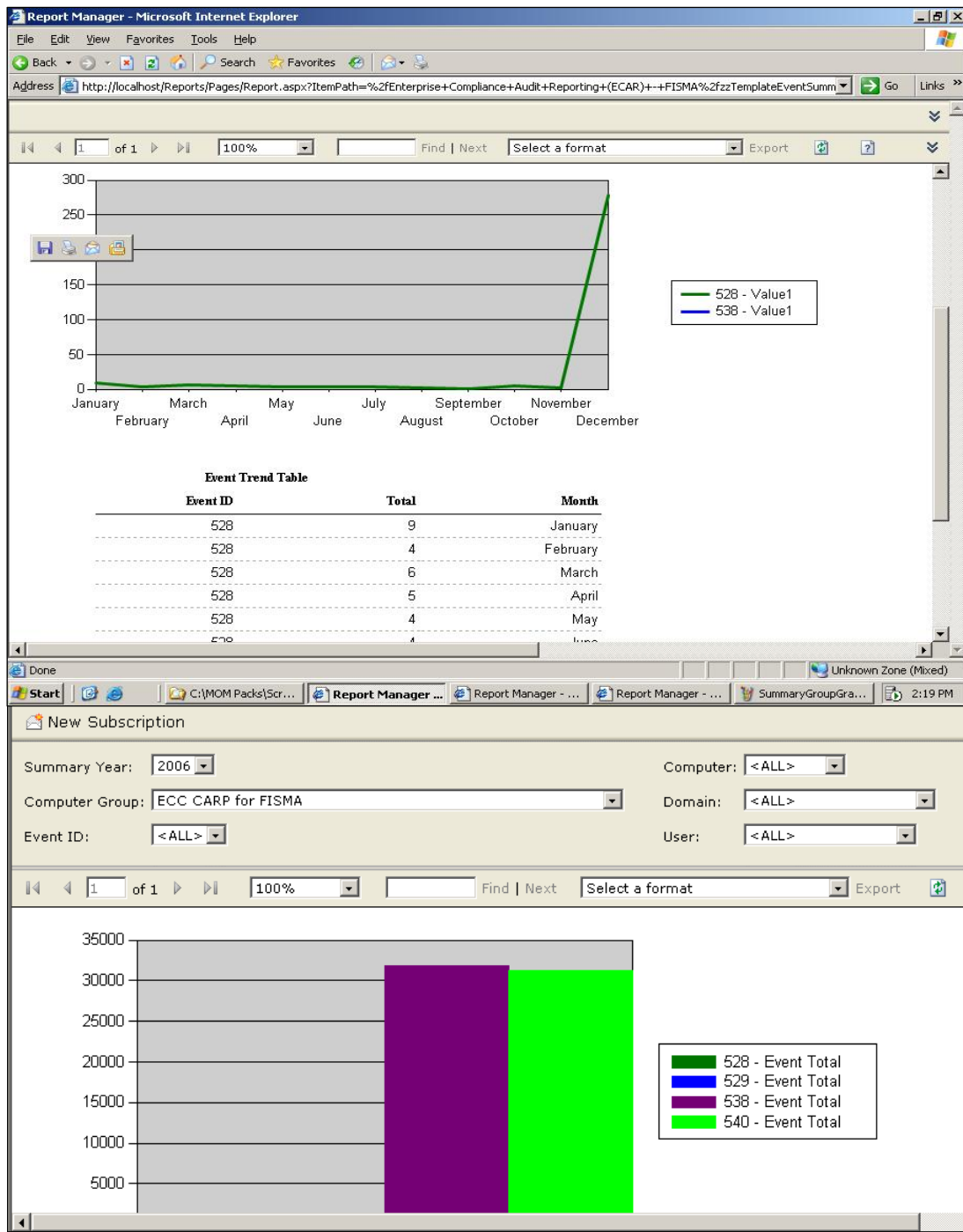
1 of 1 | 100% | Find | Next | Select a format | Export

