AHCA Florida Health Care Connections (FX)

T-8: Enterprise Data Security Plan

Version: 300

Date: June 28, 2021

Author: The SEAS Vendor

Submitted To: AHCA FX Program Administration Team

Revision History

DATE	VERSION	DESCRIPTION	AUTHOR
6/28/2018	001	T-8: Enterprise Data Security Plan Development Draft Version (Entry)	Andreas Casey
8/29/2018	002	T-8: Enterprise Data Security Plan Revised to address Agency Review Comments	Rich Cefola / Paul Moore
9/11/2018	100	T-8: Enterprise Data Security Plan Final Version	Sean Gibbs
8/2/2019	101	Annual deliverable refresh	Barry McConnell
9/12/2019	200	T-8: Enterprise Data Security Plan approval of annual refresh	Carol Williams
11/21/2019	201	T-8: Enterprise Data Security Plan Q2-2019 Quarterly Deliverable Refresh	Joanna Redding Steve Ruszkowski
12/11/2019	202	T-8: Enterprise Data Security Plan Revised to address Agency Review Comments	Joanna Redding Steve Ruszkowski
12/12/2019	225	T-8: Enterprise Data Security Plan Approved Q2-2019 Quarterly Deliverable Refresh	Carol Williams Eric Steinkuehler
5/20/2021	226	T-8: Enterprise Data Security Plan draft deliverable refresh updates made: ▪ Updated Section 1 boilerplate language and made minor grammatical edits and standardization throughout ▪ Added new Section 5.2.5 – *Use and Protection of Federal Tax Information Data*	Steve Ruszkowski Francisco Acevedo
6/21/2021	227	T-8: Enterprise Data Security Plan revised to address Agency Review Comments	Steve Ruszkowski
6/28/2021	300	T-8: Enterprise Data Security Plan Approved Final	Carol Williams

Modifications to the approved baseline version (100) of this artifact must be made in accordance with the FX Artifact Management Standards.

Quality Review History

DATE	REVIEWER	COMMENTS
7/24/2018	Sean Gibbs	QA Review for initial submission
8/29/2018	Scott Mildenberger	QA Review for second submission
8/1/2019	Carol Williams	QA Submission Review of annual deliverable refresh
11/18/2019	Michael Avello	QA Submission Review of quarterly deliverable refresh
12/11/2019	Eric Steinkuehler	QA Submission Review
5/20/2021	Carol Williams	Conducted QA review
6/21/2021	Carol Williams	Conducted QA review

Table of Contents

Table of Exhibits

SECTION 1 INTRODUCTION

1.1 BACKGROUND

The Florida Agency for Health Care Administration (AHCA or Agency) is adapting to the changing landscape of healthcare 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 is complex; it includes services, business processes, data management and processes, technical processes within the Agency, and interconnections and touchpoints with systems necessary for administration of the Florida Medicaid program that reside outside the Agency. The future of the Florida Medicaid Enterprise integration is to allow the Agency to secure services that can interoperate and communicate without relying on a common platform or technology.

The Florida Medicaid Management Information System (FMMIS) has historically been the central system within the Florida Medicaid Enterprise; functioning as the single, integrated system for claims processing and information retrieval. As the Medicaid program has grown more complex, the systems needed to support the Florida Medicaid Enterprise have grown in number and complexity.

The Medicaid Enterprise System (MES) Procurement Project was re-named Florida Health Care Connections (FX) in the summer of 2018. FX is a multi-year transformation to modernize the current Medicaid technology using a modular approach, while simultaneously improving overall Agency functionality and building better connections to other data sources and programs.

1.2 PURPOSE

Establishing standards for controls, technology, and capabilities diminishes risk, reduces the threat surface, and increases the confidentiality, integrity, and availability for FX. The *T-8: Enterprise Data Security Plan* is the information and technical security strategy guiding secure development of FX, 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 *T-8: Enterprise Data Security Plan* organizes security information for the secure development and operation of FX, including:

- Policy guiding security decisions for the Agency and CMS
- Control objectives identified in federal and state regulations
- Technology 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 FX into a single reference source for the secure planning, development, implementation, and oversight of FX

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 for each of the FX stakeholders during the design and implementation phases of an FX 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, Department of Management Services (DMS) Florida Division of State Technology (DST), and FX.
- **Section 4 Incident Reporting Process and Templates** – Outlines the process to manage cyber security incident/breach investigations, resolution management, and reporting in coordination with the Agency Information Security Manager (ISM) and the Agency's Health Insurance Portability and Accountability Act of 1996 (HIPAA) Compliance Office. Additional reporting standards may also be specified in the Business Associate Agreement (BAA) and will be required to meet compliance.
- **Section 5 Security Requirements Analysis** – Defines the life cycle for evaluating and analyzing FX security compliance. Documents the process for determining corrective actions and prescribes at what levels to grant an Interim Authorization to Operate (IATO).
- **Section 6 Security Management and Reporting** – Describes the process for reporting enterprise security management to the Technology Standards Committee (TSC) and defines the catalog of reports to be included with compliance reporting.

1.4 GOALS AND OBJECTIVES

- **Goal #1 – Secure FX Development.** The following objectives guide success toward this goal:
  - Objective #1 – Define governing security frameworks and industry standards
  - Objective #2 – 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 FX Project Owners
  - Objective #2 – Define process for monitoring and reporting incidents in accordance with State and Agency policy and procedures
- **Goal #3 – Secure FX Operation.** The following objectives guide success toward this goal:
  - Objective #1 – Objective and consistent FX security assessment for issuing an IATO
  - Objective #2 – Actionable security intelligence reporting framework and enforcement system
  - Objective #3 – Periodic operational certification of FX's 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, Subparts C, D, and E
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 113th Congress to amend Chapter 35 of Title 44, United States Code
Federal Information Processing Standards	Sets the approved technology standards and guidelines for federal information systems.	Federal Government - NIST	S.1124 of the 104th 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 FX platforms.	Federal Government (Centers for Medicare and Medicaid Services (CMS))	Affordable Care Act: Medicaid Program: Federal Funding for Medicaid Eligibility Determination and Enrollment Activities (Federal Register 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 Cybersecurity Framework (CSF) and Federal Information System Management Act (FISMA) as guiding documents.	State of Florida	Rule 60GG-2.001 through 60GG-2.006, Florida Administrative Code
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	Rule 60GG-5.003, Florida Administrative Code
SEAS Contract	Authorizes Florida Agency for Health Care Administration to expend funds in support of developing the strategy and governance for the FX 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, as described in **Exhibit 2-1: Roles and Responsibilities** below.

