Centers for Medicare & Medicaid Services
Centers for Medicaid and CHIP Services

STREAMLINED MODULAR CERTIFICATION GUIDANCE

VERSION 2.0

Record of Changes

Version	Date	Description of Change
1.0	April 14, 2022	Version 1.0 published with SMD #22-201
2.0	October 21, 2025	Electronic Visit Verification (EVV) Outcomes Based Certification (OBC) will now follow SMC; refer to subsection 3.1, EVV OBC Alignment with SMC.
		Removed the CMS-required outcome appendix from this document; they will now be located only in the MES Certification Repository on CMS GitHub.
		Clarified what should follow SMC; refer to Section 2. Scope of Certification.
		Introduced a new required status report template available at the MES Certification Repository Templates page.
		Updated the Intake Form template as follows (refer to the MES Certification Repository for the template): • Renamed to SMC Intake Form • Updated and clarified text in the instructions row on all tabs • Removed the Metric Description column from the Outcomes & Metrics tab (leaving just the Metrics ID) • Added a new Required Artifacts tab • Included one blank SMC Intake Form and one pre-populated SMC Intake Form with EVV outcomes
		Updated for the now required Operational Report Workbook (ORW) template that is available at the MES Certification Repository.
		Introduced a new CEF metric for all MES modules; refer to the MES Certification Repository for metric details.

Table of Contents

List of Figures

List of Tables

1. About Streamlined Modular Certification

Streamlined Modular Certification (SMC) aims to reduce the burden on states and the Centers for Medicare & Medicaid Services (CMS) while ensuring compliance with statutory and regulatory requirements. SMC delivers consistency and accountability for Medicaid Enterprise Systems (MES), a term synonymous with mechanized claims processing and information retrieval systems (MCPIRS) as defined in 42 CFR 433.111(b). MES encompasses the totality of Medicaid information technology (IT) systems used by State Medicaid Agencies (SMA) to manage, monitor, and administer state Medicaid programs.

The SMC approach is designed to:

- Demonstrate measurable improvements to a state's Medicaid program resulting from the delivery of a new module.
- Use data and testing to evaluate the successful deployment of systems and guidance for future funding decisions.
- Facilitate operational reporting on system performance and functionality, ensuring continuous oversight of data and evidence to demonstrate the consistent achievement of required and desired outcomes.
- Alleviate the certification process burden on states and CMS while maintaining CMS's obligation to ensure that all systems meet statutory and regulatory requirements.

2. Scope of Certification

In accordance with 42 CFR 433.116, Federal Financial Participation (FFP) is available at 75 percent of expenditures for the operation of a CMS-approved MCPIRS. The SMA must operate these systems and/or modules, either directly or through a documented agreement on its behalf.

While all MES activities are subject to oversight via outcomes, metrics, and/or operational reporting to demonstrate continued benefit to the Medicaid program, some activities do not require certification to receive 75 percent FFP. Outcomes and metrics are generally required for states receiving enhanced funding, except for routine activities or planning and operational functions like hardware maintenance, gap analysis, development of procurement instruments, and security patches.

The following list of definitions of systems, modules, and services is necessary to understand when determining whether certification is required for the approval of retroactive enhanced funding for operations.

- **System** – "System" refers to all modules or components developed to support the Medicaid Management Information System (MMIS) and/or eligibility and enrollment (E&E) system that may be implemented as discrete, independent, interoperable elements. For example, an E&E system is used to process applications from Medicaid and/or Children's Health Insurance Program (CHIP) applicants and beneficiaries to determine eligibility for enrollment in the Medicaid or CHIP programs, as well as change in circumstance updates and renewals, while the MMIS is used to process claims for

Medicaid payment from providers of medical care and services furnished to beneficiaries under the medical assistance program and to perform other functions necessary for economic and efficient operations, management, monitoring, and administration of the Medicaid program.[1]

- **Module** – "Module" means a packaged, functional business process or set of processes implemented through software, data, and interoperable interfaces that are enabled through design principles in which functions of a complex system are partitioned into discrete, scalable, reusable components.[2] The most frequently implemented MES modules are listed in Table 1 below with their general functions.

- **Services** – "Service" means a self-contained unit of functionality that is a discretely invokable operation. Services can be combined to provide the functionality of a large software application.[3]

- **Shared Service** – "Shared service" means the use of a service, including SaaS, by one part of an organization or group, including states, where that service is also made available to other entities of the organization, group, or states. Thus, the funding and resourcing of the service is shared and the providing department effectively becomes an internal service provider.[4]

- **Software-as-a-Service (SaaS)** – SaaS means a software delivery model in which software is managed and licensed by its vendor-owner on a pay-for-use or subscription basis, centrally hosted, on-demand, and common to all users.[5]

Table 1, Examples of MES Modules, presents a non-exhaustive list of such systems and modules.

[1] 42 CFR § 433.111(b)(1-2)
[2] 42 CFR § 433.111(h)
[3] 42 CFR § 433.111(f)
[4] 42 CFR § 433.111(g)
[5] 42 CFR § 433.11(j)

Table 1. Examples of MES Modules

Module (Typical Function)	Module Abbreviation
Claims Processing (Receives claims from a fee-for-service (FFS) provider and processes them for payment or denial.)	CP
Decision Support System Data Warehouse (Pulls data from multiple sources into a single data repository for advanced analytics and decision-making support. The DSSDW should perform more than services such as displaying and exchanging data.)	DSSDW
Electronic Visit Verification (Electronically verifies that providers delivered services as billed during in-home visits for Personal Care Services and Home Health Care Services.)	EVV
Eligibility & Enrollment (Includes both Modified Adjusted Gross Income (MAGI) and non-MAGI processes for eligibility determination and enrolling individuals in and retaining Medicaid coverage.)	EE
Encounter Processing System (Ingests encounter data, including submissions and re-submissions, from managed care organizations (MCOs) and returns quality transaction feedback. The data is used for capitation rate setting, MCO contract monitoring, and enforcement.)	EPS
Financial Management (Calculates FFS payment or recoupment amounts and initiates payment or recoupment action. It may also support provider appeals, capitation payments, drug rebates, and third-party liability amounts.)	FM
Health Information Exchange (Electronic exchange of clinical information that allows health care providers and patients to access and securely share a patient's medical information, provided the Medicaid agency owns, operates, and actively uses the HIE. If the Medicaid agency only receives reports from HIE, it is classified as a service.)	HIE
Long-Term Services and Supports (Enrolls members who have difficulty with self-care due to aging, chronic illness, or disability in LTSS programs. This includes assessing needs, documenting care plans, and facilitating case management.)	LTSS
Member Management (Assigns enrolled members to an MCO (voluntary or mandatory) or FFS provider and supports member communications.)	MM
Pharmacy Benefit Management (Performs pharmacy claims adjudication, drug rebate administration, drug utilization review, and preferred drug list oversight.)	PBM
Prescription Drug Monitoring Program (Tracks controlled substance prescriptions to prevent misuse and improve patient safety, provided that the Medicaid agency owns, operates, and uses the PDMP.)	PDMP
Program Integrity (Analyzes data to identify, monitor, and prevent fraud, waste, and abuse; also provides case management functionality.)	PI
Provider Management (Screens and enrolls Medicaid providers, maintains up-to-date provider information, and supports provider communications.)	PM
Third-Party Liability (Identifies other sources of insurance coverage to ensure that the appropriate party pays for services.)	TPL