Event ID	Event Total	Domain	Computer	User
528	1	ENTCERT	SQLSERVER	Administrator
538	3	ENTCERT	ADSERVER	SYSTEM
1st Quarter Total 10				
2nd Quarter				
Event ID	Event Total	Domain	Computer	User
528	2	ENTCERT	ADSERVER	LOCAL SERVICE
528	1	ENTCERT	ADSERVER	NETWORK SERVICE
528	1	ENTCERT	SQLSERVER	LOCAL SERVICE
528	1	ENTCERT	SQLSERVER	NETWORK SERVICE
528	2	ENTCERT	SQLSERVER	SYSTEM
538	3	ENTCERT	ADSERVER	Administrator
2nd Quarter Total 10				
3rd Quarter				
Event ID	Event Total	Domain	Computer	User
528	4	ENTCERT	SQLSERVER	Administrator
528	1	ENTCERT	SQLSERVER	LOCAL SERVICE
528	1	ENTCERT	SQLSERVER	NETWORK SERVICE

Taskbar: Start | C:\MOM Packs\Scr... | Report Manager - ... | Report Manager ... | Report Manager - ... | SummaryTrendGra... | 2:21 PM

There are two optional report templates that provide graphical output as shown in the screen shots that follow:

1. Trend Analysis – illustrates event activity over type
2. Group Analysis – provides a comparison of identified events



Report Configuration – Report output can be defined by the administrator as shown in the following example screen.

The screenshot displays the SSRS report configuration page for 'AC_2_EventDetail'. The 'Reporting Filter Information' section shows the following details:

- Begin Time:** 01/01/2006 12:26:11 PM
- End Time:** 2/16/2006 12:26:11 PM
- Computer Group:** ECC CARP for FISMA
- Computer:** <ALL>
- Domain:** <ALL>
- User:** <ALL>
- Event ID:** <ALL>
- Created On:** 2/16/2006 12:31:21 PM

The report output table is as follows:

Event ID	Date Time	Type	Domain	Computer	User
647	1/24/2006 8:18:03 A.M.	Audit Success	TRNTYCERT	TEST	Administrator

Report Output – Reports can be saved and output to a number of formats including common text delimited forms, Excel, and XML. The Export pull down menu is located at report option window.

APPENDIX A: IT Security Events

- 512 Server Startup
- 513 Server Shutdown
- 514 Authentication package was located by the Local Security Agent (LSA)
- 515 Trusted Logon Process was registered by the Local Security Agent
- 516 Audit Log was exhausted
- 517 Event Log was cleared
- 518 Notification package was loaded on the Security Accounts Manager
- 519 Process is using an invalid located procedure call (LPC) port to impersonate a client and reply or read from or write to a client address space
- 520 The system time was change
- 521 Security log auditing failed
- 522 Audit Collection failed
- 523 Audit Log Capacity
- 528 Logon was successful
- 529 Logon failure from unknown user name or bad password
- 530 Logon failed by user outside allocated time
- 531 Logon to disabled account failed
- 532 Logon to expired account failed
- 533 Logon by unauthorized computer user failed
- 534 Logon by non-allowed type failed
- 535 Logon due to expired password failed
- 536 Logon failed due to inactive logon service
- 537 Logon for other reasons failed
- 538 Logoff by user was completed
- 539 Logon during account lock-out failed
- 540 Logon to network was successful
- 541 Main Mode IKE Connection to peer was complete
- 542 Data channel was terminated
- 543 Main mode was terminated
- 544 Main mode failed due to peer invalid certificate or signature
- 545 Main mode failed due to Kerberos failure or invalid password
- 546 IKE security establishment failed due to invalid peer proposal
- 547 IKE handshake failed
- 548 Logon failure due to SID difference with trusted domain and account domain
- 549 Logon from untrusted forest namespace failed
- 550 Notification of possible denial of service attack was sent
- 551 User log off process was initiated
- 552 User logon with explicit credentials while logged on as different user
- 560 Access was granted to an already existing object
- 561 Handle allocated

- 562 Handle to an object was closed
- 563 Attempt to open an object with the intent to delete it was made
- 564 A protect object was deleted
- 565 Access was granted to an already existing object type
- 566 A generic object operation took place
- 567 Permission associated with a handled was used
- 568 Attempt to create a hard link to a file being audited was made
- 569 Resource Manager of Authorization Manager attempted to create a client context
- 570 The client attempted to access an object
- 571 The client context was deleted by the Authorization Manager
- 572 Administrator Manager initialized the application
- 573 Process generates nonsystem audit event with Authorization API
- 577 Privilege Service Called
- 578 Privileges were used on an already open handle to a protected object
- 592 New Process was created
- 593 Process Exit
- 594 Object handle was duplicated
- 595 Object was indirectly accessed
- 596 Data Protection Master Key was backed up
- 597 Data Protection Master Key was recovered from a recovery server
- 598 Audible Data was protected
- 599 Audible Data was unprotected
- 600 Primary Token was assigned to an object
- 601 User attempted to install a service
- 602 Schedule job was created
- 608 User right was assigned
- 609 User right was removed
- 610 Trust Relationship with another domain was created
- 611 Trust Relationship with another domain was removed
- 612 Audit policy was changed
- 613 IPSec Policy Agent was started
- 614 IPSec Policy Agent was disabled
- 615 IPSec Policy was changed
- 616 IPSec Policy agent encountered a potentially serious failure
- 617 Kerberos policy was changed
- 618 Encrypted Data Policy was changed
- 619 Quality of Service Policy Changed
- 620 Trust Relationship with another domain is changed
- 621 System access was granted
- 622 System access was removed
- 623 Auditing policy was set on a per-user basis
- 624 User Account was created
- 625 User Account type was changed
- 625 Per User Audit Policy was changed
- 626 User Account was enabled
- 627 User Account password was changed
- 628 User Account password was set
- 629 User Account was disabled
- 630 User Account was deleted

- 631 Global Group was created
- 631 Global Group was created
- 632 Global Group member was added
- 633 Global Group member was removed
- 634 Global Group was deleted
- 635 Local Group was created
- 636 Local Group member was added
- 637 Local Group member was deleted
- 638 Local group was deleted
- 639 Local group account was changed
- 640 General account database was changed
- 641 Global Group was changed
- 642 User Account was changed
- 643 Domain Policy was changed
- 644 User Account was locked
- 645 Computer Account was created
- 646 Computer Account was changed
- 647 Computer Account was deleted
- 648 Local Security Group with Security Disabled was Created
- 649 Local Security Group with Security Disabled was Changed
- 650 Local Security Group Member Added
- 651 Security Disabled Local Group Member Removed
- 652 Security disabled local group was deleted
- 653 Security-disabled Global Group was created
- 654 Security-disabled Global Group was changed
- 655 Member of a Security-disabled Global Group was added
- 656 Member of Global Security-disabled Group was removed
- 657 Security-disable Global Group was deleted
- 658 Universal Group was created
- 659 Universal Group was changed
- 660 Member of a Universal Group security-enabled was added
- 661 Member of Universal Group security-enabled was removed
- 662 Universal Group was delete
- 663 Universal Security-disabled group was created
- 664 Universal Security-disabled group was changed
- 665 Member of Universal Security-disabled group was added
- 666 Member of Universal Security-disabled group was removed
- 667 Member of Universal Security-disabled group was deleted
- 668 Group type was changed
- 669 Add SID History (Success)
- 670 Add SID History(Failure)
- 671 User Account Unlocked
- 672 Authentication Service (AS) ticket was issued and validate
- 673 Ticket Granting Service (TGS) ticket was issued
- 674 Security Principal was renewed as AS or TGS Ticket
- 675 Preauthorization failed
- 676 Authorization ticket failed
- 677 TGS ticket was not granted
- 678 An account was successfully mapped to a domain account