ROLE	RESPONSIBILITY
Agency Information Security Manager (ISM)	▪ Evaluate and track incident reports from FX Project Owners and initiate Agency Computer Security Incident Response Team (CSIRT) process when necessary, per Rule 60GG-2.005, Florida Administrative Code ▪ Coordinate with DST 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 IATO and Final Authorization to Operate (ATO) ▪ Implement data security tracking tool and provide scan results to Contract Management and Procurement
Agency Computer Security Incident Response Team (CSIRT)	▪ Develop templates for managing cyber security incident/breach investigation and resolution management reporting ▪ Creating and maintaining an incident response plan (IRP) ▪ Investigating and analyzing incidents ▪ Managing internal communications and updates during or immediately after incidents ▪ Communicating with employees, stakeholders, vendors, and the communications team about incidents as needed ▪ Remediating incidents ▪ Recommending technology, policy, governance, and training changes after security incidents
Agency Director, Information Technology/Chief Information Officer	▪ Advocate and fund information security requirements during budget planning and execution to support FX development ▪ Coordinate with Agency, Agency Information Security Manager, and SEAS Vendor to establish workflow and touch points for use of Agency security tools and processes
SEAS Vendor	▪ Ensure tools and processes are in place for the execution of the *T-8: 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 FX Project Owners on Project Standards, Integrated Processes, and Design and Implementation Standards ▪ Use 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 FX projects and services ▪ Develop and document a process to report on enterprise data security management and reporting results at enterprise governance ▪ Provide standards support and expertise throughout FX

ROLE	RESPONSIBILITY
FX Project Owners	▪ Assign principal Project Security Officer (PSO) to manage project security and reporting ▪ Maintain project security profile and role-based security for review by CMS, State, external, and internal auditors ▪ Maintain Plan of Actions and Milestones (POA&M) for project 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 project 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 project development
Agency Privacy Officer	▪ Evaluate and track privacy incident reports from FX Project Owners ▪ Review procurements and provide privacy review of responses to solicitations ▪ Provide privacy assessment input and recommendation to Agency Information Technology Director / Chief Information Officer for IATO and Final Authorization to Operate (ATO)
Integration Services / Integration Platform (IS/IP) Vendor	▪ All responsibilities described for FX Project Owners are applicable for the Integration Platform implemented by the IS/IP Vendor ▪ Implement and operate the enterprise-level role-based Single Sign-On / authentication solution ▪ Support FX Project Owners in implementing secure technical integration and interoperability between systems and projects
Medicaid Fiscal Agent Operations (MFAO)	▪ Oversee and approve access for State employees and external organizations. Perform audit functions such as verifying appropriate role permissions and employee status (active/terminated). Oversee and approve access for Agency staff and external organizations

ROLE	RESPONSIBILITY
FX Independent Verification and Validation (IV&V) Vendor	▪ 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 FX 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 FX Project deliverables for an effective project ▪ Evaluate project progress, resources, cost, schedules, workflow, 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 FX Project deliverables for the project's success

Exhibit 2-1: Roles and Responsibilities

SECTION 3 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 FX projects.

This section describes the framework of applicable security related standards and how they intersect across the scope of impact of industry, CMS, DST, Agency, and specific FX projects and align to the security topics of:

- Data Security
- Identity and Access Management / Single Sign-On
- 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 FX projects and eventual Authorization to Operate and system certification.

The CMS Information Security (IS) Acceptable Risk Safeguards (ARS) is a comprehensive information security document put forth by CMS outlining broad-based, best practices for CMS information systems. Additionally, the document uses the most current version of NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* publication and other departmental specific documents as guidance in regard to information security.

Attachment D – Information Security Risk Assessment Template is a CMS document that is part of the RMH Chapter 14: Risk Assessment. This template should be used to perform the risk assessment.

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. Document source: www.cms.gov.

FX vendors will utilize the most current CMS approved template to construct the SSP.

Together, the CMS IS ARS, CMS Minimum Security Requirements (CMSR) and the CMS 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 an Excel report on the FX 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 displays the correlation between the precedence and the types of rule-making bodies.

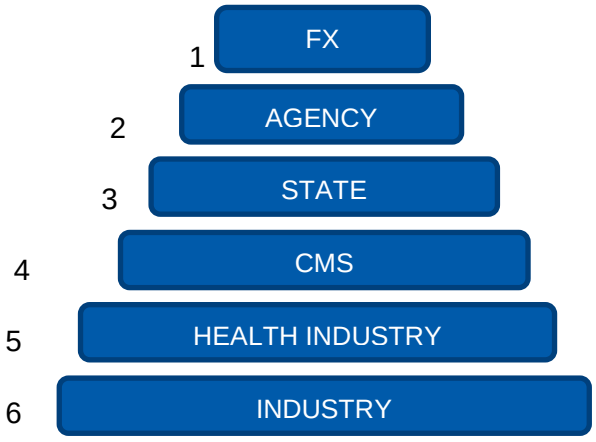

Exhibit 3-1: TSRG Standards Hierarchy

When competing standards exist, the TSRG Standards Hierarchy will allow FX Project Owners or other users to evaluate the 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 FX 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: Includes topics such as:
    - Data Standards
    - Security and Privacy

3.5 SECURITY GOVERNANCE AND STANDARDS MODEL

Exhibit 3-2: Security Governance Model shows the overarching standards that guide secure FX development and operation. The most recent version of each standard is applicable.

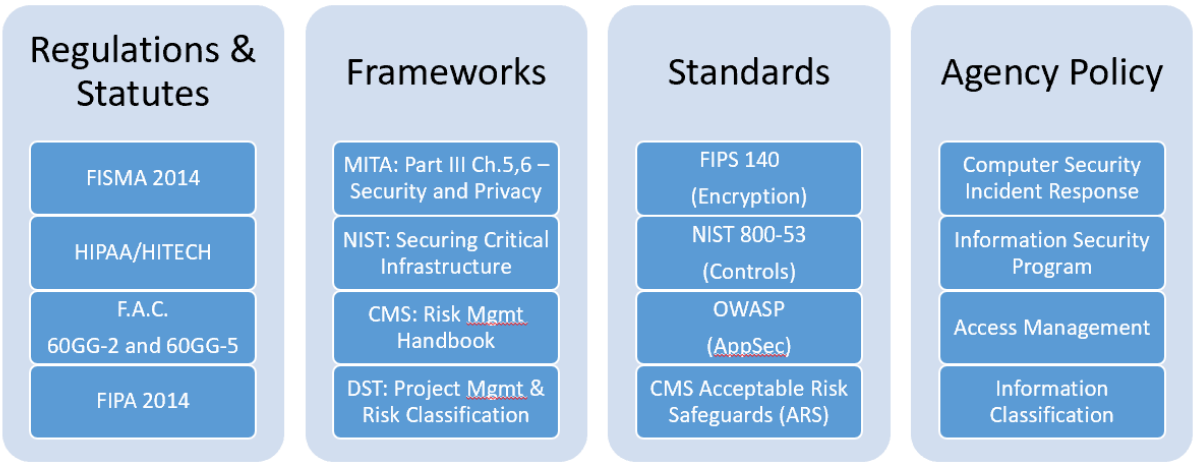

Exhibit 3-2: Security Governance Model

3.6 STANDARDS SUPPORT

The SEAS Vendor shall support use of security standards by the Agency and FX Project Owners for the implementation of FX projects. For security standards, the SEAS Vendor shall:

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

Using common technology standards processes and providing relevant technical expertise will help the SEAS Vendor guide FX Project Owners, and ultimately the Agency, to implement FX projects that achieve the FX 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 and originating from many sources including Agency contract language, Agency standards, DST, State, CMS, and industry sources. The TSRG is the repository of applicable standards with levels 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 and sets the expectations for vendors to comply with standards from multiple sources, even as those standards evolve. The TSRG includes a compliance approach for each standard's 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. Providing detailed prescriptive requirements:

- Is not a CMS recommendation
- Is uncommon in the market
- Is inconsistent with other state MMIS procurements
- Increases vendor response costs thereby discouraging responses and competition
- Extends procurement timeframes

Specifying discrete requirements would have minimal net risk reduction to the Agency and may even 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 life cycle, the security certification and accreditation processes, risk assessment (RA) processes, and SSP processes. Additionally, the Medicaid Enterprise Certification Life Cycle (MECL) processes include checklists and processes to assess and reduce security risk.

The SEAS Vendor shall use 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 FX technology domain standards improves consistency, efficiency, understanding, and communication. Specifically, the SEAS Vendor shall use the processes and procedures in the SEAS deliverable *T-6: Technology Standards*.