Standalone services, including shared services, deployed in support of and/or contribute to an approved MCPIRS, are not required to receive discrete approval for enhanced funding for maintenance and operations. States must still define outcomes and metrics in Advanced Planning Documents (APD) and submit monthly operational reports using the Operational Report Workbook and upload the file to the appropriate metrics file location in the CMS designated repository. The following non-exhaustive list presents examples of state Medicaid standalone services and operational activities that do not require certification[6]:

[6] If a state needs additional clarity on other services, the CMS MES State Officer can advise on a case-by-case basis.

- Services with stand-alone disaster management systems to enhance services for disaster and crisis response teams
- Services leveraged to allow for secure messaging services
- Services leveraged to make data available to support meeting state and federal requirements for reporting standardized quality metrics, and/or standardized public health reporting
- Services that only provide passive inputs in the format of reports (instead of driving specific business processes)
- Services allowing states to receive updates regarding available housing for their Home and Community Based Services Medicaid beneficiaries
- Services providing Admission, Discharge, and Transfer notifications, also referred to as Encounter Notification Services
- Services that provide health and human services agencies with registries of beneficiaries at shelters during natural disasters
- Services that only provide data mapping or extract, transform, and load capabilities
- Services that only provide data definitions and extracts to subscribing stakeholders
- Affordable Care Act (ACA) exchange intake portal services that integrate consumer eligibility and enrollment portals for both state-based exchange and Medicaid
- Services to enable Preadmission Screening and Resident Review, designed primarily for pre-screening for admission to a Medicaid-certified nursing facility
- Auxiliary services that interact with MES and/or non-MES systems to facilitate Medicaid data exchanges
- Other services, including design, development, implementation (DDI) service contracts for enhancements, system configuration or installation, reconfiguration of an existing module, transitioning to cloud technology, application interfaces, platform, infrastructure development, quality assurance, etc.

3. Elements for Streamlined Modular Certification

The SMC process is structured to address the following three elements for MES:

1. **Conditions for Enhanced Funding (CEF)**
    a. To receive enhanced federal matching funds for MES expenditures, states must ensure that their systems comply with all conditions for enhanced funding as specified in 42 CFR 433.112(b) and remain compliant with federal Medicaid requirements once operational per 42 CFR 433.116. Refer to Appendix A, Conditions for Enhanced Funding (CEF) for the 22 conditions that must be addressed, refer to the MES Certification Repository for the required and example evidence.
2. **Outcomes**
    a. Outcomes describe the measurable improvements to a state's Medicaid program resulting from the delivery of a new module or enhancement to an existing system. These outcomes should support Medicaid program priorities, be directly enabled by

the state's IT project, and be stated in the APD. CMS encourages states to develop measurable, achievable outcomes reflecting the MES project's short-term goals.

b. **CMS-required outcomes** are based on statutory or regulatory requirements and provide a baseline for MES, ensuring efficient, economical, and effective administration of the state's Medicaid program. Refer to the MES Certification Repository for the module-specific CMS-required outcomes. A state must use all outcomes from the applicable module. If the module includes additional functionality, the state should create corresponding state-specific outcomes.

c. **State-specific outcomes** address unique circumstances or characteristics of the state and its Medicaid program, focusing on improvements not covered by CMS-required outcomes. For example, a state may seek funding to increase no-touch eligibility determinations or improve encounter data quality for better oversight of managed care entities. States requesting enhanced FFP for systems that meet business needs beyond minimum legal requirements should work with their CMS MES State Officer to finalize these outcomes.

   States may need to revisit and update state-specific outcomes and metrics over time (and possibly during the certification process) due to lessons learned or changing Medicaid priorities. If a state revises its outcomes and metrics, an APD-Update (APD-U) is required. States should regularly consult their CMS MES State Officer to discuss such updates.

3. **Metrics**

   a. Metrics must be measurable and provide evidence that a state meets its outcomes on an ongoing basis. In accordance with 42 CFR 433.112(b)(15) and 433.116(b), (c), and (i), states must produce data, reports, and performance information from their MES modules to facilitate evaluation, continuous improvement, and transparency.

      Metrics reporting enhances accountability of IT solutions, ensuring that MES and its modules meet statutory and regulatory requirements and state program goals. State reporting also provides early and ongoing insights into program evaluation and opportunities for continuous improvement. Default metrics for MES modules and CEF are available at: MES Certification Repository.

3.1 EVV OBC Alignment with SMC

CMS has aligned the EVV OBC guidance with SMC to streamline the certification process, as announced in the State Health Official (SHO) letter #25-003[7] "Streamlining Medicaid Enterprise Systems (MES) Templates to Improve Monitoring and Oversight to Ensure Fiscal Integrity." This new letter formally sunsets the existing EVV OBC process. EVV OBC components now align with the SMC and its elements, namely CEF, CMS-required outcomes, state-specific outcomes, and metrics. States must adhere to the latest version of the *SMC Guidance*.

States are encouraged to discuss EVV module certification plans with their CMS MES State Officers, who can provide state-specific advice regarding this updated SMC guidance. As SMC

[7] https://www.medicaid.gov/federal-policy-guidance/downloads/sho25003.pdf

evolves, CMS will provide additional guidance and work collaboratively with states.

Through the adoption of the SMC process, EVV modules must now adhere to all the major components of SMC. The applicable changes for EVV include the following:

1. **CEF**
    a. The EVV module must address all 22 CEF criteria and provide unredacted evidence as listed in the MES Certification Repository. States must identify non-applicable CEF criteria within the SMC Intake Form and explain why they are not applicable. The CEF criteria replace the previous EVV8 (508 compliance) and Security 1 (security assessment report and penetration test results) outcomes, specifically CEF 09 and CEF 12.
2. **Outcomes**
    a. EVV criteria are now recognized as CMS-required outcomes.
    b. States can adopt state-specific outcomes that describe the business outcomes and benefits to the Medicaid program relevant to their EVV modules. As with all modules under SMC, states must ensure that state-specific outcomes and all respective metrics detail the benefit to the Medicaid program and population and are measurable. States must continue to provide the pre-identified EVV outcome evidence for EVV outcomes to successfully complete their review.
3. **Metrics**
    a. EVV Key Performance Indicators (KPI) are now recognized as metrics. The KPI related to the Security 1 outcome will be replaced with the new CEF metric.
    b. To schedule an EVV CR, states must submit metric data back to the go-live date and up to the most recent month-end, in addition to all entry criteria for CR. The metric data submitted for certification should span the entire period sought for retroactive certification. Given the data required for certification, states should plan strategically when scheduling their final CR to ensure there are no delays in receiving approval for certification. For example, if EVV has been operational for 14 months but the state only has 12 months of data until they run a report, the state can send the 12 months of data for scheduling the CR, which meets the entry criteria; however, the state must submit the full 14 months of data two weeks before the CR meeting.
4. **SMC Intake Form**
    a. The EVV Intake Form will be obsolete following the unification of the EVV OBC and SMC processes. All modules, including MMIS, E&E, and EVV, must be input into the SMC Intake Form, which is available on the MES Certification Repository.
    b. States will be expected to provide detailed evidence for both outcomes and the CEF for all modules, including EVV, within the SMC Intake Form.
    c. For any outcome or CEF identified as “Not Applicable,” states must provide a written justification within the SMC Intake Form.
    d. A pre-populated SMC Intake Form will be available for EVV modules only on the MES Certification Repository. Along with the adoption of the SMC Intake Form,

EVV modules will now be adjudicated with the measures of "Evidence Satisfactory," "Evidence Not Satisfactory," and "Not Applicable."

e. States will continue to receive observations and recommendations from the CMS Certification Team within the SMC Intake Form, as applicable, following the completion of an ORR and CR. The state is expected to use the updated SMC Intake Form throughout the entire certification process.

5. Operational Reporting

a. After certification, states are expected to continue operational reporting for their modules within their Operational Report Workbook (ORW). For ongoing EVV operational reporting to CMS, states are required to adhere to a minimum quarterly reporting schedule for submitting metrics, as outlined in Table 2, EVV Metric Reporting Schedule. States also have the option to submit reports monthly. The metric date within the ORW must be broken down by month.

Table 2. EVV Metric Reporting Schedule

Performance Period Covered	Report Due
October – December	End of March
January – March	End of June
April – June	End of September
July - September	End of December

3.2 The Streamlined Modular Certification Process

Streamlining the modular certification process depends on an engagement model that (a) relies on a close, ongoing partnership between CMS and the state throughout the IT investment lifecycle and (b) involves regular discussions and check-ins on state progress toward achieving shared goals for the project. States should regularly engage with their CMS MES State Officers throughout the IT investment lifecycle, especially as they begin to plan their IT investments.

As shown in Figure 1, SMC Process Touchpoints, engagement during each phase of the IT investment lifecycle will include the following touchpoints:

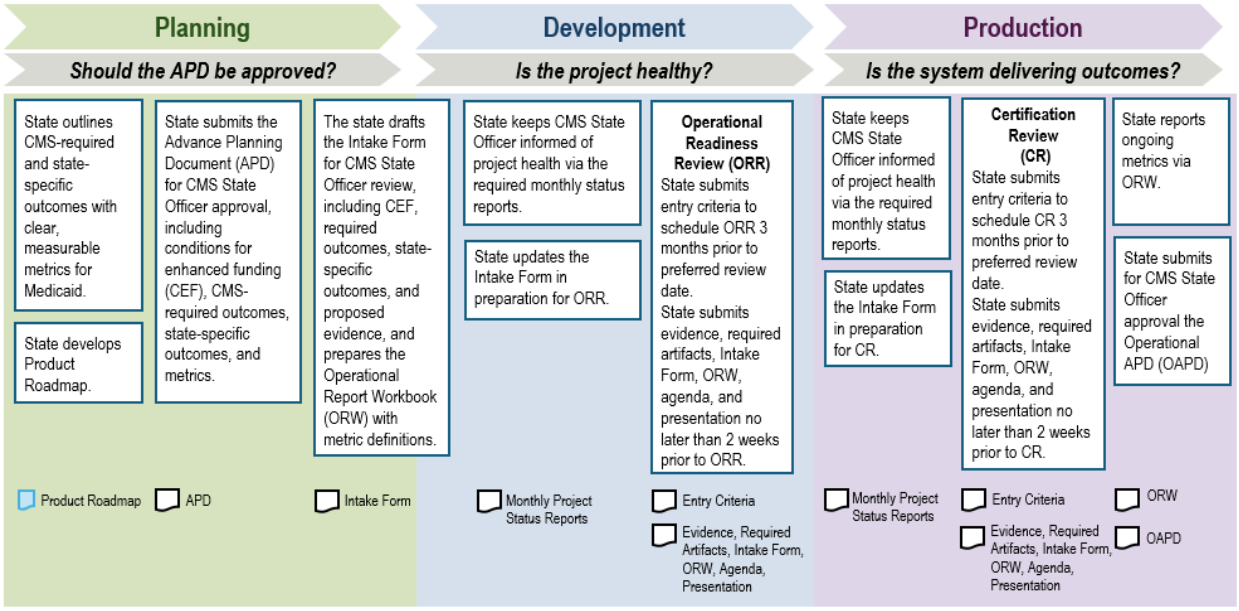

Figure 1. SMC Process Touchpoints

4. Project Planning Phase

SMC emphasizes early and frequent collaboration between states and CMS. Before drafting an APD, the state should outline planned outcomes and metrics. The state must ensure that state-specific outcomes and all respective metrics describe the benefit to the Medicaid program and population and are measurable. Next, the state should:

- Articulate a planned product roadmap that aligns with an overall state MES roadmap.
- Draft and review the APD with their CMS MES State Officer.
- Submit the APD for official CMS review and approval.

The APD should describe the programmatic value aligned to state priorities that a state plans to achieve with their project. The APD should include measurable outcomes and metrics that align with the desired Medicaid program goals. During the planning process, a state should be in frequent contact with its CMS MES State Officer. This ensures CMS support with the state's development of APDs that reference the applicable CEF and include outcomes and metrics that clearly align the proposed IT project with the state's goals, whether to solve a problem or achieve improvements to the Medicaid program.

If a state has an approved project APD that does not include applicable outcomes, CMS will work closely with the state to identify and validate outcomes for that project as part of the APD process or during preparation for a certification review.

4.1 Procurement Planning Phase

Once the APD is approved, the state transitions into procurement planning. The state is encouraged to consult with its CMS MES State Officer to make certain that the state clearly communicates its desired outcomes to prospective vendors. Before releasing a procurement instrument (e.g., request for proposal [RFP]), the state should include the approved outcomes and metrics from the APD in the SMC Intake Form template. This SMC Intake Form tracks certification information and maintains an audit record for ORR and CR. If the state is preparing the proposed module for certification, the SMC Intake Form must include all CMS-required outcomes for the module. If any CEF and outcomes are deemed inapplicable, the state should provide a justification within the SMC Intake Form that explains why they are not pertinent to the module's certification. States may need to revisit and update outcomes and metrics over time (and possibly during the certification process) due to lessons learned or changing Medicaid priorities. If a state revises its outcomes and metrics, an APD-U is required. States should regularly consult their CMS MES State Officer to discuss such updates.

Refer to the MES Certification Repository for the SMC Intake Form Template and pre-populated EVV template, as well as for guidance on using the SMC Intake Form.

After drafting the SMC Intake Form, the state should review the form with its CMS MES State Officer. A preliminary list of evidence and required artifacts for both ORR and CR should be added to the applicable tabs. The state should draw on existing documentation from the upcoming DDI process. There is no need to create a separate wraparound file; submitting the files individually is sufficient. This approach should reduce the burden on states when submitting documentation for certification. Refer to the MES Certification Repository CEF page for the CEF example and required evidence.

Evidence to support outcome achievement may include, but is not limited to:

- Demonstrations
- Testing results
- Production reports
- Plans for organizational change management (e.g., managing stakeholders and users, training, and help desk)

Once the DDI begins, the CMS Certification Team will host a kickoff call with the state to explain the SMC process and address any questions. Following the call, CMS will send a follow-up email to the state and include a copy of the kickoff slide deck and any other relevant materials.

States should be sure to share any concerns or questions regarding outcomes and metrics with their CMS MES State Officer early and often to prevent any delays or resolve any roadblocks as they move toward ORR and CR.

5. Development Phase

At the beginning of the development phase, the state should develop a Master Test Plan in consultation with the MES Testing Guidance Framework. The state should provide its CMS MES State Officer with system development and testing progress in the form of summary testing results, defect reports, and software demonstrations, as requested. The state should also regularly apprise its CMS MES State Officer of progress toward achieving the CEF and outcomes.

The state must begin using the new Monthly Project Status Report Template available on the MES Certification Repository. This template is required for submitting monthly project status reports for certifications, ensuring that the state's IT project aligns with SMC guidelines and accurately reflects project health. The goal of the new status report is to provide structured, consistent data across states to better enhance the reporting and decision-making processes. The status report supplies a clear and concise project status update to the CMS MES State Officer. Like its predecessor, the monthly project status report must include updates on risks, issues, milestones, progress since the last report, and an updated financial project budget versus expenditures. The state submits the completed report to the CMS MES State Officer and uploads it to the appropriate CMS designated repository.

CMS has found that adequately tested systems, and especially those tested by actual users throughout the entire development process, demonstrate successful implementations. Therefore, CMS emphasizes testing in the certification process. The *MES Testing Guidance Framework* offers specific MES testing expectations and recommendations.

CMS will continue to provide comprehensive technical assistance to states during the Development phase of each state's IT investment lifecycle.

5.1 Pre-Production Phase: Operational Readiness Review

The state must conduct an ORR with its CMS MES State Officer before releasing the system/module into production. Once the system/module has been in production for at least six (6) months and the state can report on approved metrics dating back to the date for retroactive certification approval date as identified in the state's Certification Request Letter to CMS, the state can request a CR with its CMS MES State Officer. The ORR must be completed before the module goes live (and after most of the User Acceptance Testing [UAT] is complete).

The state must provide evidence that its module is production-ready by including test results and data demonstrating its effectiveness. Each state must also ensure compliance with privacy and security standards, demonstrate the system's capability to achieve approved CMS-required and state-specific outcomes, and support the generation and reporting of metrics as specified in the ORW. The state should verify that its operations staff are fully prepared for implementation by documenting relevant training sessions and other organizational change management activities that were conducted or are ongoing. This preparation is crucial for the successful deployment and continuous operation of the module.

If a state follows a phased approach to implementation, the state must align and document each implementation phase with all applicable outcomes; the state and CMS MES State Officer will then determine the most suitable point for conducting the ORR. CMS recommends that the state collaborate with its CMS MES State Officer to select an ORR review date that leaves sufficient

time to prepare for the review and address any issues identified during the ORR before the state goes live.

Proper and complete systems testing, notably testing with users, is an important indicator of project success. Evaluating testing results is a core part of ORR. The evidence provided must clearly demonstrate that:

- The state has met the required CEF applicable to that project and attested to in the APD.
- The system functionality associated with the applicable CMS-required and state-specific outcomes has been developed and tested in accordance with the state's Master Test Plan.
- The system/module will support the collection and reporting of metrics described in the SMC Intake Form.

Starting three (3) months before the preferred review date, the state may propose a date for the ORR. However, this date cannot be confirmed until the required entry criteria are submitted and approved by the CMS Certification Team. These criteria are essential to ensure the state is prepared for the review; without confirmation, we cannot conduct the review. To secure the preferred date, the state must submit the entry criteria at least four weeks in advance. The SMC review calendar opens on the first day of each month for the following three months, including the current month.

Refer to the MES Certification Repository SMC Process Overview, Development page for the entry criteria for scheduling an ORR.

Note that meeting the entry criteria for ORR only clears the way to schedule the ORR. In order to conduct the review, the state must provide the most up-to-date documents two (2) weeks before the ORR in the CMS designated repository for evaluation by the CMS Certification Team.

Once the entry criteria are met and a review date has been finalized, the state may request additional calls with the CMS Certification Team for technical assistance.

Two (2) weeks before the scheduled review date, the state must upload the unredacted evidence, required artifacts, SMC Intake Form, ORW, agenda, and presentation into the CMS designated repository. The state should include only the minimum evidence necessary to demonstrate compliance. For lengthy documents, relevant sections or paragraphs should be noted in the SMC Intake Form comments to avoid slowing the review process. There is no need to create a separate wraparound file; submitting the files individually is sufficient. This approach should reduce the burden on states when submitting documentation for certification. Once the evidence is uploaded, the review process begins.

One (1) week before the review, the state will receive an Information Request Listing (IRL) for any additional clarifications needed. Although providing written responses to these questions before the review is encouraged, it is not mandatory. The state should be prepared to address all outstanding questions from the IRL during the ORR discussions and demonstrations.

The ORR meeting should begin with a brief overview of the state's Medicaid program and project. Next, the state should describe the training details, testing summaries, and defect status, followed by module demonstrations and a review of metric definitions. The ORR meeting should conclude with a recap of action items and a discussion of the next steps. Throughout the review,

the CMS Certification Team will ask questions to ensure clarity and understanding. Because the ORR focuses on both outcome achievement and system deployment, CMS encourages states to include subject matter experts (SME) from the program, business operations, and IT.

One (1) week after the ORR, CMS will have entered comments into the SMC Intake Form before returning it to the state. The state will also receive a tear-out document listing observations, recommendations, and any action items from the review. The state should work closely with its CMS MES State Officer to address ORR observations and findings as the project transitions into production and prepares for the CR.

6. Production Phase: Requesting a Certification Review

Once the system/module has been in production for at least six (6) months and the state can report on approved metrics dating back to the date for retroactive certification identified in the state's Certification Request Letter to CMS, the state can request a CR with its CMS MES State Officer. To initiate a CR, states must submit an official Certification Request Letter and the system acceptance letter via email to the CMS MES State Officer and MES@cms.hhs.gov. These letters are also considered Required Artifacts and must be uploaded to the appropriate certification folder on the CMS designated repository. Refer to the Certification Request Letter Template on the MES Certification Repository.

Within the Certification Request Letter, the state will attest to being in compliance with the Transformed Medicaid Statistical Information System (T-MSIS). This compliance involves the following state activities:

- The state maintains monthly production submissions of T-MSIS files. A state does not meet timeliness requirements if it submits T-MSIS files later than one (1) month after the T-MSIS reporting period.
- The state maintains complete and accurate historical T-MSIS data for program evaluation and the continuous improvement in business operations pursuant to 42 CFR 433.112(b)(15).
- The state can demonstrate that it is meeting the targets for Outcomes-Based Assessment (OBA) critical priority data quality checks, high-priority data quality checks, and the expenditure data content category. The state should also demonstrate it is working in good faith to resolve such data quality issues. Generally, the state will not meet the T-MSIS requirements for complete and accurate data if the state does not meet the targets for OBA criteria in critical priority data quality checks, high-priority data quality checks, and the expenditure data content category, and/or if the state is not working in good faith to resolve any identified data quality issues..
- The state meets all requirements delineated in the T-MSIS Reporting for any Large System Enhancement (LSE) Standard Operating Procedures (SOP) affecting T-MSIS reporting.

Starting three (3) months before the preferred review date, the state may propose a date for the CR. However, this date cannot be confirmed until the required entry criteria are submitted and approved by the CMS Certification Team. These criteria are essential to ensure the state is prepared for the review; without confirmation, we cannot conduct the review. To secure the

preferred date, the state must submit the entry criteria at least four weeks in advance. The SMC review calendar opens on the first day of each month for the following three months, including the current month.

Refer to the MES Certification Repository SMC Process Overview and Production page for the entry criteria for scheduling a CR.

Note that meeting the entry criteria for CR only clears the way to schedule the CR. The state must provide the most up-to-date documents two (2) weeks before the CR in the CMS designated repository for evaluation by the CMS Certification Team.

Once the entry criteria are met and a review date has been finalized, the state may request additional calls for technical assistance from the CMS Certification Team.

6.1 Production Phase: Certification Review

States seeking enhanced federal funding for system maintenance and operations must first complete a CR. Each state must demonstrate through appropriate evidence that the system or module in production has achieved the approved CMS-required and state-specific outcomes and metrics. In contrast to the ORR (which focuses on demonstrating functionality associated with the applicable CMS-required and state-specific outcomes in pre-production), the CR demonstrates the impact of functionality in production, as assessed by metrics.

For EVV modules, the state's CR will continue to focus on the six EVV outcomes (EVV1, EVV3, EVV4, EVV5, EVV7, and EVV8) that must be demonstrated in the production environment, provided they apply to the state's EVV model. (For example, EVV 4 may not apply to a state that mandates the exclusive use of a state-procured EVV system.) If warranted, CMS may require that the state demonstrate achievement of additional criteria. The state must upload all unredacted evidence to the applicable CMS designated repository.

Two (2) weeks before the scheduled review date, the state must upload the unredacted evidence, required artifacts, SMC Intake Form, ORW, agenda, and presentation into the CMS designated repository. Only the minimum evidence necessary to demonstrate compliance should be included. For lengthy documents, the state should note relevant sections or paragraphs in the SMC Intake Form comments to avoid slowing down the review process. There is no need to create a separate wraparound file; submitting the files individually is sufficient. This approach should reduce the burden on states when submitting documentation for certification. Once the evidence is uploaded, the review process begins.

One (1) week before the review, the state will receive an IRL for any additional clarifications needed. Providing written responses to these questions before the review is encouraged but not mandatory. The state should be prepared to address all outstanding questions from the IRL during the CR discussions and demonstrations.

The CR meeting should begin with a brief overview of the state's Medicaid program and a project summary. A recap of ORR observations, recommendations, and any actions taken by the state should follow. Next, the state should provide module demonstrations in the production environment and review the metrics. The CR meeting should conclude with a recap of action items and a discussion of the next steps. Throughout the review, the CMS Certification Team will ask questions to ensure clarity and understanding. CMS encourages states to include SMEs

from the program, business operations, and IT.

After the CR, CMS will review and enter comments into the SMC Intake Form and assemble the certification package. CMS will follow up with the state to discuss any necessary remediations. Once certification is approved, the state will receive the updated SMC Intake Form, the certification report, and the certification letter from CMS.

6.1.1 Operational Reporting Phase (Ongoing)

To efficiently demonstrate ongoing, successful system operations, states must submit Operational Report Workbooks with data that shows that the modules are meeting all applicable requirements for the state's claimed federal matching funds. States should upload these ORWs to the CMS-designated repository on a monthly basis after certification, and every OAPD submission should include an attestation specifying the CMS repository folder location of the submitted Operational Report Workbooks. States must submit monthly project status reports for each MES project to demonstrate alignment with Conditions for Enhanced Funding, regulatory requirements, and overall project health. Operational reports should include metric data corresponding to the agreed outcomes for each applicable MES module. In addition to operational reports, the state must submit an OAPD per 45 CFR 95.611 to obtain enhanced funding authorized through certification (per 42 CFR 433.116) for any system or module for which the state requests enhanced federal matching funds for the state's expenditures in operating an existing system.

For all modules, the state must provide a monthly breakdown of metric data within its ORW, as applicable (may be combined for multiple modules). The ORWs of EVV modules must be submitted to CMS on a quarterly basis, as specified in Table 2, EVV Metric Reporting Schedule.

The states must use the ORW template on the MES Certification Repository to provide relevant details such as the metric ID, outcome reference number, metric name, description, and the proposed calculation for each metric. Please refer to the ORW template instructions for additional details.

For previously certified systems, any systems operating as a system of record, and/or those for which the state is claiming enhanced federal matching funds for DDI or operations, the state should coordinate with its respective CMS MES State Officers to agree on an approach and submission of operational reporting.

In accordance with 42 CFR 433.119, CMS may periodically review and reapprove each system initially approved under 42 CFR 433.114 for 75 percent enhanced federal matching for state expenditures on the system's ongoing operations. CMS may review an entire system or a module's operation, or the Agency may focus the review on the operation of specific parts of the system or module. At a minimum, any CMS review conducted under 42 CFR 433.119 will assess whether the system operates in compliance with all applicable regulatory requirements and will pay specific attention to areas where the system or module demonstrated weaknesses in previous reviews. In general, the reapproval process may include going through the SMC process.

Appendix A. Conditions for Enhanced Funding

Table 4 - Conditions for Enhanced Funding (CEF), as outlined in 42 CFR 433.112, which are applicable to all MES modules.

Table 3. Conditions for Enhanced Funding (CEF)

Reference #	Condition
CEF01	CMS determines the system is likely to provide more efficient, economical, and effective administration of the State plan.
CEF02	The system meets the system requirements, standards, and conditions, and performance standards in Part 11 of the State Medicaid Manual, as periodically amended.
CEF03	The system is compatible with the claims processing and information retrieval systems used in the administration of Medicare for prompt eligibility verification and for processing claims for persons eligible for both programs.
CEF04	The system supports the data requirements of quality improvement organizations established under Part B of Title XI of the Act.
CEF05	The State owns any software that is designed, developed, installed, or improved with 90 percent FFP.
CEF06	The Department has a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use and authorize others to use, for Federal Government purposes, software, modifications to software, and documentation that is designed, developed, installed, or enhanced with 90 percent FFP.
CEF07	The costs of the system are determined in accordance with 45 CFR 75, subpart E.
CEF08	The Medicaid agency agrees in writing to use the system for the period of time specified in the advance planning document approved by CMS or for any shorter period of time that CMS determines justifies the Federal funds invested.
CEF09	The agency agrees in writing that the information in the system will be safeguarded in accordance with subpart F, part 431 of this subchapter.
CEF10	Use a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces; the separation of business rules from core programming, available in both human and machine-readable formats.
CEF11	Align to, and advance increasingly, in MITA maturity for business, architecture, and data.
CEF12	The agency ensures alignment with, and incorporation of, standards and implementation specifications for health information technology adopted by the Office of the National Coordinator for Health IT in 45 CFR part 170, subpart B. The agency also ensures alignment with: the HIPAA privacy, security, breach notification and enforcement regulations in 45 CFR parts 160 and 164; and the transaction standards and operating rules adopted by the Secretary under HIPAA and/or section 1104 of the Affordable Care Act. The agency meets accessibility standards established under section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities, and compliance with Federal civil rights laws; standards and protocols adopted by the Secretary under section 1561 of the Affordable Care Act.
CEF13	Promote sharing, leverage, and reuse of Medicaid technologies and systems within and among States.
CEF14	Support accurate and timely processing and adjudications/eligibility determinations and effective communications with providers, beneficiaries, and the public.
CEF15	Produce transaction data, reports, and performance information that would contribute to program evaluation, continuous improvement in business operations, and transparency and accountability.
CEF16	The system supports seamless coordination and integration with the Marketplace, the Federal Data Services Hub, and allows interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services as applicable.

Reference #	Condition
CEF17	For E&E systems, the State must have delivered acceptable MAGI-based system functionality, demonstrated by performance testing and results based on critical success factors, with limited mitigations and workarounds.
CEF18	The State must submit plans that contain strategies for reducing the operational consequences of failure to meet applicable requirements for all major milestones and functionality.
CEF19	The agency, in writing through the APD, must identify key state personnel by name, type, and time commitment assigned to each project.
CEF20	Systems and modules developed, installed, or improved with 90 percent match must include documentation of components and procedures such that the systems could be operated by a variety of contractors or other users.
CEF21	For software systems and modules developed, installed or improved with 90 percent match, the State must consider strategies to minimize the costs and difficulty of operating the software on alternate hardware or operating systems.
CEF22	Other conditions for compliance with existing statutory and regulatory requirements, issued through formal guidance procedures, determined by the Secretary to be necessary to update and ensure proper implementation of those existing requirements.

Appendix B. Required Artifacts List

Table 4, Required Artifacts. It lists the artifacts required for an ORR and CR. Although the table provides minimum requirements for each document, this is not an exhaustive list of what each artifact typically includes. States are encouraged to add elements, as appropriate.

It is important to distinguish between required artifacts and evidence. *Evidence* is documentation or data that proves the achievement of an outcome, as listed in the SMC Intake Form on the Outcomes & Metrics tab. *Required Artifacts*, on the other hand, are documents that demonstrate the progression of a state's project and are not typically used as evidence for outcomes.

Table 4. Required Artifacts

Document / Artifact	Minimum Required Content and Notes	Required at ORR, CR, or Both
Certification Request Letter	• The date the system became the system of record (usually the implementation date). • The effective date for which the state requests certification approval. • A proposed timeframe for the CR. • A declaration that the state's system meets all the requirements of law and regulation, including 42 CFR 433.117, for all periods for which the state claims 75 percent Federal Financial Participation (FFP). • Confirmation that the state is T-MSIS compliant. • Confirmation that the state is ready for CMS certification based on the system's performance in demonstrating achievement of outcomes. • A copy of the state's letter to the vendor, contractor, or state development team accepting the system/module(s).	CR
System Acceptance Letter	A copy of the state's acceptance letter addressed to the system developer, indicating that the system or module was accepted as fully operational. The system acceptance date recorded in the letter must be earlier than the date of the Certification Review.	CR
Monthly Project Status Reports	The Status Report template includes the following items: • Project Information. • Executive summary including recent accomplishments and activities planned for the next period. • Major deliverables and milestones status. • Budget (approved and actual costs) status. • High-priority open risks, issues, and defects (roadblocks).	Both
Master Test Plan	• The Master Test Plan describes the various types of testing prescribed for the project and how it will be managed. The plan should contain definitions of defect severity to ensure consistency across all testing. **Note:** The Master Test Plan does not consist of separate test plans (such as a system test or UAT plan). • Refer to Expectation 2 under Test Planning within the MES Testing Guidance Framework for elements of the plan.	ORR

Document / Artifact	Minimum Required Content and Notes	Required at ORR, CR, or Both
Test Summary Reports	• Test summary reports should be provided for each type of test on the project. • A summary test report should include, but is not limited to: o Objective o Test approach o Entry and exit criteria o Summary of the test cases executed by status (such as passed, failed, blocked, or cancelled) • For CR, the state can submit a sample of UAT cases and results from changes made since go-live. • Test results should validate the iterative delivery of system functionality and confirm that the system will produce metrics associated with outcomes. • Refer to Expectation 3 under Test Execution within the MES Testing Guidance Framework for additional information on different types of testing.	Both
Deployment Plan	• A clear and efficient deployment plan will help ensure a seamless transition from development to production and streamline the deployment process. • Refer to Expectation 5 under Test Execution within the MES Testing Guidance Framework for components.	ORR
Defect List	A defect list should include all defects for the entire project (DDI and operations), regardless of status or severity. A defect list should include, but is not limited to: • Summary. • Status. • Severity. • Open Date. • Estimated Closure Date. • Actual Closure Date. • Business impact for all open Severity 1 and 2 defects. • Workaround for all open defects, including frequency and severity (covering all critical and high defects), along with the associated implementation timelines.	Both
Risk List	A risk list should include all risks for the entire project (DDI and operations), regardless of status. A risk list should include, but is not limited to: • Status. • Open and closed dates. • Priority. • Mitigation, resolution, or a risk acceptance statement.	Both
Issue List	An issue list should include all issues for the entire project (DDI and operations), regardless of status. An issue list should include, but is not limited to: • Status. • Open and closed dates. • Priority.	Both

Appendix C. Guidelines for the Independent Third-Party Security and Privacy Assessment for Medicaid Enterprise Systems

C.1 Introduction

The state MES is the custodian of sensitive information, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), for millions of individuals receiving coverage through Medicaid and CHIP. The state and its business partners share responsibility for ensuring the protection of this sensitive information. States and their respective business partners must demonstrate continuous monitoring and regular security and privacy control testing through an independent security and privacy assessment.

This appendix provides an overview of the independent security and privacy assessment requirements. It presents guidelines for both cloud-based and non-cloud-based environments. The state can tailor guidelines based on the solution's implementation. This appendix is applicable for states that work directly with a third-party assessment vendor or a MES solution vendor working with a third-party assessment vendor.

C.2 Requirements Background

Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations at 45 CFR 164.308(a)(1)(ii)(A), a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out HIPAA standards and implementation specifications. Therefore, a risk analysis must be completed to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards of PII/PHI. Furthermore, the National Institute of Standards and Technology (NIST), Security Assessments Control, CA-2, requires an independent assessment of all applicable security and privacy controls. States should have a fully completed and implemented System Security and Privacy Plan (SSPP) before starting the security and privacy assessment. CMS highly recommends that states use an independent third-party assessor to conduct the assessment.

If the state has adopted a framework similar to or complementary to NIST that supports the HIPAA requirements, it may use that framework for risk analysis.

If NIST is not the core framework of the third-party assessor, then the third-party assessor should provide a translation or crosswalk of the supported framework to the NIST controls.

C.3 Purpose

This appendix provides an overview of the independent security and privacy assessment requirements through the following objectives:

- Define the independent third-party assessor (subsection C.4).
- Explain the scope of the security and privacy control assessment and provide assessment planning considerations (subsection C.5).
- Provide a basic security and privacy control assessment methodology (subsection C.6).

- Summarize security and privacy assessment reporting (subsection C.7).

This appendix is not intended to provide detailed guidance for assessment planning and performance or for state planning and action to address assessment findings.

C.4 Independent Third-Party Security and Privacy Assessor

Pursuant to 45 CFR 95.621(f) and consistent with State Medicaid Directors Letter (SMDL) #06-022,[8] CMS requires that state agencies employ assessors or assessment teams to conduct periodic security and privacy control assessments of the MES environment. The assessor's role is to independently assess the effectiveness of implementations of security and privacy safeguards for the MES environment and to maintain the integrity of the assessment process. The assessor organization cannot be the same organization that performs design, development, and implementation activities. Alternatively, states can require that vendors conduct their own independent third-party assessment and provide assessment results.

C.4.1 Assessor Independence and Objectivity

An assessor must be free from any real or perceived conflicts of interest, including any personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An assessor is considered independent if there is no perceived or actual conflict of interest involving the developmental, operational, financial, and/or management chain associated with the system and the determination of security and privacy control effectiveness.

NIST Special Publication (SP) 800-39, *Managing Information Security Risk,*[9] states that:

> Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.

C.4.2 Assessor Qualifications

Experience and competencies are important factors in selecting an assessor. CMS recommends that the MES assessor possess a combination of privacy and security experience and relevant assessment certifications. Examples of acceptable privacy and security experience may include, but are not limited to:

- Reviewing compliance with HIPAA security standards.
- Reviewing compliance with the most current NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.[10]

[8] https://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD092006.pdf
[9] https://csrc.nist.gov/pubs/sp/800/39/final
[10] If a state uses a framework other than NIST, the state should identify that framework and provide a crosswalk of the framework to the NIST controls.

- Reviewing compliance with CMS's *Minimal Acceptable Risk Standards for Exchanges*.
- Reviewing compliance with the Federal Information Security Management Act.
- Participating in the Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization.
- Reviewing compliance with the Statement on Standards for Attestation Engagements 16.
- Experience assessing the implementation of the Center for Internet Security (CIS) benchmarks.
- Reviewing compliance with the Open Web Application Security Project (OWASP).

The assessor organizations should have relevant security and privacy accreditations, and their respective assessor team leads should have relevant security and privacy certifications. Examples of relevant security and privacy auditing certifications are:

- Certified Information Privacy Professional.
- Certified Information Privacy Manager.
- Certified Information Systems Security Professional.
- Fellow of Information Privacy.
- HealthCare Information Security and Privacy Practitioner.
- Certified Internal Auditor.
- Certified Risk Management Professional.
- Certified Information Systems Auditor.
- Certified Government Auditing Professional.
- Certified Expert HIPAA Professional.

C.4.3 Assessor's Options

CMS strongly recommends using an experienced third-party security and privacy assessor. Internal state staff may serve in this capacity, provided they have appropriate qualifications to evaluate the implementation of security and privacy controls. The internal state staff must be familiar with HIPAA regulations, NIST standards, and other applicable federal privacy and cybersecurity regulations and guidance. They must also meet the assessor's independence, objectivity, and qualifications as documented in subsections C.4.1, Assessor Independence and Objectivity, and subsection C.4.2, Assessor Qualifications. Furthermore, these independent assessors must be capable of performing penetration testing and vulnerability scans.

C.5 Assessment Scope and Planning

C.5.1 Scope of the Independent Security and Privacy Control Assessment

The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. SCAs also identify areas of risk that require the state's attention and remediation. The independently conducted SCA provides an understanding of the following items:

- Compliance of the MES application or system with the state's security and privacy control requirements.
- Security posture of the underlying infrastructure.
- Remediation of any application and/or system security, data security, and privacy vulnerabilities to improve the MES's security and privacy posture.
- Adherence to the state's security and privacy program, policies, and guidance.

C.5.2 Vulnerabilities and Testing Scenarios

Given the sensitivity of data processed in the MES and the high threat of today's web environment, it is critically important that the security of web applications deployed adequately meets the present-day security attack vectors and situations. The Open Web Application Security Project (OWASP) keeps an up-to-date list identifying such attacks and situations.[11] In addition to the mandated security and privacy controls, the independent SCA requires that vulnerability assessments determine vulnerabilities associated with known attacks and situations obtained from the current OWASP Top 10 for 2021 – *The Ten Most Critical Web Application Security Risks*. The assessment should adjust the SCA scope to address the current OWASP list of vulnerabilities.

The state should regularly review the following list to determine the current vulnerabilities in the OWASP Top 10 for 2021, including but not limited to:

- Broken Access Control.
- Cryptographic Failures.
- Injection.
- Insecure Design.
- Security Misconfiguration.
- Vulnerable and Outdated Components.
- Identification and Authentication Failures.
- Software and Data Integrity Failures.
- Security Logging and Monitoring Failures.
- Server-Side Request Forgery.

C.5.3 Assessment of Critical Security Controls

Test scenarios should adequately assess the implementation status of critical security controls identified by the Center for Internet Security.[12] The CIS controls are mapped to the NIST controls. The testing scenario information for each CIS control is available at the CIS site. The main testing points identified by the CIS are incorporated into the SCA scope, corresponding Security and Privacy Controls Assessment Test Plan (SAP), and testing criteria.

CIS benchmarks are specific to environmental components such as server operating system hardening, networking configurations, or cloud service implementations. However, available

[11] https://owasp.org/Top10/
[12] https://www.cisecurity.org/controls/cis-controls-list

benchmarks should also be applied to system configurations.

C.5.4 Assessment Planning

The state is encouraged to develop an assessment strategy and procedure following a standardized approach for planning and resourcing the SCA of its applications, systems, and underlying components. Toward that end, the state is responsible for ensuring that each SCA has:

- Budget and assigned resources suitable for completing the assessment.
- Clear objectives and constraints.
- Well-defined roles and responsibilities.
- Scheduling that includes defined events and deliverables.

During planning for the SCA, the state develops a scope statement that is dependent on, but not limited to, the following factors:

- Application or system boundaries.
- Known business and system risks associated with the application or system.
- Dependence of the application or system on any hierarchical structure.
- Current application or system development phase.
- Documented security and privacy control requirements.

The assessor's SCA contract statement of work should include requirements to clarify findings and make corrective action recommendations after the assessment. The SCA contract terms should also specify that all assessor staff execute appropriate agreements, such as a Non-Disclosure Agreement, Memorandum of Understanding, or HIPAA Business Associate Agreement, for the protection of sensitive data before accessing any information related to the security and privacy of the application or system. Requests to access information should only be granted based on a demonstration of a valid need-to-know level, not a position, title, level of investigation, or position sensitivity level.

C.6 Security and Privacy Control Assessment Methodology

The SCA methodology described here originates from the standard CMS methodology used to assess all CMS internal and business partner applications or systems.

Assessment procedures for testing each security and privacy control should be consistent with the methodology documented in the most current version of NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*.[13] The assessor should prepare a detailed assessment plan using these security and privacy control assessment procedures, the main testing points for the CIS critical controls, and detailed directions for addressing the penetration testing procedures for the OWASP Top 10 vulnerabilities. The assessor should modify or supplement the procedures to evaluate the application or system vulnerability to different types of threats, including those from insiders, the Internet, or the network. The assessment methods should include examination of documentation, logs, configurations, interviews with personnel, and testing of technical controls.

Control assessment procedures and associated test results provide information to identify the following issues:

- Application or system vulnerabilities, the associated business and system risks, and potential impact.
- