

Medicaid Enterprise System (MES) Procurement Project

Strategic Enterprise Advisory Services (SEAS)

T-8: Enterprise Data Security Plan

Version: 100

Creation Date: September 11, 2018

Created By: The SEAS Vendor

Submitted To: AHCA MES Project Management



Revision History

DATE	VERSION	DESCRIPTION	AUTHOR
6/28/18	001	T-8: Enterprise Data Security Plan Development Draft Version (Entry)	Andreas Casey
8/29/18	002	T-8: Enterprise Data Security Plan Revised to address Agency Review Comments	Rich Cefola / Paul Moore
9/11/18	100	T-8: Enterprise Data Security Plan Final Version	Sean Gibbs

Modifications to the approved baseline version (100) of this artifact must be made in accordance with the Change Control process that is part of the Scope Management Plan.

Quality Review History

DATE	REVIEWER	COMMENTS
7/24/18	Sean Gibbs	QA Review for initial submission
8/29/18	Scott Mildenerger	QA Review for second submission

Table of Contents

Section 1	Introduction.....	1
1.1	Background.....	1
1.2	Purpose	1
1.3	Scope Statement	2
1.4	Goals and Objectives.....	3
1.5	Referenced Documents	3
Section 2	Roles and Responsibilities.....	5
Section 3	Enterprise Data Security Plan Standards and Processes.....	7
3.1	Security Standards.....	7
3.2	CMS Security Requirements and Best Practices	7
3.3	Technology Standards Reference Guide	8
3.4	Security Standards Taxonomy	9
3.5	Security Governance and Standards Model.....	9
3.6	Standards Support.....	10
Section 4	Incident Reporting Process and Templates	12
4.1	Security Event Definition and Response Planning	12
4.2	Triage and Reporting	14
4.3	Incident Tracking Tool.....	16
4.3.1	Incident Tracking Tool Requirements.....	17
4.3.2	Incident Tracking Tool Selection and Implementation	17
4.3.3	Tracking System Security Policies and Practices.....	17
Section 5	Security Requirements Analysis.....	18
5.1	Analysis of Current State Controls	18
5.1.1	Agency Wide Governance	18
5.1.2	System Specific Analysis and Governance	19
5.1.3	Recommendations for Secure Development of MES Modules	21
5.2	Compliance Evaluation and Analysis	21
5.2.1	Certification and Accreditation	23
5.2.2	Risk Assessment	24

5.2.3	System Security Plan	24
5.2.4	Module Security Plan	24
5.2.5	Module Security Plan Document Requirements	24
5.2.6	Controls	27
5.2.7	Plan Maintenance	29
5.3	Module Development Security Life Cycle	29
5.3.1	Authorization to Operate	31
Section 6	Data Security Management and Reporting	33
6.1	MES Data Security Compliance Reporting.....	33
6.1.1	Project Specific Compliance Reporting	33
6.1.2	Cross Project Standards Compliance Reporting	34
6.1.3	Formal Reporting	35
6.2	Data Security Process and Criteria	35
6.2.1	Operational Security	35
6.3	Security Management Reports.....	36
6.3.1	Security Reporting Requirement Framework.....	36
6.3.2	Inventory of Security Reporting Requirements	36
6.4	Security Standards Update Process	37
Section 7	Appendix A – Supporting Attachments.....	39
	Attachment A – Security Standards Reference Guide	39
	Attachment B – CMS Risk Management Handbook (RMH) Incident Response Chapter	39
	Attachment C – CMS Standard System Categorization Worksheet	39
	Attachment D – CMS Example Memorandum of Understanding and Interconnection Security Agreement.....	39
	Attachment E – CMS Required Security and Privacy Control Baselines	40
	Attachment F – NIST CSF to NIST 800-53 and HIPAA Controls.....	40
	Attachment G – OWASP Application Security Verification Standard.....	40
	Attachment H – CMS Risk Management Handbook Vol I Chapter I – Risk Management in the XLC	40
	Attachment I – CMS Risk Management Framework Overview.....	40
	Attachment J – MES Systems Security Analysis	41

Reference to Other Deliverables.....	41
--------------------------------------	----

Table of Exhibits

Exhibit 1-1: Referenced Documents.....	4
Exhibit 2-1: Roles and Responsibilities	6
Exhibit 3-1: TSRG Standards Hierarchy	8
Exhibit 3-2: Security Governance Model	10
Exhibit 4-1: Security Event Categorizations.....	14
Exhibit 4-2: Example Security Event Notification Flow.....	16
Exhibit 5-1: FMMIS Connected System Governance.....	21
Exhibit 5-2: System Delivery Management Security Phases	22
Exhibit 5-3: Security Artifacts Produced System Delivery Management Stage	23
Exhibit 5-4: NIST Cyber Security Framework	28
Exhibit 5-5: Security Control Implementation Life Cycle	29
Exhibit 5-6: NIST Risk Management Framework.....	31
Exhibit 5-7: Testing and Certification Requirements by SDLC Phase.....	31
Exhibit 6-1: Security Reporting Requirement Framework	36
Exhibit 6-2: Security Reporting Requirements	37
Exhibit 6-3: Security Standards Refresh Events	38

SECTION 1 INTRODUCTION

1.1 BACKGROUND

The Florida Agency for Health Care Administration (Agency) is preparing for the changing landscape of health care administration and increased use of the Centers for Medicare and Medicaid Services (CMS) Medicaid Information Technology Architecture (MITA) to improve the administration and operation of the Florida Medicaid Enterprise. The current Florida Medicaid Enterprise includes services, business processes, data management and processes, technical processes within the Agency, and interconnections and touch points with systems that reside outside the Agency necessary for administration of the Florida Medicaid program. The current Florida Medicaid Enterprise System (MES) includes the Florida Medicaid Management Information System (FMMIS), Decision Support System (DSS), and other systems operated by different vendors. These systems in the MES interface primarily through the exchange of data files via Secured File Transfer Protocol. These point-to-point interfaces become more complex and costly as the number of systems and applications increase. The future of the Florida Medicaid Enterprise integration is to allow Florida Medicaid to secure services that can interoperate and communicate without relying on a common platform or technology. Connecting services and infrastructures, and developing integration standards are the next steps for advancing the MES level of MITA maturity and system modularity modernization.

The CMS released the Medicaid Program Final Rule: Mechanized Claims Processing and Information Retrieval Systems in December 2015. This final rule modifies regulations pertaining to 42 Code of Federal Regulations (CFR) 433 and 45 CFR 95.6111, effective January 1, 2016. Among other changes, this final rule supports increased use of the MITA Framework. MITA is a CMS initiative that fosters an integrated business and information technology (IT) transformation across the Medicaid enterprise to improve the administration and operation of the Medicaid program. The Agency documents its high-level plans to increase service interoperability and advance the maturity of the MES in accordance with the MITA Framework in the Florida MES Procurement Strategy document.

Per the MITA Framework, the security and privacy of the Medicaid Enterprise System is a requirement to protect the users and data stored within the system. Effective management of risk, technical security, and privacy requires controls, processes, and an implementation and maintenance life cycle that are consistent across modules. These components must be clearly defined and executed by staff trained and knowledgeable in the areas of healthcare IT, enterprise risk management, security event management, and system security plan development.

1.2 PURPOSE

Establishing standards for controls, technology, and capabilities, diminishes risk, reduces the threat surface, and increases the confidentiality, integrity, and availability for the MES. The T-8 Enterprise Data Security Plan (EDSP) is the information and technical security strategy guiding secure development of the MES modules, and describes the security architecture, life cycle,

and processes used to satisfy Federal and State regulations, industry standards, and Agency policy.

1.3 SCOPE STATEMENT

The scope of the EDSP organizes security information for the secure development and operation of MES modules, to include:

- Policy guiding security decisions for Florida Agency for Health Care Administration (AHCA) and Centers for Medicare and Medicaid Services (CMS)
- Control objectives identified in Federal and State regulations
- Technical standards established by the National Institute of Standards and Technology (NIST) and other industry standards according to technical domains
- Procedures defined by specific management plans for the MES Project into a single reference source for the secure planning, development, implementation, and oversight of the MES Project modules.

The scope for each section is as follows:

- **Section 1 Introduction** – Outlines the background, purpose, scope statement, goals and objectives, and reference documents used to prepare the deliverable.
- **Section 2 Roles and Responsibilities** - Lists the responsibilities of each of the MES stakeholders during the design and implementation phases of the project.
- **Section 3 Enterprise Data Security Plan Standards and Processes** - Describes applicable security related standards and how they intersect across the bodies such as market, industry, CMS, Agency for State Technology (AST), Agency and MES project specific.
- **Section 4 Incident Reporting Process and Templates** - Outlines the process to manage cyber security and HIPAA incident/breach investigations, resolution management, and reporting in coordination with the Agency's Information Security Manager (ISM) and the Agency's Health Insurance Portability and Accountability Act of 1996 (HIPAA) Compliance Office.
- **Section 5 Security Requirements Analysis** - Defines the life cycle for evaluating and analyzing the security compliance of MES modules, will document the process for determining corrective actions, and prescribe at what levels to grant an Interim Authority to Operate (IATO).
- **Section 6 Security Management and Reporting** - Describes the process for reporting enterprise security management to the enterprise governance board and defines the catalog of reports to be included with reporting.

1.4 GOALS AND OBJECTIVES

- **Goal #1 – Secure MES Module Development.** The following objectives guide success toward this goal:
 - › Objective #1 – Define governing security frameworks and industry standards
 - › Objective #2 – Define CMS, State, and Agency checklists for development
 - › Objective #3 – Develop and maintain security life cycle to validate compliance with security and privacy requirements during development
- **Goal #2 – Effective and Efficient Security Event Management.** The following objectives guide success toward this goal:
 - › Objective #1 – Identify Incident Management key personnel and required security roles for MES module vendors
 - › Objective #2 – Define process for monitoring and reporting incidents in accordance with State and Agency policy and procedures
- **Goal #3 – Secure MES Module Operation.** The following objectives guide success toward this goal:
 - › Objective #1 – Objective and consistent MES Module security assessment for issuing Interim Authority to Operate (IATO)
 - › Objective #2 – Actionable security intelligence reporting framework and enforcement system
 - › Objective #3 – Periodic operational certification of MES Module use of current secure technology, governance, and standards

1.5 REFERENCED DOCUMENTS

Exhibit 1-1: Referenced Documents lists the documents referenced to support development of this deliverable.