SECTION 4 INCIDENT REPORTING PROCESS AND TEMPLATES

The incident reporting and process section describes the process and guidance for the reporting of cyber security incidents and any resulting breach investigations. 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
- Describes the Agency and internal departments, external organizations (including federal and state agencies and FX Project Owners), and their roles and responsibilities within the context of an enterprise system and data security
- Defines the current and future processes, templates, and tools used for incident reporting of security incidents
- Plans 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, RA, and 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 (sections 501.171, 282.0041, 282.318(2)(i), F.S.) and federal regulations, including the federal HIPAA breach notification rule, provide guidance on data breaches. These events have the potential to put data at risk of unauthorized acquisition, access, use, disclosure, modification, or destruction. FX Project Owners shall evaluate Security Events and triage for reporting to the Agency ISM and potential activation of the Agency's 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 also enters into a Business Associate Agreement (BAA) with vendors. The provisions of the BAA apply to HIPAA requirements and may have additional reporting requirements. Reporting timeframes for Security Events and BAA provisions are different; in such cases the more restrictive timeframe will apply. Although HIPAA and BAA requirements are primarily concerned with PHI data, these timeframes apply to all data.

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 one (1) hour of detection if the attack is ongoing, and FX Project Owner 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 **FX Project Owners are NOT required to report malicious logic that has been successfully quarantined by anti-malware software*
CAT 4	Inappropriate Use	Individual violation of appropriate use policy of any FX 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 FX information assets AND does **NOT** result in compromise or denial of service	Weekly on an agreed to schedule
CAT 6	Investigation	Open reviews of suspicious activity that FX Project Owner 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 FX. Event management minimizes lost information, speeds triage, reduces outages, and increases organizational knowledge to prevent future events and incidents.

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

FX Project Owners shall document, submit to the Agency ISM, and maintain a formal and approved SERP that includes the components outlined in the most current version of the CMS Risk Management Handbook (RMH): Chapter 08: Incident Response.

Some the components outlined in the handbook include:

- Assignment of a single individual, with appropriate backup, as the FX Project Owner Security Event Manager (SEM) to serve as the point of contact for all communications and reporting between the FX Project Owner 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 walk-through 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 ISM of a potential Security Incident

The Agency will allow FX Project Owners to respond with SERP templates based on best practices and expertise. Once a template is approved, the template will be added to the *T-8: Enterprise Data Security Plan* for future FX Project Owners' use as a standard.

It is highly recommended that FX Project Owners model SERP and its components according to 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 required next steps. 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 FX Project Owner 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 FX Project Owner's Security Event Management should contain. The Agency will allow FX Project Owners 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 *T-8: Enterprise Data Security Plan* for future FX Project Owners' use as a standard.

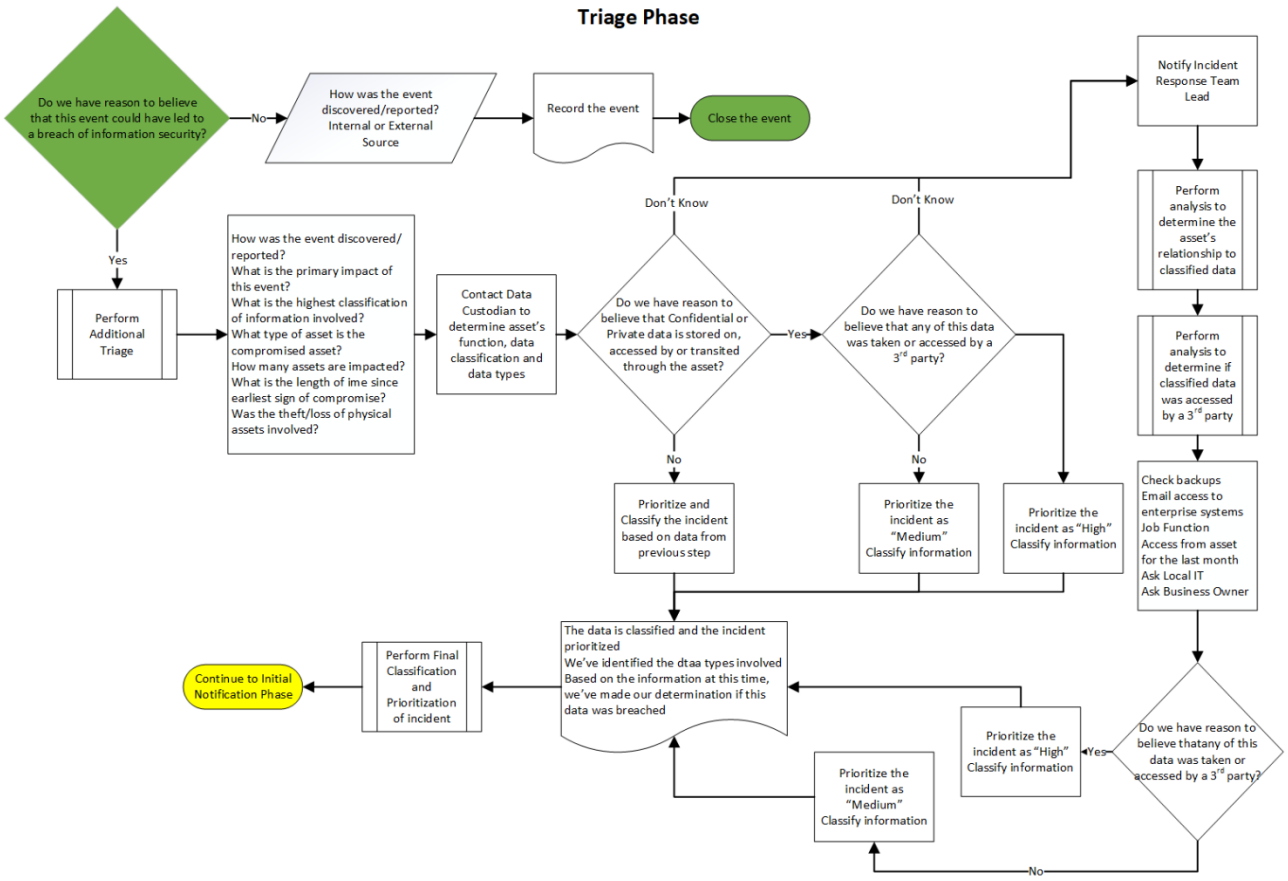

Exhibit 4-2: Example Security Event Notification Flow

The CMS Incident Response Plan Template and Incident Response Reporting Template can be found in *Attachment F – Risk Management Handbook, Chapter 8: Incident Response.*

4.3 INCIDENT TRACKING TOOL

The Agency currently uses the FX Projects Repository 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 Security Event Management process that requires all FX Project Owners to submit all qualified events to the Agency ISM for evaluation.

Immediate capability requirements for development include:

- Security Event Management portal for FX Project Owners to submit Security 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 Security 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. FX Project Owners shall ensure their Security 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 FY18-19, the SEAS Vendor met with the Agency to select a product that meets the incident tracking tool requirements. After review, the Agency decided to extend the Agency's Cherwell tracking system to include security incident as defined in the vendor's contract and Business Associate Agreement and HIPAA incidents as defined as any use or disclosure of protected health information not provided for in this contract. The SEAS Vendor will be available to provide assistance in developing any required templates when requested by the Agency.

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 FX and FX vendor security policies and practices. The SEAS Vendor shall review the module vendors provided Plan of Action and Milestones (POA&M), which documents the 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 Agency standard procurement language.

SECTION 5 SECURITY REQUIREMENTS ANALYSIS

Standardized security requirements for development and operations of FX projects 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 ATO
- System Security Plan (SSP) per Module
- Process for evaluating compliance with federal, State, and Agency regulations, rules, and policies

5.1 CURRENT STATE CONTROLS

The current FMMIS is an Agency Owned / Contractor Operated (AO/CO) closed system governed by Service Level Agreements (SLAs). Gainwell (formerly Hewlett-Packard Enterprise) maintains the security operations for FMMIS and provides the Agency with periodic reports on security compliance and security events. The Agency maintains access control to FMMIS using the Medicaid Enterprise User Provisioning System (MEUPS).

The security controls for the FMMIS system are documented in the CMS SSP. The Agency is required to produce an SSP template with appropriate controls for new modules replacing the FMMIS system. The SSP template will document controls used and carried forward to FX Project Owners.

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

5.1.1 AGENCY-WIDE POLICIES

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 Agency 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 MES. The existing systems were implemented before the development of Strategic, Programmatic, and Technology strategies, standards, and guidance developed by the SEAS Vendor. The

Agency and vendors that operate those systems have control of and address audit reviews and findings. To protect the Agency and systems from exploitation of vulnerabilities, this document does not describe system analysis of vulnerabilities or control deficiencies.

The review of existing MES systems produced:

- A summary of governance for FMMIS connected systems (below)
- Recommendations for secure development
- Inputs to the security standards (documented in the TSRG and Appendix A)

5.1.2.1 GOVERNANCE ANALYSIS

Exhibit 5-1: FMMIS Connected System Governance lists systems and additional controls and Agency-wide controls for systems that connect and share data with 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 Tirion Solutions. Logging and reporting provided as necessary.	Gainwell Orlando 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 AHS. Logging and reporting provided as necessary.	Gainwell Orlando Data Center
Third Party Liability	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII PHI	Currently designed, developed, implemented by HMS. Logging and reporting provided as necessary.	Not available
Prior Authorization	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII PHI	Currently designed, developed, implemented by eQHealth. Logging and reporting provided as necessary.	Not available

System Name	Access Management	Data Types Processed or Stored	Governing Controls	Inherited Control Environment
Provider Data Management System	MEUPS - Joiner/Leaver process controlled by Business Owner request and Agency review process	PII	Currently designed, developed, implemented by Gainwell. Logging and reporting provided as necessary.	Gainwell Orlando Data Center
Health Quality Assurance (HQA) Licensure VERSA	Standalone Security DB	PII	Not available	DMS Division of State Technology Data Center
Home Health Electronic Visit Verification System	Standalone Security DB	PII PHI	Implemented by Centric based on Tellus system. Logging and reporting provided as necessary.	Not available
Care Provider Background Screening Clearinghouse	Standalone Security DB	PII	Currently designed, developed, implemented by Tellus. Logging and reporting provided as necessary.	DMS Division of State Technology Data Center

Exhibit 5-1: FMMIS Connected System Governance

5.1.3 Recommendations for Secure Development of FX

The following alternatives for developing FX projects to use Agency processes and resources should be considered:

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

These recommendations continue to have FX Project Owners primarily responsible for secure development. Responsibility for secure development **does not mean** delegation of security governance and responsibility for security control selection to project owners without any provision for direct oversight by the Agency besides receiving reports of some kind from the project owners. FX projects are expected to have security controls equivalent to or greater than

those used for FMMIS. The SEAS Vendor shall 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 FX Project Owners any updates that affect development or operations of FX.

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 points for enterprise security audits.

CMS provides significant guidance on the security compliance evaluation phases and activities in the system development life cycle. FX shall align with the major security compliance and evaluation processes defined by CMS. This section elaborates additional security compliance evaluation and analysis guidance specific to FX'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 the 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.

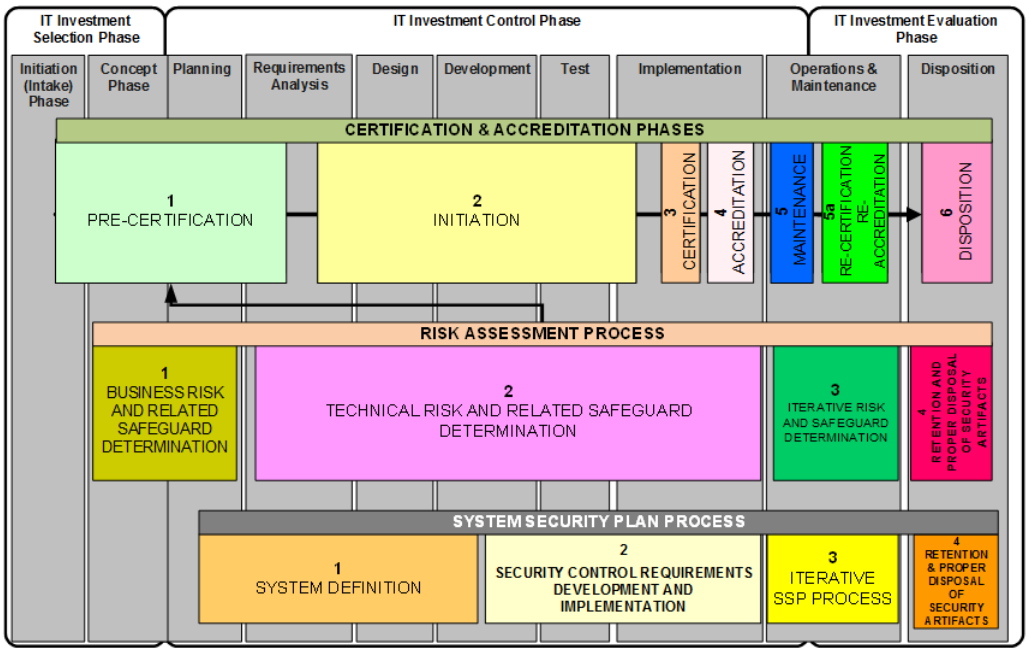

Exhibit 5-2: System Delivery Management Security Phases

The Agency Planning and Security Office 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 RA and SSPs are significant artifacts that report much of the information of interest to enterprise security and risk management groups.

The system delivery security phases produce security artifacts used to evaluate compliance with security standards. FX 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 FX Projects Repository. The template for each artifact type originates from the corresponding CMS eXpedited Life Cycle (XLC) template. Security templates will evolve with FX specific customizations throughout.

PHASES		Initiation & Concept	Planning	Requirements Analysis	Design	Development	Testing	Implementation	Operations & Maintenance	Disposition
ARTIFACTS/ INFORMATION	**REVIEWS**	AR, ISR	PBR	RR	PDR, DDR	ERR1 (VRR)	ERR2 ERR3 (IRR, PRR)	ORR	PIR, AOA	DR
System Security Category		**P/F**								
Privacy Impact Assessment		**P**	**I**	**I**	**I**	**I**	**F**		**U**	
System Security Plan		**P**	**B**	**I**	**I**	**I**	**F**		**U**	**U**
Information System Risk Assessment		**P**	**I**	**B**	**I**	**I**	**F**		**U**	**U**
Security Requirements		**P/F**							**U**	
Security Control Description				**P**	**B**	**F**	**U**		**U**	
Software Assurance Misuse Cases				**P**	**B**	**I**	**F**		**U**	
Security Control Assessment							**P**	**F**	**U**	
ATO Submission								**P/F**	**U**	
Plan of Action & Milestones								**P/F**	**U**	
CMS CIO-Issued ATO								**P/F**	**U**	
Security Monitoring Reports									**U**	
								B – Baseline F – Final I – Interim P – Preliminary U – Update Yearly		
Security Artifacts										
Security Information from Tasks										

AR- Architecture Review ISR- Investment Selection Review PBR- Project Baseline Review RR- Requirements Review PDR – Preliminary Design Review DDR – Detailed Design Review	ERR – Environment (Validation, Implementation, Production) Readiness Review ORR – Operational Readiness Review PIR – Post Implementation Review AOA – Annual Operational Analysis DR – Disposition Review

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

5.2.1 CERTIFICATION AND ACCREDITATION

FX shall 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

FX shall perform the RA processes defined by CMS. The RA 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

FX shall use the CMS formally defined SSP process. The SSP includes the following phases:

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

5.2.4 SYSTEM SECURITY PLAN DOCUMENT REQUIREMENTS

Each FX Project's security context is identified uniquely to ensure implementation of risk and control evaluations specific to each system's development and operation.

5.2.4.1 IDENTIFICATION

For projects that impact multiple systems or business areas, compliance tracking is imperative. To better facilitate that tracking, the Agency will assign an identification number to each project component. The Agency ISM will assign a Security Unique Identification Number (SUID) to associate the project with an authorization package and all future operational assessment and Plan of Action and Milestone (POA&M) reports.

5.2.4.2 SECURITY POINTS OF CONTACT

FX Project Owner shall maintain a roster of key security personnel in the SSP for each project. The specific titles will vary, however there must be an individual tasked with the roles listed below.

The roster at a minimum shall include:

- A project security officer, supported by the project director of operations if they are not available
- A project security event manager, supported by the project director of development if they are not available
- A project director of development
- A project director of operations
- All team members of the Project Security Event Management Team

The FX Project Owner shall maintain the roster of contact information for each team member and validate and send to the Agency ISM on at least a quarterly basis.

5.2.4.3 AUTHORIZATION BOUNDARY

FX projects shall have their boundaries identified, defined, and documented within the SSP to facilitate the accurate categorization and selection of security controls. Definition of the project boundaries provides the authorizing official with accurate context to evaluate the project and resident information. Boundary definition must occur before security categorization and ensures the accurate categorization of the FX Project.

The authorization boundary contains:

- A narrative description and purpose of the project including business processes and FX functions supported
- A roster of all application components with version levels, capabilities, and functions supported by each. Examples of components include COTS products, configuration files, Java Archives (JARs), Web Archives (WARs), etc.
- 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 FX
- The management team and personnel developing and maintaining FX
- The network boundary drawings showing the edge of communication and data flow
- A data flow diagram that shows production and consumption of project data, and categorizes the information as external or internal to the project

5.2.4.4 CATEGORIZATION

The FX Project Owner shall evaluate the project's 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. CMS classifies all MMIS implementations as Moderate. Should requirements change in the future then the CMS System Security Categorization Worksheet would be used to determine the correct classification level.

Rule 60GG-2, Florida Administrative Code, and the NIST Risk Management Framework require the following minimum information set from the vendor to accurately categorize FX:

- Full descriptive name and all associated acronyms and *known as* identifiers for the version of the project evaluated
- The SUID
- The owning organization and key personnel that manages, controls, and owns the information within the project
- Purpose, functions, and capabilities of the project, and the business processes supported
- Types of information processed by the project
- 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 B –System Categorization Worksheet contains an example of the CMS Standard System Categorization Worksheet.

5.2.4.5 INTERCONNECTION AND INFORMATION SHARING

An FX Project interconnection is the direct connection of a system implemented or used in an FX Project with external systems to share data. FX Project interconnections shall be documented by the FX Project Owner and maintained in the SSP in the form of one or more of the following:

- 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 and technical overview. A MOU/A is primarily applicable to large and complex interfaces that support broader business purposes.
- The Business Associate Agreement – provides an agreement for complying with the requirements of HIPAA. The agreement is applicable if the FX Project Owner is a business associate within the meaning of the Privacy and Security Regulation, 45 CFR 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 (Application Programming Interface).

Attachments J and K – CMS Interconnection System Agreement Template and *CMS MOU Template* contain examples of the CMS ISA and MOU/A.

5.2.5 USE AND PROTECTION OF FEDERAL TAX INFORMATION DATA

In order for FX to support the storage and processing of Federal Tax Information (FTI) data, the Internal Revenue Service (IRS) guidelines documented in IRS Pub 175 must be followed. The guidelines call for the following processes to be implemented:

- Recipients of FTI data must at a minimum meet the following requirements:
  - Protect the confidentiality of information by implementing safeguards to prevent the unauthorized use of FTI data.
  - The IRS Office of Disclosure needs to be contacted with a request for approval and authorization for any use of the data other than the one originally agreed upon and authorized.
  - Movement of data between the IRS and FTI data recipients must be made following the Secure Data Transfer (SDT) program established by the IRS, which provides for encryption of the FTI data.
  - Anytime FTI data is to be used to conduct statistical analysis, tax modeling, or revenue projections, recipients of the data must notify the IRS by submitting a signed **Need and Use Justification for Use of Federal Tax Information** form and follow established guidelines.
- The recipients of FTI data are subject to on-site *Safeguard Review* evaluations by the IRS to assess the use of FTI and the measures being used to protect the data.
- The recipients of FTI data must provide secure storage methods to protect the FTI data. These methods include but are not limited to locked containers, vaults, rooms, and or/ buildings, guards, electronic security systems, fences, identification systems, and other control measures.
- Additional safeguards made to protect the FTI data can include the following:

- Training education and awareness programs are necessary to provide individuals with access to FTI with the knowledge and tools to protect the data and should be implemented by the recipients of FTI data.
- Employees and contractors must go through security screening procedures and must complete annual training and recertification courses to maintain their authorization to access FTI.
- Internal Inspections should be conducted to ensure that no unauthorized access, data breaches, or disclosures of FTI data have occurred.
- Copies of all initial and subsequent requests for FTI data must be maintained for a minimum of five (5) years.
- Access to FTI data should only be made by individuals who are authorized for its use.
- Shredding or burning of both FTI data and any material generated from it (e.g., copies, photo impressions, computer printouts, notes, working papers, etc.) should occur when the need to destruct and dispose arises. If a different method is used, it must render the FTI data unreadable and unusable.
- The recipients of FTI data must provide reasonable assurances to the IRS that only personnel with a need-to-know have access to FTI data through the use of the computer systems at the site.

- FTI data recipients must report on the procedures established and used to protect the confidentiality of FTI data received as per IRS 6103(p)(4)(E).
  - Reports sent to the IRS Office of Safeguards via email should be transmitted following IRS-approved encryption methods. Refer to IRS 6103(p)(4)(E).
  - Safeguard security reports should be redacted and maintained by the recipients.
- When FTI data is no longer needed, recipients must either return or destroy the FTI data (by approved methods discussed earlier) they received, as well as any copies that were made. Refer to IRC 6103(p)(4)(F).

  Recipients must adhere to and follow the steps, criteria, and frequency to protect FTI data as stated in the *Audit Review, Analysis, and Reporting (AU-6)* guideline. The guideline also specifies the steps to be followed when unauthorized access or breaches of FTI data are discovered.

- Recipients must set up an information system that protects all the audit information and audit tools used to protect FTI data from unauthorized access, modification, or deletion as stated in *The Protection of Audit Information (AU-9)* guideline.

  Recipients must retain audit records of events affecting FTI data for seven (7) years to support after-the-fact investigations of security incidents, as well as to meet regulatory and Agency information retention requirements as stated in listed in Section 9.3.3.2, *Audit Events (AU-2) the Audit Record Retention (AU-11)*.

- Details on the multiple guidelines to be followed for incident response controls, which apply to both physical and information system security relative to the protection of FTI can be found in Section 9.3.8 *Incident Response* of IRS Publication 1075.

References: For additional details, information, and a complete description of the guidelines on FTI can be found at the following link: https://www.irs.gov/pub/irs-pdf/p1075.pdf.

5.2.6 CONTROLS

Security controls are the administrative, physical, and technical measures prescribed to protect the confidentiality, integrity, and availability of FX. 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 a project from a Common Control Provider (e.g., data center, cloud operator, access broker, etc.)
- **Project Specific Controls**: a security control that is designed and implemented for a specific project, 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 a project

5.2.6.1 CONTROL SELECTION AND DOCUMENTATION

FX Project Owner 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
- Project availability requirements
- Agency security program governance as prescribed

The specific controls applicable to a project will vary by the scope of the project. 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 FX Project Owner shall select controls necessary to ensure levels of confidentiality, availability, and integrity appropriate for the security categorization of the project.

FX Project Owners shall document proposed controls according to the NIST Cybersecurity Framework (CSF) and its defined categories. **Exhibit 5-4: NIST Cybersecurity Framework** shows the major components of the NIST CSF.

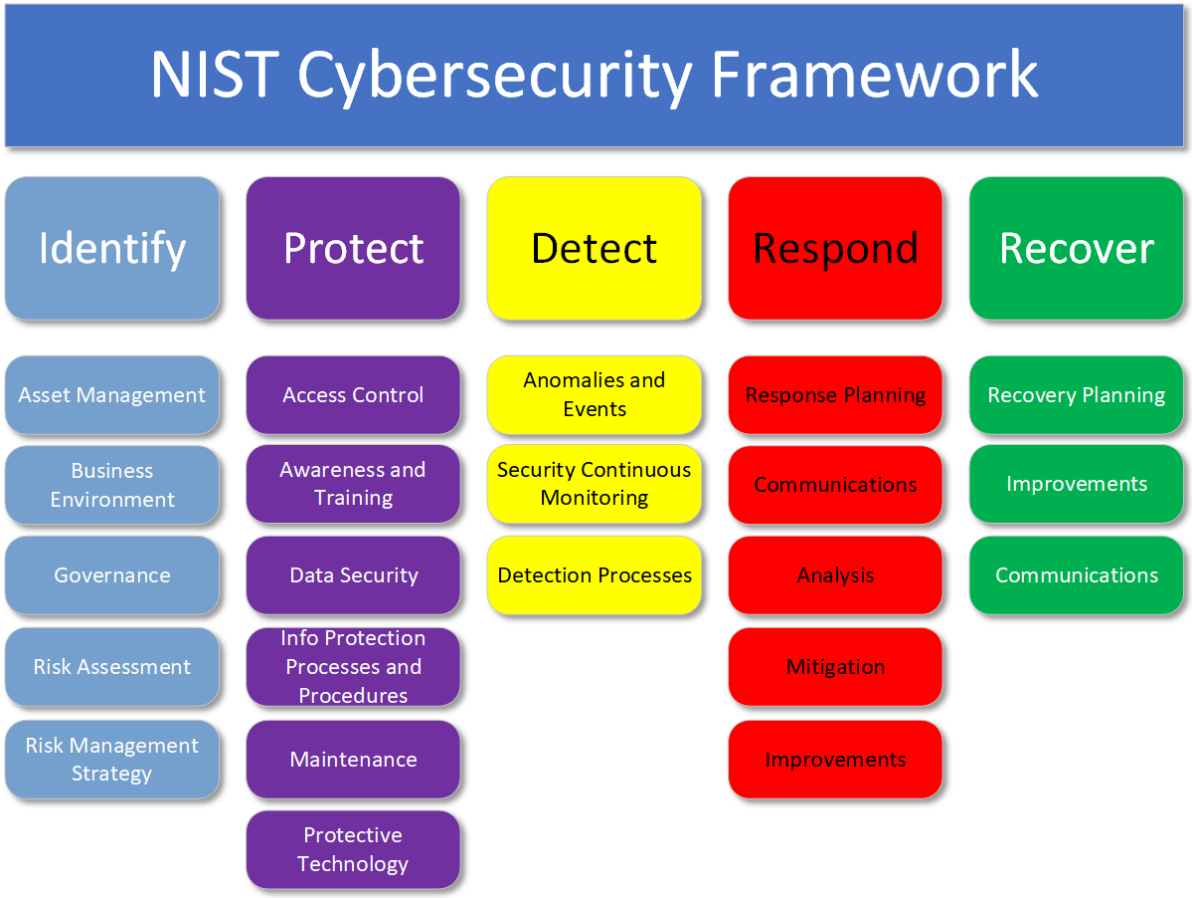

Exhibit 5-4: NIST Cybersecurity Framework

FX Project Owners shall document selected controls according to the CMS Risk Management Handbook Vol I Chapter 12: Security & Privacy Planning.

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

5.2.6.2 CONTROL IMPLEMENTATION

Security control implementation is comprised of four stages. FX Project Owners shall ensure control implementation occurs throughout the FX Project Life Cycle as described in **Exhibit 5-5: Security Control Implementation Life Cycle.**

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 *Attachment I – OWASP Application Security Standard* for list of required controls.	Document control statements for each requirement in accordance with the 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 the 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 FX Project Owner and the Agency ISM will review and update the SSP to address changing standards and operational requirements. The Agency Division of IT may use contracted services such as staff augmentation or cybersecurity specialist firms to assist with this responsibility.

5.3 PROJECT DEVELOPMENT SECURITY LIFE CYCLE

Florida Cybersecurity Standards (Rule 60GG-2, F.A.C.) requires information system owners and developers to use the NIST CSF to ensure information security for systems that support operations and assets of Florida Agencies. Within the CSF, NIST prescribes the 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.

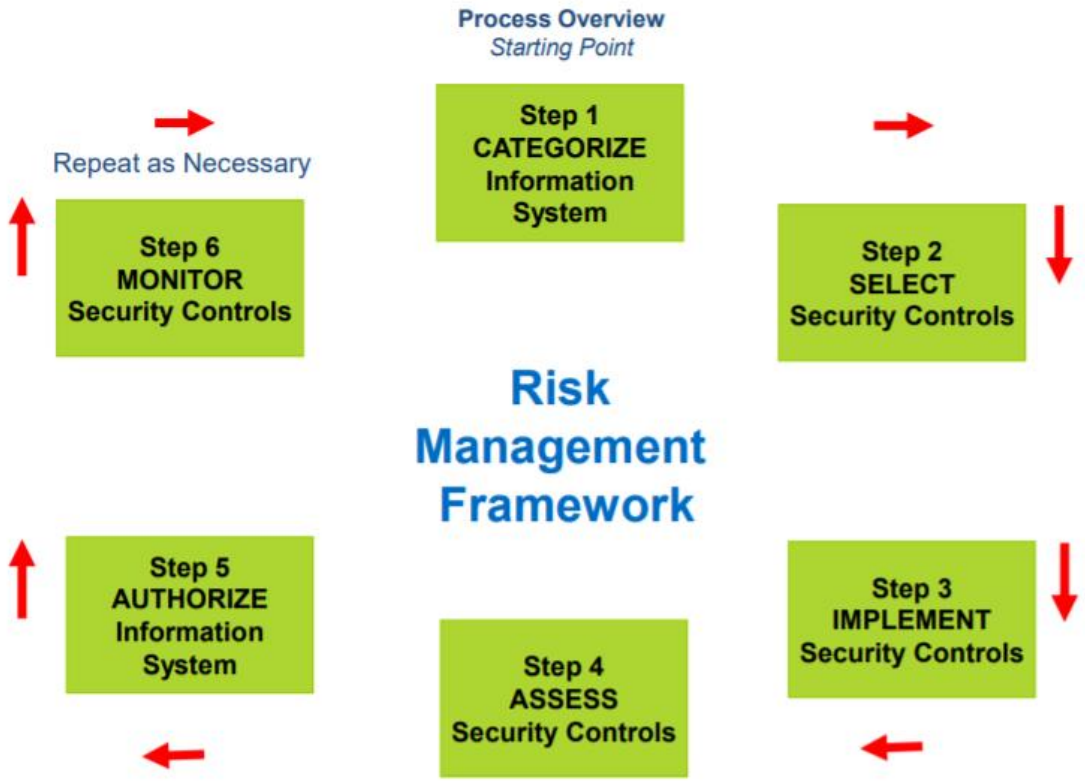

Exhibit 5-6: NIST Risk Management Framework

FX Project Owners shall use the NIST RMF to develop, document, implement, and communicate the security controls used to secure the project.

5.3.1 AUTHORIZATION TO OPERATE

The Agency will evaluate FX to ensure development for operations with an acceptable level of risk. The following sections outline the evaluation and process to achieve an ATO for a project within the specified environment.

FX Project Owner shall comply with all applicable evaluation processes, and coordinate review and approval of proposed CMS Security with the Agency ISM.

The CMS Security Assessment Review (SAR) provides an assessment of security controls. Because the module vendor or an independent third party performs the SAR, the assessment is independent of the FX Project Owner. CMS will evaluate the Agency ATO based on project specific risk considerations.

5.3.1.1 TESTING AND CERTIFICATION REVIEWS

Exhibit 5-7: Testing and Certification Reviews by SDLC Phase shows the testing and certification reviews organized by the SDLC phases defined in the FX Security Standards.

SEAS VENDOR TECHNICAL EXPERTISE PROVIDED	REQUIREMENTS ANALYSIS AND DESIGN PHASE	DEVELOPMENT AND TEST PHASE	IMPLEMENTATION PHASE	OPERATIONS & MAINTENANCE PHASE
AHCA Vulnerability Management Evaluation		✓	✓	✓
AHCA Application Security Testing Evaluation		✓	✓	✓
CMS Security Assessment Review	✓	✓	✓	✓
DMS Division of State Technology (DST) Risk Assessment	✓	✓	✓	✓

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

- **AHCA Vulnerability Management Evaluation** – acceptable risk as defined by the AHCA Security Program
- **AHCA Application Security Testing Evaluation** – acceptable risk as defined by the AHCA Security Program
- **CMS Security Assessment Review** – acceptable risk as defined by the CMS Acceptable Risk Framework
- **DMS/DST Risk Assessment** – acceptable risk as defined by Rule Chapter 60GG-2, F.A.C. (Florida Cybersecurity Standards)

5.3.1.2 INTERIM AUTHORIZATION TO OPERATE

CMS will grant an IATO to authorize a project for operation with risks that are not permanently acceptable. Granting an IATO is temporary and requires the development of a POA&M in accordance with the CMS Risk Management Handbook Volume I Chapter 1 to remediate all unacceptable risks and monitor all residual 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 project.

5.3.1.3 FINAL AUTHORIZATION TO OPERATE

CMS will grant a Final ATO upon successful mitigation of risks to an acceptable level. This ATO grants operation for three (3) years. FX Project Owners 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, CMS can issue a DATO and cease project operations.

SECTION 6 DATA SECURITY MANAGEMENT AND REPORTING

This section describes the:

- Process to track and report the security compliance to the Technology Standards Committee (TSC)
- Security reporting framework and inventory of security reports
- Process to update security standards

The Technology Standards Committee is part of the structure for project, technology, program and strategic decision-making and direction setting.

6.1 FX Data Security Compliance Reporting

The types of FX 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 occur throughout the system delivery management stage of the FX 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 Artifact Reviews

FX Project Life Cycle defines the FX Project Life Cycle Artifacts produced by FX projects. There are many security related project artifacts applicable to FX projects. The specific artifacts produced for each project will vary based on scope and complexity of the project. The SEAS Vendor reviews FX Project deliverables and provides findings and recommendations.

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: FX Project Management Standards*.

Project specific artifacts shall be stored in the FX Projects Repository and are accessible to authorized parties such as the Technology Standards Committee. Appropriate Agency security staff shall also have access to project security artifacts.

6.1.1.2 PROJECT LIFE CYCLE REVIEWS

FX 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 shall be stored in the FX Projects Repository specified for each project and are accessible to authorized parties. Appropriate Agency security staff shall also have access to project life cycle review 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 in the FX Projects Repository and are accessible to authorized users.

The IV&V Vendor 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.

The SEAS Vendor shall be responsible for performing a security analysis of the FX Project Owner's SSP upon completion and following any revisions, to ensure compliance with applicable standards of the Agency, State, CMS, and other involved stakeholders. The analysis shall be documented using the format provided in *Attachment E - FX Systems Security Analysis*.

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 shall provide reports of findings, recommendations, and decisions that need to be made related to security standards compliance to the Technology Standards Committee.

The security compliance reporting content, compliance reporting content distribution, and recommendations, described in SEAS deliverable *T-6: Technology Standards* Section 4 and further elaborated in *Attachment E – Technology Standards Communication, Support, Compliance, and Compliance Reporting Procedures*, 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 Technology Standards Committee and the audiences specified per reporting requirement.

6.2 Data Security Process and Criteria

This section identifies requirements for security processes and specific tools in use by the Agency or available and/or open to FX Project Owners.

6.2.1 Operational Security

The FX Project Owner shall maintain secure operations of FX data 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. FX Project Owners shall make projects available or perform testing and evaluation during all development, implementation, and operational phases. The FX Project Owner is responsible for vulnerability testing. The decision to use Agency resources or other vendors to perform independent vulnerability testing will be made by the Agency on a project-by-project basis. The FX Project Owner will be required to perform vulnerability testing on a quarterly or annual basis, at the Agency's discretion.

At a minimum, the vendor vulnerability testing should include Network, Application, Code, Compliance, SSL, and Database Scans. Penetration testing should also be performed to validate the significant vulnerabilities discovered during the vulnerability testing.

6.2.1.2 Application Security

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

Attachment I – OWASP Application Security Verification Standard contains the OWASP Application Security Verification Standard (ASVS) with examples of misuse cases. FX Project

Owner shall address all application development controls for the applicable Verification level in the SSP control selection and implementation documentation.

The Agency has acquired IBM AppScan for use in application development and Rapid7 InsightVM for vulnerability management. Although OWASP provides a minimum basis, the guidance for FX Project Owners is to not rely solely on OWASP but to consider the Agency tools as the minimum level of compliance.

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 Framework

Exhibit 6-1: Security Reporting Framework shows a framework of security related reporting for FX projects.

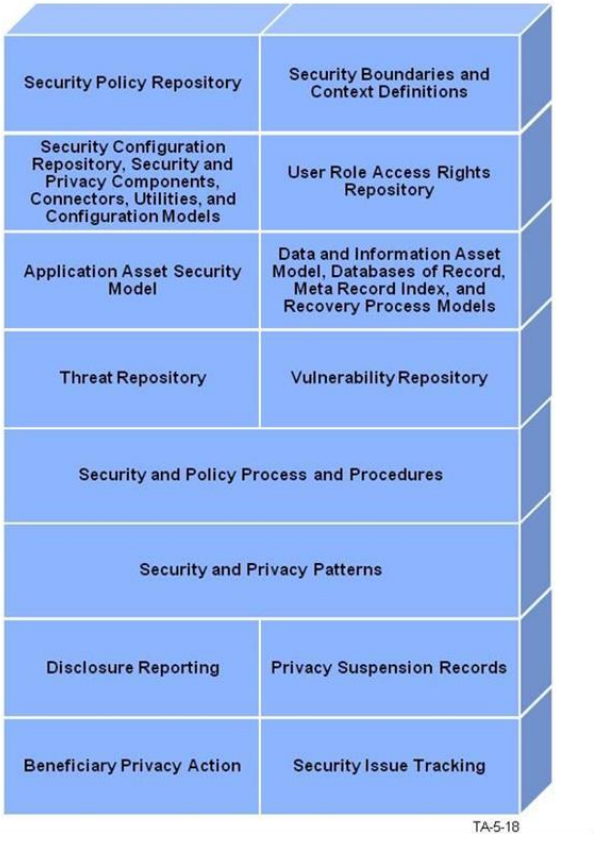

Exhibit 6-1: Security Reporting Framework

6.3.2 INVENTORY OF SECURITY REPORTING REQUIREMENTS

FX has formal security reporting requirements, as identified and described in the Project Process Agreement (PPA). **Exhibit 6-2: Security Reporting Requirements** lists security reporting requirements and the audience of each report. The ISM and the project teams review reports for informational purposes. Issues and decisions resulting and direction setting, resulting from content of reports, would follow the FX Governance processes.

NAME	FREQUENCY	REQUIREMENT	AUDIENCE
System Security Category and System Categorization Worksheet (*see Appendix A – Attachments A & B*)	Project Initiation and Ad Hoc for Significant Change	Establish the system security levels and electronic authentication (e-Authentication) assurance levels for the information and information systems that support the operations and assets of CMS.	CMS, Agency ISM, Technology Standards Committee, DMS Division of State Technology - Chief Information Security Officer (CISO)
System Security Plan (*see Appendix A – Attachment C*)	Annual and Ad Hoc for Significant Change	Management review, update, and certification of System Security Plan.	CMS, Agency ISM, Technology Standards Committee, DMS Division of State Technology - CISO
Information Security Risk Assessment Template (*see Appendix A – Attachment D*)	Annual and Ad Hoc for Significant Change	Risk assessment in accordance with CMS, DMS Division of State Technology, and Florida Cybersecurity Standards. Documents and coordinates with System Security Plan (SSP) to address findings from audits, assessments, and standards reviews.	CMS, Agency ISM, DMS Division of State Technology - CISO, Technology Standards Committee
Vulnerability Reports	In accordance with agreed to reporting frequency, either quarterly or annually at the Agency's discretion	Systematic examination of systems and applications in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.	CMS, Agency ISM, DMS Division of State Technology - CISO, Technology Standards Committee
Security Event Response	As needed in accordance with Security Event Response Plan	Collect and submit information in accordance with documented SERP. Events will be monitored and managed by SIEM tool.	Agency ISM
POA&M (*see Appendix A – Attachment G*)	In accordance with agreed to reporting frequency	Document progress toward mitigating risks allowed for issuance of IATO.	Agency ISM, CMS, DMS Division of State Technology - CISO, Project Security Plan

NAME	FREQUENCY	REQUIREMENT	AUDIENCE
Vendor Security Score Card (*see Appendix A – Attachment H*)	During procurement	Provide independently verified security score rating.	Procurement Team, Agency Contract Manager, Agency ISM

Exhibit 6-2: Security Reporting Requirements

6.4 SECURITY STANDARDS UPDATE PROCESS

As the result of compliance reporting findings or other events, the SEAS Vendor and the Agency may need to update the security standards. Keeping security standards updated improves data protection and privacy. It is the SEAS Vendor's and 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: Technology Standards* Section 4: Technology Standards Reference Guide is a Word document that describes the structure, maintenance, and communication of 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. 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 shall be reviewed and updated as necessary.

EVENT	DESCRIPTION
Annual Review	The SEAS Vendor shall 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 shall 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.

EVENT	DESCRIPTION
Publication of new MITA Standard(s)	If there is a material change in MITA Part III – Technical Architecture, the SEAS Vendor shall conduct a review of the security standards in the TSRG as compared to MITA. If required, existing security standards shall be updated and new security standards relevant to the Agency shall be added to the TSRG.
FX Project Need	As part of an FX Project, the FX Project Owner may recommend additional standards to be included in the TSRG. The SEAS Vendor shall conduct a review of existing standards to determine appropriateness and need to add to the TSRG.

Exhibit 6-3: Security Standards Refresh Events

APPENDIX A – SUPPORTING DOCUMENTATION

The following attachments are stored in the FX Projects Repository to serve as supporting documentation for the *T-8: Enterprise Data Security Plan*. (i.e., FX Hub > Standards & Plans > Category: Technology).

ATTACHMENT A – SYSTEM SECURITY LEVELS

Attachment A – describes the system security levels for the information and information systems that support the operations and assets of CMS.

ATTACHMENT B – SYSTEM CATEGORIZATION WORKSHEET

Attachment B – worksheet that categorizes the information system and the information resident within that system based on the Federal Information Processing Standards Publication 199 (FIPS 199).

ATTACHMENT C – SYSTEM SECURITY PLAN (SSP) EXAMPLE TEMPLATE

Attachment C – provides a copy of the current version of the CMS approved SSP template at the time of publication of this document. Vendors must use the most current version of the CMS approved template for their SSP.

ATTACHMENT D – INFORMATION SECURITY RISK ASSESSMENT TEMPLATE

Attachment D – contains a list of threats and vulnerabilities, an evaluation of current security controls, their resulting risk levels, and any recommended safeguards to reduce risk exposure. The IS RA also supports risk management through the evaluation of risk impact upon the enterprise security model.

ATTACHMENT E – SYSTEM SECURITY ANALYSIS

Attachment E – describes the security analysis of FX Systems to identify security governance, practices, and standards applicable to FX projects to improve security and data protection for systems in FX. This document will evolve in periodic iterations throughout the life of FX.

ATTACHMENT F – RISK MANAGEMENT HANDBOOK, CHAPTER 8: INCIDENT RESPONSE

Attachment F – describes standard operating procedures that facilitate the implementation of security controls associated with the Incident Response (IR) family of controls taken from the most current version of the National Institute of Standards and Technology (NIST) Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations.*

ATTACHMENT G – POA&M TEMPLATE

Attachment G – includes a template that facilitates a disciplined and structured approach to tracking risk mitigation activities in accordance with the Agency priorities. The POA&M includes security findings for the system from periodic security assessments and ongoing continuous monitoring activities. The POA&M includes the Vendor's intended corrective actions and current disposition for those findings.

ATTACHMENT H – PERFORMANCE MEASUREMENT GUIDE FOR INFORMATION SECURITY

Attachment H – is a guide to assist in the development, selection, and implementation of measures to be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and security programs.

ATTACHMENT I – OWASP APPLICATION SECURITY VERIFICATION STANDARDS

Attachment I – is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test and verify secure applications.

ATTACHMENT J – INTERCONNECTION SECURITY AGREEMENT (ISA)

Attachment J – is a template used to establish procedures for mutual cooperation and coordination between CMS and other organizations.

ATTACHMENT K – MEMORANDUM OF UNDERSTANDING (MOU) TEMPLATE

Attachment K – is a template that details the agreement between CMS and its organizations regarding the principles under which the initiative will be implemented and operated. It also outlines the activities which CMS and its organizations agree to conduct in preparation for planned implementation of the initiative.

ATTACHMENT L – CMS REQUIRED CONTROL BASELINES

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

APPENDIX B – REFERENCE TO OTHER DELIVERABLES

The following attachments are stored in the FX Projects Repository to serve as supporting documentation for the *T-8: Enterprise Data Security Plan* (i.e., FX Hub > Standards & Plans > Category: Technology).

SEAS DELIVERABLE T-6: TECHNOLOGY STANDARDS

The *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 LIST

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.

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.