-
- 680 NTLM Successfully Authenticates User
 - 681 NTLM failed when login attempt to a domain
 - 682 User reconnected to a disconnected terminal server connection
 - 683 User disconnected terminal services connection without logging off
 - 684 Set the security redirector for administrative groups
 - 685 Name of an account was changed
 - 686 Password for the user accessed
 - 697 Password Policy Checking API Called
 - 768 Collision detected between a namespace element in one forest and namespace element in another forest
 - 769 Trusted forest information was added
 - 770 Trusted forest information was deleted
 - 771 Trusted forest information was modified
 - 772 Certificate Manager denied a pending certificate request
 - 773 Certificate Services received a resubmitted certificate request
 - 774 Certificate Services revoked a certificate
 - 775 Certificate Services received a request to publish the certificated revocation list (CRL)
 - 776 Certificate Services publish the CRL
 - 777 A certificate request extension was made
 - 778 One or more certificate request attributes changed
 - 779 Certificate Services received a request to shutdown
 - 780 Certificate Services backup started
 - 781 Certificate Services backup completed
 - 782 Certificate Services restore started
 - 783 Certificate Services restore completed
 - 784 Certificate Services started
 - 785 Certificate Services stopped
 - 786 The security permissions for Certificate Services changed
 - 787 Certificate Services retrieved an archival file
 - 788 Certificate Services imported a certificate into the database
 - 789 The audit filter for Certificate Services changed
 - 790 Certificate Services received a certificate request
 - 791 Certificate Services approved a certificate request
 - 792 Certificate Services denied a certificate request
 - 793 Certificate Services set the status of a certificate request to pending
 - 794 The certificate manager settings for Certificate Services change
 - 795 A Configuration entry changed in Certificate Services
 - 796 A property of Certification Services change
 - 797 Certificate Services archived a log
 - 798 Certificate Services imported and archived a key
 - 799 Certification services published the certificate authority (CA) certificate to AD
 - 800 One or more rows have been deleted from certificate database
 - 801 Role separation enabled
 - 805 Event log service read the security log configuration for a session

APPENDIX B: REFERENCES

LAWS, DIRECTIVES, POLICIES, STANDARDS, AND GUIDELINES

Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, May 2003.

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003.

Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), *Core Set of Security Requirements*, February 2004.

Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000.

Director of Central Intelligence Directive 6/3 Policy, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999.

Electronic Government Act (P.L. 107-347), December 2002.

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (projected for publication December 2005).

Federal Information Processing Standards Publication 201, *Personal Identity Verification for Federal Employees and Contractors*, February 2005.

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

General Accounting Office *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999.

Information Technology Management Reform Act (P.L. 104-106), August 1996. International Organization for Standardization/International Electrotechnical Commission FDIS 17799, *Code of Practice for Information Security Management*, November 2004.

National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

National Institute of Standards and Technology Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, June 2004.

National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-40, *Procedures for Handling Security Patches*, August 2002.

National Institute of Standards and Technology Special Publication 800-42, *Guideline on Network Security Testing*, October 2003.

National Institute of Standards and Technology Special Publication 800-45, *Guidelines on Electronic Mail Security*, September 2002.

National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002.

National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (projected for publication spring 2005).

National Institute of Standards and Technology Special Publication 800-56, *Recommendation on Key Establishment Schemes*, (initial public draft) January 2003.

National Institute of Standards and Technology Special Publication 800-57, *Recommendation on Key Management* (draft), April 2005.

-
- National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.
- National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
- National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.
- National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004.
- National Institute of Standards and Technology Special Publication 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004.
- National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.
- National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.
- National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.
- Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
- Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model (v2.0)*, June 2003.
- Office of Management and Budget Memorandum 03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.
- Office of Management and Budget Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
- Office of Management and Budget Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.
- Paperwork Reduction Act of 1995 (P.L. 104-13), May 1995.

APPENDIX C: ACRONYMS

COMMON ABBREVIATIONS

CFR Code of Federal Regulations

CIO Chief Information Officer

CNSS Committee for National Security Systems

COTS Commercial Off-The-Shelf

ECAR™ ECC Enterprise Compliance Reporting and Auditing software

ECC Enterprise Certified Corporation

DCID Director of Central Intelligence Directive

FEA Federal Enterprise Architecture

FIPS Federal Information Processing Standard(s)

FISMA Federal Information Security Management Act

GLBA Gramm Leach Bliley Act

GOTS Government Off-The-Shelf

IEEE Institute of Electrical and Electronics Engineers

IPv6 Internet Protocol Version 6

MAC Media Access Control

MOA Memorandum of Agreement

MOM Microsoft Operations Manager

MOU Memorandum of Understanding

NIST National Institute of Standards and Technology

NSA National Security Agency

OMB Office of Management and Budget

SOX Sarbanes-Oxley Act

TCP/IP Transmission Control Protocol/Internet Protocol

USC United States Code

VPN Virtual Private Network

VOIP Voice Over Internet Protocol