NAME	DESCRIPTION	GOVERNING BODY	STATUTORY REFERENCE
Security Standards for the Protection of Electronic Protected Health Information	Commonly referred to as HIPAA Security Rule . Provides specific standards and safeguards for health information protection	Federal Government	45 CFR Part 164, Subpart C
Federal Information Security Modernization Act of 2014	Establishes the Secretary of Homeland Security as the responsible party to implement policies and practices to secure Federal information systems.	Federal Government (Department of Homeland Security)	S.2521 of the 113 th Congress to amend Chapter 35 of Title 44, United States Code
Federal Information Processing Standards	Sets the approved technical standards and guidelines for federal information systems.	Federal Government (NIST)	S.1124 of the 104 th Congress - Information Technology Reform Act of 1996

NAME	DESCRIPTION	GOVERNING BODY	STATUTORY REFERENCE
Medicaid Information Technology Architecture (MITA) Framework	Provides authority for states to receive enhanced federal funding by developing highly interactive and interoperable MES platforms.	Federal Government (Centers for Medicare and Medicaid Services (CMS))	Affordable Care Act: Medicaid Program: Federal Funding for Medicaid Eligibility Determination and Enrollment Activities (CFR Vol. 76, No. 75)
Florida Cybersecurity Standards	Establishes the Florida Cybersecurity Standards (FCS), the minimum standards for state agencies to secure IT resources. Uses the NIST CSF and Federal Information System Management Act (FISMA) as guiding documents.	State of Florida	Florida Administrative Code 74-2.001 through 74-2.006
Florida Technology Architecture Standards – Identity Management	Creates the Identity Management Services framework to provide secure, reliable, and interoperable mechanisms for authenticating the identity of devices, application services, and users that consume state information and application resources. This rule is modeled after the Identity Ecosystem Framework Baseline Functional Requirements v1.0	State of Florida	Florida Administrative Code 74-5.003
SEAS Contract	Authorizes Florida Agency for Health Care Administration to expend funds in support of developing the strategy and governance for the State's MES transition.	Florida Agency for Health Care Administration	SEAS Contract MED-191

Exhibit 1-1: Referenced Documents

SECTION 2 ROLES AND RESPONSIBILITIES

This section identifies the roles and responsibilities for the primary stakeholders that maintain or use this document.

ROLE	RESPONSIBILITY
Agency Information Security Manager	<ul style="list-style-type: none"> ▪ Evaluate and track incident reports from MES Project Vendors and initiate CSIRT process when necessary per FL Administrative Code Rule 74-2.005. ▪ Coordinate with Agency for State Technology and Florida Department of Law Enforcement during CSIRT events ▪ Review procurements and provide security review and ratings of responses to solicitations ▪ Provide security assessment input and recommendation to Agency Information Technology Director / Chief Information Officer for Interim Authority to Operate (IATO) and final Authorization to Operate (ATO) for MES Modules
Agency Director, Information Technology/Chief Information Officer	<ul style="list-style-type: none"> ▪ Advocate and fund information security requirements during budget planning and execution to support MES Module development ▪ Coordinate with Agency, Agency Information Security Manager and SEAS Vendor to establish workflow and touchpoints for use of Agency security tools and processes
SEAS Vendor	<ul style="list-style-type: none"> ▪ Ensure tools and processes are in place for the execution of the MES Enterprise Data Security Plan. ▪ Develop a SEAS Management Plan and SEAS integrated processes ▪ Coordinate integrated security processes ▪ Administer security assessment processes ▪ Develop adequate system security training for MES Project Vendors on Project Standards, Integrated Processes, and Design and Implementation Standards ▪ Acquire and implement data security tracking tool ▪ Transfer ownership of tracking tool to the Agency ▪ Utilize the approved tracking tool and templates and provide documented analyses, corrective action requirements, recommendations, and resolutions from enterprise data security management ▪ Produce timely and accurate status reporting including implementation status reporting of MES projects and services. ▪ Develop templates for managing cyber security and HIPAA incident/breach investigation and resolution management reporting ▪ Develop and document a process to report on enterprise data security management and reporting results at enterprise governance ▪ Provide standards support and expertise throughout the MES Project

ROLE	RESPONSIBILITY
MES Project Vendors	<ul style="list-style-type: none"> ▪ Assign principal Module Security Officer (MSO) to manage module security and reporting ▪ Maintain module security profile and role-based security for review by CMS, State, external, and internal auditors ▪ Maintain Plan of Actions and Milestones (POA&M) for module updates and ATO/IATO compensating controls ▪ Create Security Event Response Team with key personnel and backups ▪ Capture, organize, and triage information in support of Agency CSIRT efforts ▪ Provide scheduled and ad hoc reporting during CSIRT activities ▪ Provide security and privacy continuing education and awareness to module operational support team ▪ Review and report vulnerabilities and remediation plans to Agency management on scheduled and ad hoc basis ▪ Maintain personnel suitability standards regarding data access, authorization, and module development
Integration Services / Integration Platform (IS/IP) Vendor	<ul style="list-style-type: none"> ▪ All responsibilities described for MES Project Vendors are applicable for the Integration Platform implemented by the IS/IP vendor ▪ Implement and operate the enterprise level role based SSO/authentication solution ▪ Support MES Project Vendors in implementing secure technical integration and interoperability between systems and modules
Medicaid Fiscal Agent Organization (MFAO)	<ul style="list-style-type: none"> ▪ Oversee and approve access for AHCA staff and external organizations
MES IV&V Vendor	<ul style="list-style-type: none"> ▪ Provide independent, objective assessments of project processes and report observations to appropriate level of governance as defined in the Strategic Enterprise Governance Plan to facilitate informed decision-making regarding system development and deployment ▪ Independently Monitor MES CMS Certification status and report certification progress to CMS ▪ Validate the project has the strategy, management backing, resources, skills, and incentives necessary as defined and approved by the Agency in MES project deliverables for an effective project. ▪ Evaluate project progress, resources, cost, schedules, work flow, and reporting; evaluate project reporting process and actual project reports to verify project status is accurately traced using project metrics ▪ Validate the project's organizational structure supports training, process definition, independent Quality Assurance, Configuration Management, product evaluation, and any other functions as defined and approved by the Agency in MES project deliverables for the project's success

Exhibit 2-1: Roles and Responsibilities

SECTION 3 ENTERPRISE DATA SECURITY PLAN STANDARDS AND PROCESSES

3.1 SECURITY STANDARDS

Security standards play an important role in implementing secure systems that protect data privacy. Security Standards are a set of rules to make decisions about security related technology solutions. These security standards guide the implementation of MES Projects.

This section describes the framework of applicable security related standards and how they intersect across the bodies such as market, industry, CMS, AST, Agency and MES project specific and align to the security topics of:

- Data Security
- Identity and Access Management/SSO
- Role based access authorization, auditing and credentialing
- Platform Security
- Software Security

3.2 CMS SECURITY REQUIREMENTS AND BEST PRACTICES

CMS Security Requirements provide substantial guidance on applicable security standards that will be relevant to MES Projects and eventual Authority to Operate and system certification.

The [CMS Information Security \(IS\) Acceptable Risk Safeguards \(ARS\)](#) is a comprehensive information security document put forth by the Centers for Medicare and Medicaid Services (CMS) outlining broad-based, best practices for CMS information systems. Additionally, the document utilizes the NIST SP 800-53 Revision 3 "Recommended Security Controls for Federal Information Systems" publication and other departmental specific documents as guidance in regard to information security.

Another important document is the [CMS System Security Plan \(SSP\) Procedure](#), which details the relevant procedures that have been developed to provide the applicable CMS Business Owners with the necessary tools in determining, implementing and documenting one's current level of information security (IS) controls throughout the life-cycle of its system. Source: www.cms.gov.

Together, the CMS Information Security (IS) Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR) and the CMS System Security Plan (SSP) Procedure publication seek to implement best-practices for an organization's information security framework, one that ultimately helps ensure the safety and security of critical system resources.

3.3 TECHNOLOGY STANDARDS REFERENCE GUIDE

SEAS Deliverable T-6 Technology Standards Section 4 Technology Standards Reference Guide (TSRG) defines technology standards and the purpose of the TSRG. The TSRG is the repository of data, project management, security, and technology standards applicable to the administration and operation of the enterprise and future state enterprise. Content in the TSRG is in a SharePoint list in the MES Projects Repository, which adheres to the MITA Framework.

The TSRG contains a collection of standards that originate from many sources. **Exhibit 3-1: TSRG Standards Hierarchy** shows the types of organizations that are sources of relevant security standards.

Often standards of different organizations are aligned and consistent. Higher-level organizations may adopt lower level standards or provide guidance that is more specific to the enterprise, organization, or system. In some cases, standards may conflict, or an organization may provide guidance that certain standards are waived or not applicable. The TSRG seeks to help stakeholders understand not only the universe of applicable standards, but also to provide the structure to harmonize conflicting standards or guidance.

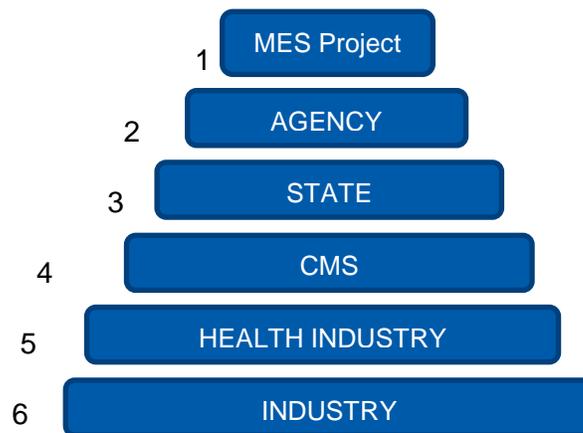


Exhibit 3-1: TSRG Standards Hierarchy

The Florida Medicaid TSRG has a unique field called “Precedence” that will enable users and MES Project Vendors to understand which standards are applicable when multiple standards exist for a security component or topic. **Exhibit 3-1: TSRG Standards Hierarchy** displays the correlation between the Precedence and the types of rulemaking bodies.

When competing standards exist, a Precedence value will be set on each entry with the highest precedence value (1 being the highest) reflecting the most important guidance. This will allow the MES Project Vendors or other users to see if there are competing standards and understand the order of importance.

3.4 SECURITY STANDARDS TAXONOMY

A security standards taxonomy is a hierarchical structure separating data into specific classes or categories based on common characteristics. The taxonomy provides a conceptual framework for discussion, analysis, or information retrieval. SEAS Deliverable T-6 Technology Standards Section 4: Technology Standards Reference Guide defines the guide and the taxonomy for technology, security, and data standards. Security standards use the following taxonomy in the TSRG on the MES Projects Repository:

- Security standard definitions used in system delivery management.
 - › These are security standards used in system delivery management. Appendix A – Security Standards Reference Guide contains an extract of security standards from the TSRG.
 - › Domain: Technical
 - › Area: Security
 - › Category: Include the topics such as:
 - › Data Security
 - › Identity and Access Management/SSO
 - › Role based access authorization, auditing and credentialing
 - › Platform Security
 - › Software Security

3.5 SECURITY GOVERNANCE AND STANDARDS MODEL

Exhibit 3-2: Security Governance Model shows the overarching standards that guide secure MES module development and operation.

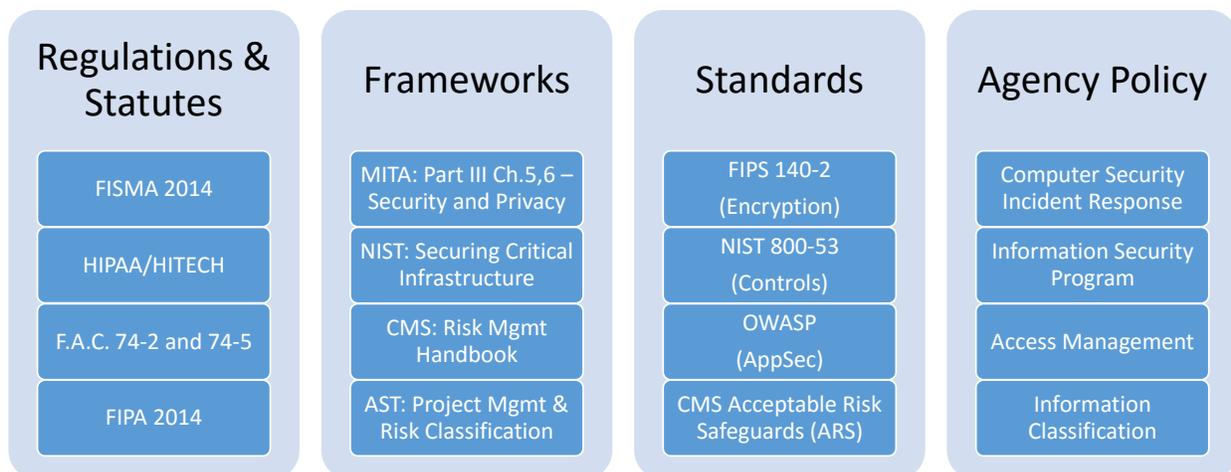


Exhibit 3-2: Security Governance Model

Attachment A - Security Standards Reference Guide contains the detailed list of specific standards governing development of MES modules.

3.6 STANDARDS SUPPORT

The SEAS Vendor will support the use of the security standards by the Agency and MES Project Vendors for the implementation of MES Projects. For the security standards, the SEAS Vendor will:

- use the common processes defined for all technology standards
- provide technical expertise relevant to the security category of technology standards

Using the combination of common technology standards processes and providing relevant technical expertise will help the SEAS Vendor guide the MES Project Vendors and ultimately the Agency implement MES projects to achieve the MES strategic vision.

The approach taken for the security standards is consistent with the approach used for other types of technology standards. The SEAS vendor is documenting and communicating the relevant security standards that have been identified originating from many sources including Agency contract language, Agency standards, AST, State, CMS, and industry sources. The TSRG is the repository of applicable standards with indications of precedence to harmonize competing or conflicting standards. The standards listed in the TSRG in most cases are collections of discrete standards. (e.g., the TSRG includes an entry to comply with NIST as opposed to documenting each discrete NIST standard's applicability). This approach is maintainable for the Program and sets the expectations for vendors to comply with standards from multiple sources as those standards evolve. The TSRG includes a compliance approach for each standards entry which describes the basis for compliance assessment to the vendor.

The SEAS vendor recommendation is that this document and the TSRG not provide a prescriptive list of discrete security requirements that elaborates requirements originating or grouped by source. Providing detail prescriptive requirements is not a CMS recommendation, is uncommon in the market, not consistent with other state MMIS procurements, increases vendor response costs discouraging responses and competition, and extends procurement timeframes. Specifying discrete requirements would likely have minimal net risk reduction to the Agency and may increase liability to the Agency if the requirements change, are misstated, or omitted. There are many processes to ensure implemented systems are secure including requirements to produce security related artifacts throughout the lifecycle including the security certification and accreditation processes, risk assessment (RA) processes, and system security plan (SSP) processes. Additionally, the Medicaid Enterprise Certification Life Cycle (MECL) processes include checklists and processes to assess and reduce security risk.

The SEAS Vendor will use the common technology standards processes to define, secure governance approval, maintain, communicate, provide ad hoc support, assess compliance, and report standards compliance to the Agency. Following consistent processes used for other categories of MES technology domain standards improves consistency, efficiency, understanding, and communication. Specifically, the SEAS Vendor will use the processes and procedures in the SEAS T-6: Technology Standards deliverable and in T-6: Technology Standards Attachment E - *Technology Standards Communication, Support, Compliance, and Compliance Reporting Procedures*.

SECTION 4 INCIDENT REPORTING PROCESS AND TEMPLATES

The incident reporting and process section describes the process and guidance for the reporting of cyber security and HIPAA incident/breach investigation. It provides a consolidated directive and describes the applicable tooling to manage security incidents. The determination of tooling will be decided through the course of discovery by the combined team. Content in this section:

- Describes the current processes of Enterprise System and Data Security and governance organization
- Describes the Agency, Departments, external organizations, and roles within the context of Enterprise System and Data Security and their responsibilities
- Define the current and future process, templates and tools used for incident reporting of security incidents
- Plan for transition from current to future state incident reporting and management processes

4.1 SECURITY EVENT DEFINITION AND RESPONSE PLANNING

The scope of this section is incident reporting activities. The security processes for Certification and Accreditation, Risk Assessment (RA) and System Security Plan (SSP) address other security related success factors, activities and controls.

A Security Event is the suspected unauthorized acquisition, access, use, disclosure, modification, or destruction of information, or the interference with system operations in an information system. Additionally, an event is the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical information intended for use in the information system. A data breach is an event in which sensitive, protected or confidential information is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Florida Statutes (Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)) and federal regulations, including the federal HIPAA breach notification rule provide guidance on data breach. These events have the potential to put data at risk of unauthorized acquisition, access, use, disclosure, modification, or destruction. The MES Project Vendors shall evaluate Security Events and triage for reporting to the Agency's Information Security Manager (ISM), and potential activation of the Agency's Computer Security Incident Response Team (CSIRT), as needed.

Exhibit 4-1: Security Event Categorizations shows examples of Security Events and corresponding reporting requirements. The reporting timeframes listed below are for security events. The Agency enters into a Business Associate Agreement (BAA) with vendors. The provisions of the BAA apply to HIPAA requirements. Reporting timeframes for security events and BAA provisions are different which is known and acceptable to the Agency.

CATEGORY	NAME	DESCRIPTION	REPORTING TIMEFRAME TO AGENCY ISM
CAT 0	Exercise/Testing	Used during Federal, State, and Agency exercises and approved testing activities of defenses and responses	N/A: for internal use during exercises
CAT 1	Unauthorized Access	Logical or physical access to information or information assets, without authorization	Within one (1) hour of detection
CAT 2	Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources	Within two (2) hours of detection if the attack is ongoing, and MES Module vendor is unable to successfully mitigate activity
CAT 3	Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects an information asset	Within one (1) hour of detection if code is not contained with a quarantine program, or cleaned with an anti-malware program <i>*MES Project Vendors are NOT required to report malicious logic that has been successfully quarantined by anti-malware software</i>
CAT 4	Inappropriate Use	Individual violation of appropriate use policy of any MES Module information asset	Cumulative weekly report. Repeat offenders shall be identified, and a remediation plan documented to prevent future violation
CAT 5	Scans/Probes/ Attempted Access	Activity that seeks to access or identify open interfaces, active protocols, or other exploits of MES Module information assets, AND does NOT result in compromise or denial of service.	Monthly on an agreed to schedule
CAT 6	Investigation	Open reviews of suspicious activity that the MES Module Vendor is actively collecting evidence and evaluating but has not yet confirmed as a Security Event.	Weekly on an agreed to schedule
PII	Personally Identifiable Information (PII) Exposure	Any information that potentially identifies and distinguishes a specific individual and can be used to de-anonymize anonymous data.	Within 1 (one) hour of detection regardless of the category of the accompanying Event
PHI	Protected Health Information (PHI) Exposure	Any health information created or received by a provider, plan, employer, insurer, school, or clearinghouse that relates to the physical or mental health or condition of any specific and individually identifiable individual, or the payment for the provision of health care to a specific individually identifiable individual.	Within 1 (one) hour of detection regardless of the category of the accompanying Event
PIFI	Personally Identifiable Financial Information (PIFI) Exposure	Any financial information that an individual provides to a financial institution that is not publicly available to include bank and credit card information.	Within 1 (one) hour of detection regardless of the category of the accompanying Event

Exhibit 4-1: Security Event Categorizations

A defined Security Event Response Plan (SERP) supports systematic and consistent identification, handling, evaluation, and escalation of anomalous events within the MES Modules. Event management minimizes lost information, speeds triage, reduces outages, and increases organizational knowledge to prevent future events and incidents.

The Agency maintains the Computer Security Incident Response Team (CSIRT) process, which defines containment, remediation, notification, law enforcement and oversight coordination, and public communications. The MES Project Vendor is responsible for notifying and providing the Agency ISM with the necessary information to activate the CSIRT team and maintaining constant contact and availability during a Security Incident to support any additional information gathering and forensic activities as needed.

MES Project Vendors shall document, submit to the ISM, and maintain a formal and approved SERP that includes the following components:

- Assignment of a single individual, with appropriate backup, as the Module Security Event Manager (SEM) to serve as the point of contact for all communications and reporting between the Module Vendor and the Agency ISM
- Key personnel roster with roles and responsibilities for a Security Event
- A triage workflow and procedures to follow during a Security Event
- Annual testing and training plan for Security Events response to include awareness and desktop walkthrough events with key personnel
- Documented and validated physical, logical, and administrative controls to detect activity that requires additional investigation
- Evaluation matrix to determine whether to notify the Agency's ISM of a potential Security Incident

The Agency will allow the MES Project Vendors to respond with SERP templates based on best practices and expertise. Once a template is approved, the template will be added to the Enterprise Data Security Plan for future MES Project Vendors to use as a standard.

It is highly recommended that MES Module Vendors model the SERP and its components on the [NIST 800-61](#): Computer Security Incident Handling Guide.

4.2 TRIAGE AND REPORTING

Triage during a Security Event captures necessary information and provides a framework for making efficient and effective decisions regarding next steps required. The Agency ISM will also require this information for reporting and coordination with Federal and State Agencies if the Security Event escalates to a Security Incident. During a Security Event, the MES Module Vendor shall capture and record **at least** the following information:

- Source of event

- Classification of information at risk
- Type of event
- Scope of assets related to the event
- Impact to operations
- Time of event
- All evidence captured
- Chain of custody for all evidence captured
- Initial perceived categorization

Exhibit 4-2: Example Security Event Notification Flow is an example workflow with acceptable information gathering and evaluation criteria. This workflow is not meant to be prescriptive, but rather demonstrate the level of detail and structure that the Project Vendors' Event Management should contain.

The Agency will allow the MES Project Vendors to respond with Security Event Notification Flow processes based on best practices and expertise. Once a process is approved, the process will be added to the Enterprise Data Security Plan for future MES Project Vendors to use as a standard.

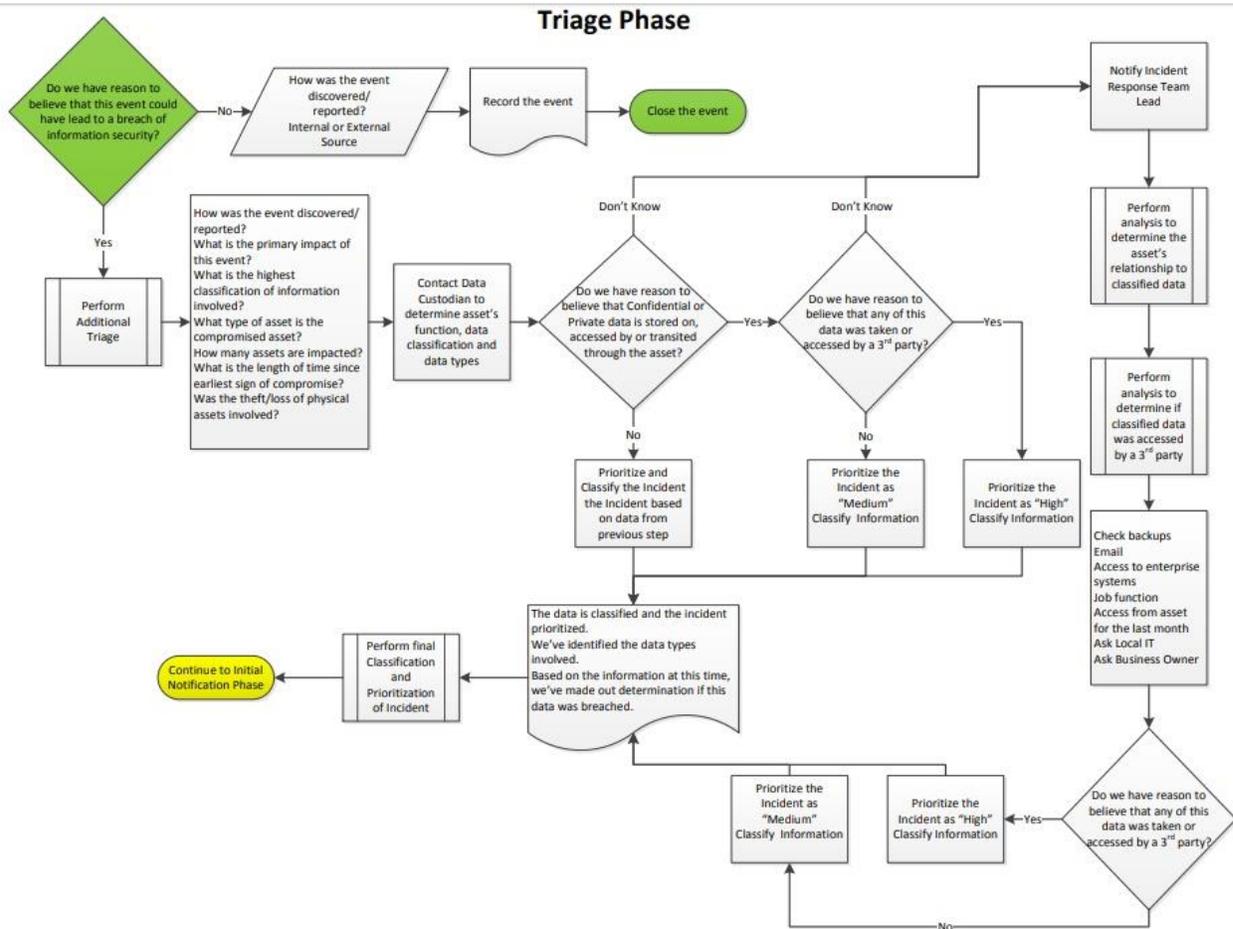


Exhibit 4-2: Example Security Event Notification Flow

Attachment B contains the CMS Incident Handling Template.

4.3 INCIDENT TRACKING TOOL

The Agency currently uses an Agency SharePoint site and internal communications during a verified Incident, and tracks activities, communications, actions, and decisions using existing office tools and manual routing workflows. This existing tool infrastructure and workflow capabilities are inadequate to support the Event Management process that requires all MES Project Vendors to submit all qualified events to the ISM for evaluation.

Immediate capability requirements for development include:

- Event Management portal for MES Project Vendors to submit Event Management information and evidence
- Business rules for notifications and workflows

- Reporting capabilities for status updates during CSIRT activation

4.3.1 INCIDENT TRACKING TOOL REQUIREMENTS

Future support for the Event Management process requires automated notification and workflow routing, secure evidence chain of custody management, and development of scalable interfaces to security information and event management detection, monitoring and investigation tools. MES Project Vendors shall ensure their Event Management processes and capabilities are regularly maintained and updated to provide the most accurate and timely information available to the Agency's Incident Management platform as it develops and matures.

4.3.2 INCIDENT TRACKING TOOL SELECTION AND IMPLEMENTATION

During the FY18-19, the SEAS Vendor will work with the Agency to select a product that meets the incident tracking tool requirements. Selection, development and implementation are to include developing templates for managing cyber security and HIPAA incident/breach investigation and resolution management and reporting, in coordination with the Agency's ISM and the Agency's HIPAA Compliance Office, respectively.

4.3.3 TRACKING SYSTEM SECURITY POLICIES AND PRACTICES

An additional use of the incident tracking tool(s) is to support analysis of systems within the MES and MES vendor security policies and practices. The SEAS Vendor shall utilize the implemented incident tracking tool and templates and provide documented analyses, corrective action requirements, recommendations, and resolutions resulting from enterprise data security management.

On an ongoing basis, the Agency should review the vendor's security posture as is incorporated in the AHCA standard procurement language.

SECTION 5 SECURITY REQUIREMENTS ANALYSIS

Standardized security requirements for development and operations of MES Modules consist of fundamental components designed to implement controls and reduce risk. These components include:

- Existing Agency security program, comprised of personnel, processes, and tools specifically employed to provide controls that reduce risk of exposure or data exfiltration.
- Documentation detailing the security controls, key personnel, and risk assessments for issuing Interim and Final Authority to Operate (ATO)
- Module Security Plan (MSP)
- Process for evaluating compliance with Federal, State, and Agency regulations, rules, and policies

5.1 ANALYSIS OF CURRENT STATE CONTROLS

The current Florida Medicaid Management Information System (FMMIS) is an Agency Owned / Contractor Operated (AO/CO) closed system governed by Service Level Agreements. The DXC Corporation (formerly Hewlett-Packard Enterprise) maintains the security operations for the FMMIS and provides AHCA with periodic reports on security compliance and security events.

The security controls for the FMMIS system are documented in the CMS System Security Plan (SSP). The SEAS vendor was not provided access to this document. The Agency is required to produce an SSP with appropriate controls for new modules replacing the FMMIS system. The SSP would document controls used and carried forward to MES vendors.

AHCA maintains access control to FMMIS using the Medicaid Enterprise User Provisioning System (MEUPS).

In addition to the FMMIS, the MES interfaces and exchanges data with downstream systems to support internal and external business operational requirements. The following sections outline the existing systems that interface with the FMMIS. The MES Project Vendors shall consider these systems when designing security controls for MES Modules.

5.1.1 AGENCY WIDE GOVERNANCE

The Florida Agency for Health Care Administration maintains Agency-wide security policies and guidance for the secure development, operation, and reporting of security systems.

Existing Agency policies are located on the AHCA Portal Site within the Policies and Procedures section.

5.1.2 SYSTEM SPECIFIC ANALYSIS AND GOVERNANCE

There are currently multiple existing systems operated by multiple vendors that comprise the Medicaid Enterprise System. The existing systems were implemented prior to the development of Strategic, Programmatic and Technology strategy, standards and guidance developed by the SEAS Vendor. The SEAS Vendor reviewed Agency-provided information about the existing systems. The provided information primarily included information gathered through interviews with security or system project leads. The SEAS Vendor did not perform independent vulnerability assessments, reviews of system specific security controls and other vulnerability activities performed in system audits and assessments. The SEAS Vendor also did not receive access to review system specific audit reports containing system specific vulnerabilities or system specific controls findings. The Agency and vendors that operate specific systems control and address system specific audit reviews and findings. To protect the Agency and specific systems from exploitation of vulnerabilities, this document does not describe system specific analysis of vulnerabilities or control deficiencies.

However, the analysis of existing MES systems produced:

- a summary of governance for FMMIS connected systems (below)
- recommendations for secure development of modules
- inputs to the security standards (documented in the TSRG and Appendix A)

5.1.2.1 MES SYSTEMS SECURITY ANALYSIS ATTACHMENT

The SEAS Vendor will provide a current security analysis of MES systems as an attachment to this document. Attachment J provides a link to the attachment document with a very high level structure of analysis content. The SEAS Vendor will populate the attachment and produce subsequent iterations of the attachment throughout the life of the MES Program.

The analysis includes the inventory and review of existing security policy and artifacts generated by 3rd party security assessments and audits aligned to these systems. Analysis shall promote:

- Findings for posture improvement related to incorporating enterprise security initiatives and risk mitigation identified by audits and external assessments
- Recommendations and follow-up to support improved security posture for future MES module procurement

For new and updated systems, the SEAS vendor will perform an analysis of system and MES vendor security policies and practices. The analysis of new and updated systems will have access to security artifacts produced during the system development life cycle.

5.1.2.2 GOVERNANCE ANALYSIS

Exhibit 5-1: FMMIS Connected System Governance lists systems and additional controls in addition to Agency wide controls that connect and share data with the FMMIS.

SYSTEM NAME	ACCESS MANAGEMENT	DATA TYPES PROCESSED OR STORED	GOVERNING CONTROLS	INHERITED CONTROL ENVIRONMENT
Florida Medicaid Management Information System (FMMIS)	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII PHI	Currently designed, developed, implemented by DXC. Logging and reporting provided as necessary.	DXC Data Center
Enrollment Broker System	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII PHI	Currently designed, developed, implemented by DXC. Logging and reporting provided as necessary.	DXC Data Center
Third Party Liability	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII PHI	Not available	Not available
Prior Authorization	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII PHI	Not available	Not available
Provider Data Management System	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII	Currently designed, developed, implemented by DXC. Logging and reporting provided as necessary.	DXC Data Center

SYSTEM NAME	ACCESS MANAGEMENT	DATA TYPES PROCESSED OR STORED	GOVERNING CONTROLS	INHERITED CONTROL ENVIRONMENT
Health Quality Assurance (HQA) Licensure VERSA	Standalone Security DB	PII	Not available	AST Data Center
Home Health Electronic Visit Verification System	Standalone Security DB	PII PHI	Not available	Not available
Care Provider Background Screening Clearinghouse	Standalone Security DB	PII	Not available	AST Data Center

Exhibit 5-1: FMMIS Connected System Governance

5.1.3 RECOMMENDATIONS FOR SECURE DEVELOPMENT OF MES MODULES

The following are recommendations for developing MES Modules that use all Agency process and resources:

- Evaluation of MES Modules using the Agency’s a Vulnerability Management platform or Agency recommended secure development evaluation tool or service throughout the development life cycle
- Evaluation of MES Modules using the Application Security Testing platform early in the development life cycle, and after any significant changes
- Continuous engagement with Agency ISM to ensure awareness of new tools and processes

This recommendation continues to have vendors primarily responsible for secure development. Responsibility for secure development does not mean delegation of security governance and responsibility for security control selection by project vendors, without any provision for direct oversight by the Agency other than receiving reports of some kind from the project vendor. MES modules are expected to have security controls consistent with those used for FMMIS. The SEAS Vendor will provide review, standards guidance, compliance assessment and compliance reporting.

The Agency will continue to mature its security processes and procedures according to the AHCA Security Program roadmap and communicate with MES Project Vendors any updates that affect development or operations of MES Modules.

5.2 COMPLIANCE EVALUATION AND ANALYSIS

This section describes the processes to evaluate and analyze vendor compliance with security standards, requirements and guidance. The focus of this section is primarily on compliance

activities related to system delivery management stages up to and including the Implementation phase. The Operations and Maintenance phase includes ongoing audits with security compliance evaluation. The Agency Director, Information Technology/Chief Information Officer and Agency IT are the coordination point for Enterprise security audits.

CMS provides significant guidance on the security compliance evaluation phases and activities in the system development life cycle. The MES Program will align with the major security compliance and evaluation processes defined by CMS. This section elaborates additional security compliance evaluation and analysis guidance specific to the MES Program’s modular solution implementation.

The security phase processes of the project life cycle include major security compliance related processes (defined by CMS) that produce important security compliance artifacts and reports. The primary security phases overlap with the phases of system delivery management stage and include the:

- Certification and Accreditation phase process
- Risk Assessment (RA) process
- System Security Plan (SSP) process

Exhibit 5-2: System Delivery Management Security Phases depicts the phases of each of the major security phase processes and their overlap with system delivery management phases.

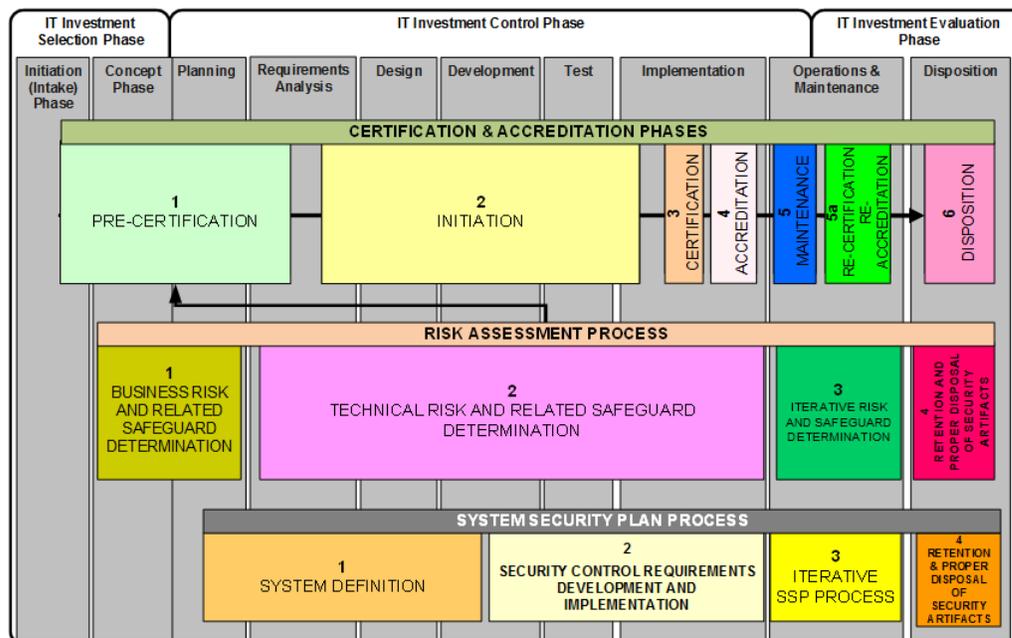


Exhibit 5-2: System Delivery Management Security Phases

The enterprise security group members will participate and or review the artifacts produced during the security phases. They will have access to detailed content which articulate security standards compliance and controls specific to a system. The Risk Assessment and System Security Plans are significant artifacts that report much of the information of interest to enterprise security governance group members.

The Security Phases of the system delivery produce security artifacts used to evaluate compliance with security standards. The MES Program security artifacts align to the CMS security artifact template names to simplify data sharing with CMS and other states. CMS categorizes the artifacts produced as security artifacts and security information from tasks. Information about each artifact type (e.g. description, templates, available samples) are listed in the [Project Life Cycle Artifacts](#) on the MES Project Repository. The template for each artifact type originates from the corresponding CMS XLC template. Security templates will evolve with MES specific customizations throughout the Program.

PHASES		Initiation	Concept	Planning	Requirements Analysis	Design	Development	Testing	Implementation	O&M*	Disposition
ARTIFACTS/ INFORMATION	REVIEWS	AR	ISR	PBR	RR	PDR DDR	ERR1 (VRR)	ERR2 (IRR) ERR (PRR)	ORR	PIR, AOA	DR
System Security Category		P/F									
Privacy Impact Assessment		P	I	I	I	I	I	F		U	
System Security Plan			P	B	I	I	I	F		U	U
Module Security Plan			P	B	I	I	I	F		U	U
Business Risk Assessment			P/F			U				U	U
Information Security Risk Assessment			P	I	B	I	I	F		U	U
Information System Description			P	I	I	I	I	B	F	U	U
Security Requirements			P/F							U	
Monitoring Strategy				P/F	U	U	U	U		U	U
Security Control Description					P	B	F	U		U	
Software Assurance Misuse Cases					P	B	I	F		U	
Contingency Plan			P	I	I	I	F	U		U	
Contingency Plan Test								P/F		U	
Security Control Assessment								P	F	U	
Authorization Package									P/F	U	
Plan of Action & Milestones									P/F	U	
CMS CIO-Issued Authority to Operate (ATO)									P/F	U	
Security Monitoring Reports										U	
Project Management Artifacts					Baseline (B) Final (F)					Reviews and Artifacts are completed/conducted per the Project Process Agreement	
Security Artifacts				Interim (I)							
Security Information from Tasks				Preliminary (P)							
Systems Development Artifacts				Update Yearly (U)							

Exhibit 5-3: Security Artifacts Produced System Delivery Management Stage

5.2.1 CERTIFICATION AND ACCREDITATION

The MES Program will perform the certification and accreditation processes defined by CMS. The Certification and Accreditation process includes the following phases:

- Pre-Certification
- Initiation

- Certification
- Accreditation
- Maintenance
- Re-Certification or Re-Accreditation
- Disposition

5.2.2 RISK ASSESSMENT

The MES Program will perform the Risk Assessment processes defined by CMS. The Risk Assessment process includes the following phases:

- Business Risk and Safeguard Determination
- Technical Risk and Safeguard Determination
- Iterative Risk and Safeguard Determination
- Retention and Disposal of Security Artifacts

5.2.3 SYSTEM SECURITY PLAN

The MES Program will use the CMS formally defined System Security Plan (SSP) process. The System Security Plan includes the following phases:

- System Definition
- Security Control Requirements Development and Implementation
- Iterative SSP Process
- Retention and Disposal of Security Artifacts

When a module equates to a system, the standard CMS SSP process is used. If a module is not a complete system, the Module Security Plan (MSP) described below provides module specific content that contributes to the system level SSP.

5.2.4 MODULE SECURITY PLAN

The Module Security Plan (MSP) identifies the MES Module's security categorization and provides an overview of the security requirements and operating procedures for the MES Module in accordance with the CMS implementation of the Risk Management Framework (RMF). The MSP documents in a single reference the security architecture, technology, controls, responsibilities, and operations procedures that satisfy the requirements specific to each MES Module and prepares the information for inclusion in the Application and Infrastructure findings reports dictated by the CMS System Security Plans.

5.2.5 MODULE SECURITY PLAN DOCUMENT REQUIREMENTS

Attachment I contains the documentation requirements organized by CMS RMF phase.

The MES Module's security context shall be identified uniquely to ensure implementation of risk and control evaluations specific to the Module's development and operation.

5.2.5.1 IDENTIFICATION

In the case of a multi-module system, the tracking of compliance will be imperative. To better facilitate that tracking, an identification number should be applied to each modular component. The Agency ISM will assign a Security Unique Identification Number (SUID) to associate the Module with an authorization package and all future operational assessment and Plan of Action and Milestone (POA&M) reports.

5.2.5.2 SECURITY POINTS OF CONTACT

The MES Project Vendor shall maintain a roster of key security personnel within the MSP for each MES Module.

The roster at a minimum shall include:

- The Module Security Officer (MSO), supported by the Module Director of Operations if they are not available.
- The Module Security Event Manager (SEM), supported by the Module Director of Development if they are not available.
- The Module Director of Development
- The Module Director of Operations
- All team members of the Module Security Event Management Team

The Vendor shall maintain the roster of contact information for each team member and validate and send to the Agency ISM on a quarterly basis.

5.2.5.3 AUTHORIZATION BOUNDARY

The MES Module shall have its system boundaries identified, defined, and documented within the MSP to facilitate the accurate categorization and selection of security controls. Definition of the Module boundaries provides the authorizing official with accurate context to evaluate the Module and resident information. Boundary definition must occur before security categorization and ensures the accurate categorization of the Module.

The authorization boundary contains:

- A narrative description and purpose of the system to include business processes and MES functions supported
- A roster of applications with version levels and the capabilities and functions supported by each
- A roster of user organizations categorized as internal or external users based on network access location
- A description of the operating environment for the system to include any interface or technical factors that require special security considerations (e.g. cloud, mobile, wireless, etc.)
- The hardware and information assets specifically supporting the MES Module

- The management team and personnel developing and maintaining the MES Module
- The network boundary drawings showing the edge of communication and data flow
- A data flow diagram that shows production and consumption of Module data, and categorizes the information as external or internal to the Module

5.2.5.4 CATEGORIZATION

The MES Project vendor shall evaluate the Module's system interfaces and information classification to develop a recommended security impact categorization. Examples of information security classification by information type are documented in the [CMS System Security and e-Authentication Assurance Levels by Information Type](#). This system categorization recommendation shall be documented in the [CMS Standard System Categorization Worksheet](#) and sent to the Agency ISM for review and approval.

Florida Rule 74-2 and the NIST Risk Management Framework require the following minimum information set from the Vendor to accurately categorize the MES Module:

- Full descriptive name and all associated acronyms and "known as" identifiers for the version of the Module evaluated
- The SUID
- The owning organization, and key personnel, that manages, controls, and owns the information within the Module
- Purpose, functions, and capabilities of the Module, and the business processes supported
- Types of information processed by the Module
- Authorization Boundary contents
- System availability requirements (Maximum Tolerable Downtime (MTD), Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), Work Recovery Time (WRT))

The final categorization will be determined and approved in accordance with Federal Information Processing Standards Publication 199 (FIPS 199) and NIST Special Publication 800-60 Revision I Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories.

Attachment C contains an example of the [CMS Standard System Categorization Worksheet](#).

5.2.5.5 INTERCONNECTION AND INFORMATION SHARING

A Module interconnection is the direct connection of distinct MES Modules with external systems to share data. All Module interconnections shall be documented and maintained in the MSP, in the form of either:

- The Interconnection Security Agreement (ISA) – provides a technical overview and identifies roles and responsibilities for managing the interconnection

- The Memorandum of Understanding/Agreement (MOU/A) – provides a business overview in addition to the technical overview; generally, not needed unless a large and complex interface exists that supports broader business purposes
- The Business Associate Agreement – provides an agreement for complying with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The agreement is applicable if the MES vendor is a business associate within the meaning of the Privacy and Security Regulation, 45 C. F. R 160 and 164.

Connections to the Integration Platform (IP) require identification of the interconnection, and require additional interconnection documentation in the form of an ISA or MOU/A, except if exposing an open public API.

Attachment D contains examples of the ISA and MOU/A.

5.2.6 CONTROLS

Security controls are the administrative, physical, and technical measures prescribed to protect the confidentiality, integrity, and availability of the MES Modules. The mechanisms to implement each control can be automated processes, manual procedures, or a combination of both. Controls are audited frequently with AHCA IT being point of contact for many audits.

All security controls shall be categorized into one of three types:

- **Common Controls:** a security control inherited by an MES Module from a Common Control Provider (e.g. data center, cloud operator, access broker, etc.)
- **System Specific Controls:** a security control that is designed and implemented for a specific MES Module, and DOES NOT contain portions of a hybrid security control
- **Hybrid Controls:** a security control that is partially inherited from a common control and partially specific to the MES Module

5.2.6.1 CONTROL SELECTION AND DOCUMENTATION

The MES Module Vendor shall evaluate the security requirements directed by:

- Governing statutes and policies
- Security categorization
- CMS Application Finding Report results
- CMS Infrastructure Finding Report results
- CMS Acceptable Risk Safeguards
- Module availability requirements
- Agency security program governance as prescribed

The specific controls applicable to a module will vary by the scope of the module. CMS defines in the application development life cycle the security certification and accreditation, risk

assessment and system security plan processes that have activities throughout the life cycle that identify risks and corresponding controls. The MES Module Vendor shall select controls necessary to ensure levels of confidentiality, availability, and integrity appropriate for the security categorization of the Module.

MES Module Vendors shall document proposed controls according to the NIST Cybersecurity Framework (CSF) and its defined categories. **Exhibit 5-4: NIST Cyber Security Framework** shows the major components of the NIST Cyber Security Framework.

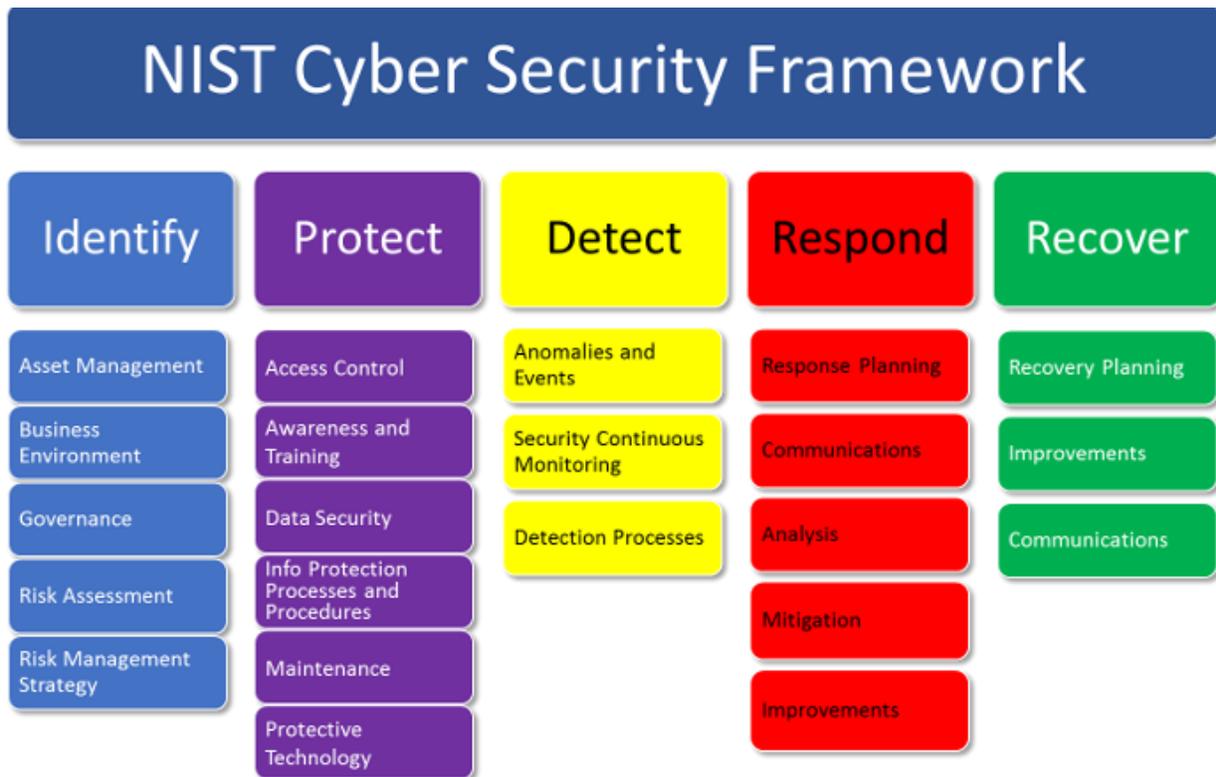


Exhibit 5-4: NIST Cyber Security Framework

Module Vendors shall document selected controls according to the CMS Risk Management Handbook Vol I Chapter 12.

Attachment E contains the CMS Required Security and Privacy Control Baselines for controls that must be implemented across the NIST CSF.

Attachment F contains the mapping of the NIST CSF to the NIST 800-53 Rev. 4 and CFR 45 Part 164 Subpart C (HIPAA Security Rule) for specific controls required by the security categorization and CMS Control Baselines.

5.2.6.2 CONTROL IMPLEMENTATION

Control implementation is comprised of four stages. MES Module Vendors shall ensure control implementation occurs throughout Module development life cycle as described in **Exhibit 5-5: Security Control Implementation Life** .

STAGE	TASK	DOCUMENTATION REQUIREMENTS
Analysis	Analyze the planned control and requirement and develop the control statement to satisfy the requirement. Software Assurance: Develop detailed requirements for misuse cases. See OWASP ASVS attachment for list of required controls.	Document control statements for each requirement in accordance with CMS Risk Management Handbook (RMH)
Design	Design each control, and select the implementation methodology (e.g. automated, manual, hybrid). Software Assurance: individual test plans are required for each misuse case identified during analysis.	Document design for each requirement in accordance with CMS RMH
Development	Develop according to the Design specification. Software Assurance: Development shall include measures to protect against identified misuse cases.	Update control documentation as needed in accordance with CMS RMH
Test	Test each control using test to failure methodology, and re-design or re-develop as necessary to ensure control satisfies requirement.	Document test results, and update control status in accordance with CMS RMH

Exhibit 5-5: Security Control Implementation Life Cycle

5.2.7 PLAN MAINTENANCE

Annually the Module Vendor and the Agency ISM will review and update the MSP to address changing standards and operational requirements. The Division of IT could use contracted services at times to assist with this responsibility.

5.3 MODULE DEVELOPMENT SECURITY LIFE CYCLE

Florida Cybersecurity Standards (F.A.C. Rule 74-2) requires information system owners and developers to use the NIST Cybersecurity Framework (CSF) to ensure information security for

systems that support operations and assets of Florida Agencies. Within the CSF, NIST prescribes the Risk Management Framework (RMF) to develop and implement minimum information security requirements and controls based on an assessment and categorization of the information and risk of exploitation within the system.

NIST states the NIST RMF provides the following support to securing information systems:

- Promotes near real-time risk management, and perpetual authorization evaluation through continuous monitoring of controls
- Champions automation to extract and compile data into useful information for leaders to make risk-based and cost-conscious decisions regarding information systems' security
- Integrates information security into enterprise architecture and the system development life cycle (SDLC)
- Prioritizes the selection, implementation, assessment, and monitoring of security controls
- Establishes responsibility and accountability for security controls deployed within an organization, and identifies ownership of controls as system specific or inherited from a provider

Exhibit 5-6: NIST Risk Management Framework shows that the RMF is a continuous evolution that progresses and adapts to changing organizational goals and changing technology requirements.

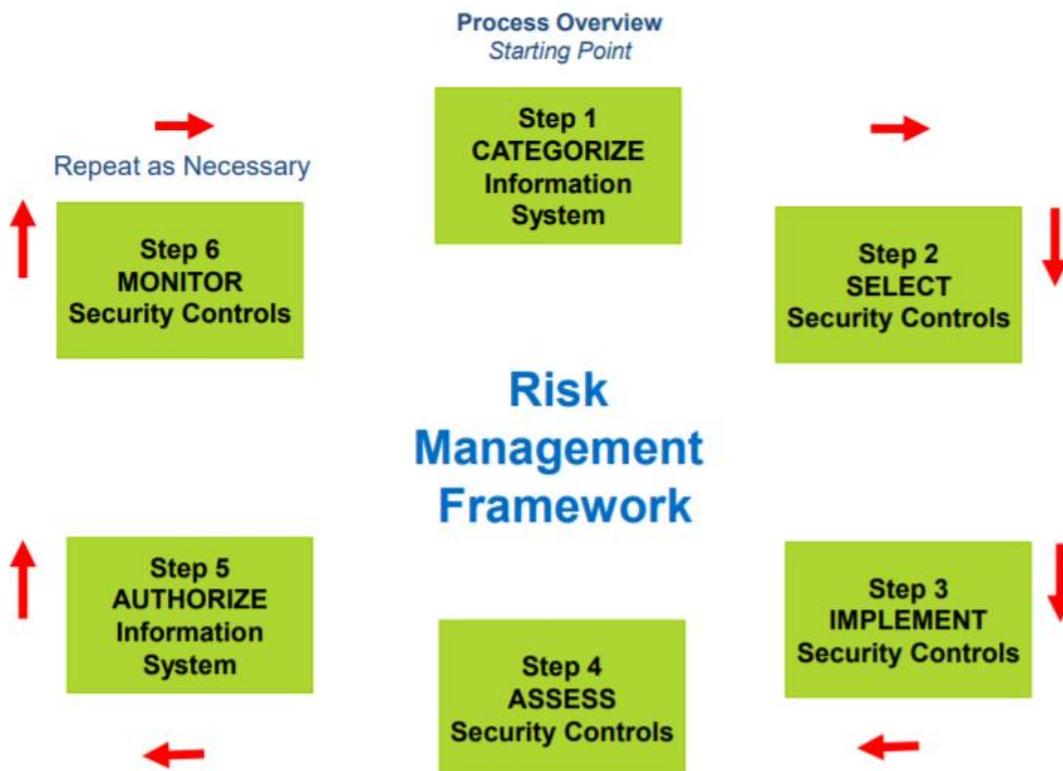


Exhibit 5-6: NIST Risk Management Framework

MES Module vendors shall use the NIST RMF to develop, document, implement, and communicate the security controls used to secure the Module.

5.3.1 AUTHORIZATION TO OPERATE

The Agency will evaluate MES Modules to ensure development for operations with an acceptable level of risk. The following sections outline the evaluation and process to achieve an Authorization to Operate (ATO) a MES Module within the specified environment.

The MES Module vendor shall comply with all applicable evaluation processes, and coordinate review and approval of proposed CMS Security Authorization Package (SAP) with the Agency ISM as defined in the CMS Risk Management Handbook (Attachment H).

The CMS Security Assessment Review provides an assessment of security controls. Because the SEAS Vendor performs the SAR, the assessment is independent of the MES Project Vendor. Agency ATO will be evaluated based on module specific risk considerations.

5.3.1.1 TESTING AND CERTIFICATION REQUIREMENTS

Exhibit 5-7: Testing and Certification Requirements by SDLC Phase shows the testing and certification requirements organized by the SDLC phases defined in the [MES Security Standards](#).

SEAS VENDOR TECHNICAL EXPERTISE PROVIDED	REQUIREMENTS ANALYSIS AND DESIGN PHASE	DEVELOPMENT AND TEST PHASE	IMPLEMENTATION PHASE	OPERATIONS & MAINTENANCE PHASE
OWASP Application Security Verification Standards 3.0	✓	✓	✓	✓
NIST Cryptographic Module Validation Program	✓	✓		
AHCA Vulnerability Management Evaluation		✓	✓	✓
AHCA Application Security Testing Evaluation		✓	✓	✓
CMS Security Assessment Review	✓	✓	✓	✓
AST Risk Assessment	✓	✓	✓	✓

Exhibit 5-7: Testing and Certification Requirements by SDLC Phase

- **Open Web Application Security Project (OWASP) Application Security Verification Standard 3.0** – demonstrate efficacy of controls designed for misuse of MES Modules
- **NIST Cryptographic Module Validation Program** – demonstrate efficacy of controls designed to secure data in all forms (in flight, at rest, and in process)
- **AHCA Vulnerability Management Evaluation** – acceptable risk as defined by AHCA Security Program
- **AHCA Application Security Testing Evaluation** – acceptable risk as defined by AHCA Security Program
- **CMS Security Assessment Review** – acceptable risk as defined by the CMS Acceptable Risk Framework
- **AST Risk Assessment** – acceptable risk as defined by F.A.C. 74-2 (Florida Cybersecurity Standard)

5.3.1.2 INTERIM AUTHORIZATION TO OPERATE

CMS will grant an Interim Authority to Operate (IATO) to authorize a Module for operation with risks that are not permanently acceptable. Granting an IATO is temporary and requires the development of a Plan of Actions and Milestones (POA&M) in accordance with the CMS Risk Management Handbook Volume I Chapter 1 to remediate all unacceptable risks.

If the Agency does not mitigate risks according to the POA&M, CMS can issue a Denial of Authorization to Operate (DATO) and direct immediate termination of operation and connection of the Module.

5.3.1.3 FINAL AUTHORIZATION TO OPERATE

CMS will grant a final Authorization to Operate (ATO) upon successful mitigation of risks to an acceptable level. This ATO grants operation for three (3) years. MES Module Vendors must maintain all controls and make the systems available for annual auditing as necessary to maintain the ATO. If the vendor's security posture is not adequate, or a specific category has not been addressed, a DATO can be issued, and operation ceased. The Agency's Enterprise Risk Manager (ERM) would be informed of this risk situation.

SECTION 6 DATA SECURITY MANAGEMENT AND REPORTING

This section describes the:

- Process to track and report the security compliance to the enterprise governance organizations
- Security reporting framework and inventory of security reports
- Process to update security standards

The enterprise governance committees provide a structure for project, technology, program and strategic decision making and direction setting. In addition, the Agency's units that perform data privacy and security today (e.g. HIPAA Privacy, AHCA Information Security) serve as the enterprise security governance group for governance and decision making.

6.1 MES DATA SECURITY COMPLIANCE REPORTING

The types of MES Data Security compliance reporting that occur include:

- Project Specific Compliance Reporting
- Cross-Project Compliance Reporting
- Formal Reporting

The sections that follow describe the reporting process for each type of reporting.

6.1.1 PROJECT SPECIFIC COMPLIANCE REPORTING

The tracking and reporting of security compliance occurs throughout the system delivery management stage of the MES Project Life Cycle. Review and compliance reporting occur in:

- Security Artifact Reviews
- Project Life Cycle Reviews
- Project Life Cycle Security Phases
- Certification Reviews

6.1.1.1 SECURITY DELIVERABLE REVIEWS

The MES Project Life Cycle defines [MES Project Life Cycle Artifacts](#) produced by MES Projects. There are many security related project artifacts applicable to MES Projects. The specific artifacts produced for each project will vary based on scope and complexity of the project. The SEAS Vendor reviews Project Vendor deliverables and provides findings and recommendations. The deliverable review reports including findings provided to the Project Manager of the MES Project.

The status of project artifact development, completion, review and approval is reported through the project work plan and project status reporting processes defined in the SEAS Deliverable [P-2 MES Project Management Standards](#).

Project specific artifacts will be stored in the artifact repository specified for each project and are accessible to authorized parties. Interested enterprise security governance members would be provided access to project security artifacts.

6.1.1.2 PROJECT LIFE CYCLE REVIEWS

The MES Project Life Cycle also defines formal system delivery management review points and templates that produce project review reports. The system delivery management reviews occur at key points in the project life cycle and provide checkpoints on project direction, progress and compliance. Security standards compliance content is included in different project life cycle review reports. SEAS Deliverable [T-7 Design and Implementation Management Standards](#) provides information about project life cycle reviews and references to review templates. The system delivery management review reports are produced by an integrated review team.

As with other project artifacts, the system delivery management review reports will be stored in the artifact repository specified for each project and are accessible to authorized parties. Interested enterprise security governance members will be provided access to project security artifacts.

6.1.1.3 CERTIFICATION REVIEWS

Certification reviews include checklists with security compliance criteria. The certification reviews update the MECT certification checklists and review of project artifacts providing information about compliance with security standards and data privacy practices. The SEAS vendor maintains the Certification checklists. The certification checklists are stored on the MES Project Repository and accessible to authorized users.

IV&V produces a quarterly report and artifact of certification that is provided directly to CMS. The Agency also receives a copy upon submission to CMS. Issues and decisions resulting from Certification checklists and IV&V quarterly reports are presented to governance committees using the standard process.

6.1.2 CROSS PROJECT STANDARDS COMPLIANCE REPORTING

The SEAS Vendor performs analysis of trends and cross-project security standards compliance issues. The SEAS Vendor will provide reports to the Projects Governance Committee and the Technology Governance Committee of findings, recommendations and decisions that need to be made related to security standards compliance.

The security compliance reporting content, compliance reporting content distribution, recommendations described in SEAS Deliverable [T-6 Technology Standards](#) Section 6 will be followed for security standards related compliance.

6.1.3 FORMAL REPORTING

Section 6.3.2 Inventory of Security Reporting Requirements lists formal reports produced at defined intervals to meet specific reporting requirements. The formal reports are provided to the enterprise security governance group in addition to the audiences specified per reporting requirement.

6.2 DATA SECURITY PROCESS AND CRITERIA

6.2.1 OPERATIONAL SECURITY

The MES Module Vendor shall maintain secure operations of MES Modules in accordance with all applicable governance outlined within this document, and as prescribed by the AHCA Security Program.

6.2.1.1 VULNERABILITY MANAGEMENT

The Agency uses vulnerability management and application security testing software platforms to consistently identify control gaps and exploitation risks. MES Module Vendors shall make Modules available or perform testing and evaluation during all development, implementation, and operational phases. The MES Project Vendor is responsible for vulnerability testing. The decision on use of Agency resources or other vendors to perform independent vulnerability testing will be made on a project by project basis.

6.2.1.2 APPLICATION SECURITY

CMS requires misuse case testing for all software, to include Commercial Off-the-Shelf (COTS) products, as a minimum assurance for software security compliance.

Attachment G contains the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) with examples of misuse cases. The MES Module Vendor shall submit a proposed Verification level, in accordance with the ASVS, to the Agency ISM for approval. Upon approval, the MES Module shall address all application development controls for the specified Verification level in the MSP control selection and implementation documentation.

The Agency is researching vulnerability management tools and application security management tools. OWASP provides a minimum basis that is the guidance for MES Project Vendors until the Agency provides guidance on use of a specific vulnerability management tool, service or process..

6.3 SECURITY MANAGEMENT REPORTS

Security management reports build from the security reporting framework and include specific security reporting requirements.

6.3.1 SECURITY REPORTING REQUIREMENT FRAMEWORK

Exhibit 6-1: Security Reporting Requirement Framework shows a framework of security related reporting requirements for MES Projects.

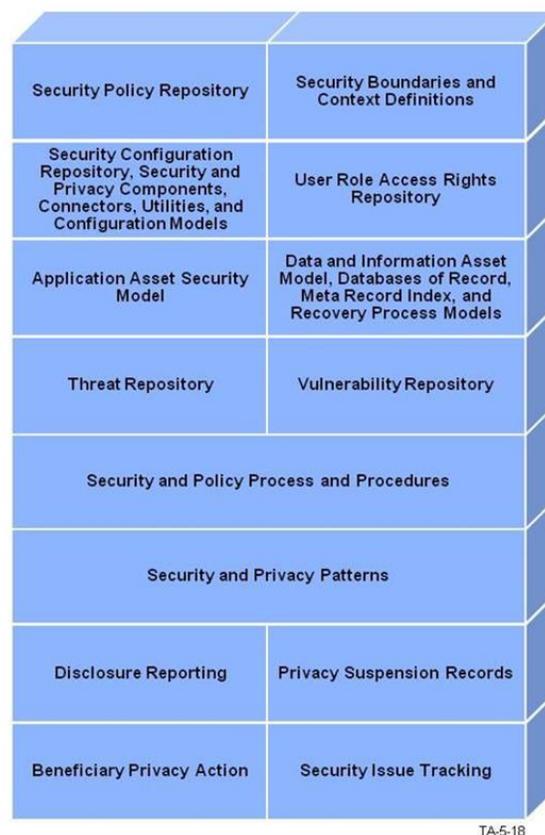


Exhibit 6-1: Security Reporting Requirement Framework

6.3.2 INVENTORY OF SECURITY REPORTING REQUIREMENTS

In addition to project and cross-project security reporting described above, the Program has formal security reporting requirements. **Exhibit 6-2: Security Reporting Requirements** lists security reporting requirements and include the audience of the report. The Technology Governance Committee is an audience to review reports for informational purposes. Issues and decisions resulting and direction setting resulting from content of reports would follow normal Program governance processes.

NAME	FREQUENCY	REQUIREMENT	AUDIENCE
FISMA Assessment	Annual	One third of security controls tested annually, and all security controls tested no less than every three years	CMS AHCA ISM Technology Governance Committee
Security Plan Review	Annual and Ad Hoc for Significant Change	Management review, update, and certification of System Security Plan	CMS AHCA ISM Technology Governance Committee
Risk Assessment	Annual and Ad Hoc for Significant Change	Risk assessment in accordance with AST and Florida Cybersecurity Standards	CMS AHCA ISM AST Chief Information Security Officer Technology Governance Committee
CMS Security Assessment Report (SAR)	Upon Initial Delivery and Annually	Documentation of Security Control Assessment (SCA) and coordinated with FISMA Annual Assessment. Develop Plan of Action and Milestones (POA&M) to address findings from audits, assessments, and standards reviews.	CMS AHCA ISM AST CISO Technology Governance Committee
Security Event Response	As needed in accordance with Security Event Response Plan	Collect and submit information in accordance with documented SERP	AHCA ISM
IATO POA&M	In accordance with agreed to reporting frequency	Document progress toward mitigating risks allowed for issuance of IATO	AHCA ISM CMS AST CISO Module Security Plan
Vendor Security Score Card	During procurement	Provide independently verified security score rating	Procurement Team AHCA Contract Manager

Exhibit 6-2: Security Reporting Requirements

6.4 SECURITY STANDARDS UPDATE PROCESS

As the result of compliance reporting findings or other events, the security standards may need to be updated. Keeping security standards updated improves data protection and privacy. It is the SEAS Vendor along with the Agency's responsibility to keep the Security Standards in the TSRG updated. The benefits for creating a defined process for updating security standards include:

- Reduced security vulnerability and data privacy risk

- Improved data and privacy protection
- Increased security compliance
- Improved consistency and efficiency of security processes

[SEAS Deliverable T-6 Section 4: Technology Standards Reference Guide](#) is a Word document that describes the structure, maintenance, and communication of the TSRG. [SEAS Deliverable T-6 Attachment B – How to Maintain the TSRG List](#) is a Word document that describes the procedures to maintain content in the Technology Standards Reference Guide. The document includes definitions of the fields in the TSRG (e.g. standards name, version, maturity, owning organization, compliance approach, status, etc.), steps for creating a new standard, and steps for updating an existing standard. The TSRG has a Compliance Approach section that contains a narrative that will be used to define the process and list of events of verifying adherence to the applicable standard.

Exhibit 6-3: Security Standards Refresh Events describes the events when the security standards will be reviewed and updated as necessary.

EVENT	DESCRIPTION
Annual Review	The SEAS Vendor will conduct an annual review of the security standards in the TSRG looking for updates to existing security standards and new security standards relevant to the Agency that should be added to the TSRG.
Issuance of ITN / Procurement	As part of the creation of ITN / Procurement documentation, The SEAS Vendor will conduct a review of the security standards in the TSRG looking for updates to existing security standards and new security standards relevant to the Agency that should be added to the TSRG.
Publication of new MITA Standard(s)	In the event of a material change in MITA Part III – Technical Architecture, The SEAS Vendor will conduct a review of the security standards in the TSRG as compared to MITA. If required, existing security standards will be updated and new security standards relevant to the Agency will be added to the TSRG.

Exhibit 6-3: Security Standards Refresh Events

SECTION 7 APPENDIX A – SUPPORTING ATTACHMENTS

ATTACHMENT A – SECURITY STANDARDS REFERENCE GUIDE

Attachment A – Security *Standards Reference Guide* contains an Excel-format extract of design and implementation management standards from the TSRG on the MES Projects Repository. This file contains content as of the date of deliverable submission. Note: as described above in Section 3.6 Standards Support, many standards included refer to well-known composite standards such as the NIST Cybersecurity framework that provide guidance on many topics. The provided standards do not attempt to derive discrete prescriptive standards from the composite standards.

ATTACHMENT B – CMS RISK MANAGEMENT HANDBOOK (RMH) INCIDENT RESPONSE CHAPTER

Attachment B – contains the CMS Risk Management Handbook (RMH) Incident Response Chapter. The Incident Response content is from Chapter 8 of the CMS Risk Management Handbook Version 1.1.

This is a link to [CMS Risk Management Handbook \(RMH\) Incident Response Chapter](#) as of the date of this deliverable.

The CMS Information Security Library contains the authoritative version of all documents:

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

ATTACHMENT C – CMS STANDARD SYSTEM CATEGORIZATION WORKSHEET

Attachment C – contains the most recent version of the CMS Standard System Categorization Worksheet. The CMS Information Security Library contains the authoritative version of all documents:

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

ATTACHMENT D – CMS EXAMPLE MEMORANDUM OF UNDERSTANDING AND INTERCONNECTION SECURITY AGREEMENT

Attachment D – contains the most recent versions of the CMS MOU and ISA for connecting external systems to the Module. The CMS Information Security Library contains the authoritative version of all documents:

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

ATTACHMENT E – CMS REQUIRED SECURITY AND PRIVACY CONTROL BASELINES

Attachment E – contains the most recent versions of the CMS Required Security and Privacy Control Baselines. The CMS Information Security Library contains the authoritative version of all documents:

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

ATTACHMENT F – NIST CSF TO NIST 800-53 AND HIPAA CONTROLS

Attachment F – contains the mapping of the NIST CSF to the NIST 800-53 Rev. 4 and CFR 45 Part 164 Subpart C (HIPAA Security Rule) for specific controls required by the security categorization and CMS Control Baselines.

ATTACHMENT G – OWASP APPLICATION SECURITY VERIFICATION STANDARD

Attachment G – contains the most recent version (3.0) of the Open Web Application Security Project (OWASP) Applications Security Verification Standard (ASVS) at the time of publication. The OWASP ASVS Project portal page contains the authoritative source for the latest versions and announcements of pending updates:

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

ATTACHMENT H – CMS RISK MANAGEMENT HANDBOOK VOL I CHAPTER I – RISK MANAGEMENT IN THE XLC

Attachment H – contains the most recent versions of the CMS Risk Management Handbook. The CMS Information Security Library contains the authoritative version of all documents:

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

ATTACHMENT I – CMS RISK MANAGEMENT FRAMEWORK OVERVIEW

Attachment I – contains the most recent versions of the CMS Risk Management Framework Overview. The CMS Information Security Library contains the authoritative version of all documents:

<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

ATTACHMENT J – MES SYSTEMS SECURITY ANALYSIS

Attachment J – contains a template for an attachment of current and future security analysis of MES Systems to identify security governance, practices, and standards applicable to MES Projects to improve security and data protection for systems in the MES Program. Security analysis content will be populated in future iterations of this attachment throughout the life of the MES Program.

REFERENCE TO OTHER DELIVERABLES

SEAS Deliverable T-6 - Technology Standards

T-6 – Technology Standards establishes the MITA compliant Florida Medicaid Technology Standards Reference Guide (TSRG) and Technology Standards Reference Model (TSRM) and describes a maintenance process.

SEAS Deliverable T-6 Technology Standards Attachment B – How to Maintain the TSRG

SEAS Deliverable T-6 Technology Standards Attachment B – *How to Maintain the TSRG* List is a Word document that describes the procedures to maintain content in the Technology Standards Reference Guide content.

SEAS Deliverable T-6 Technology Standards Attachment E – Technology Standards Communication, Support, Compliance, and Compliance Reporting Procedures

SEAS Deliverable T-6 Technology Standards Attachment E – *Technology Standards Communication, Support, Compliance, and Compliance Reporting Procedures* describes the processes to communicate new and modified standards or compliance expectations to stakeholders, support stakeholders' adherence to standards, assess stakeholders' compliance to standards, and communicate levels of standards compliance to the Agency.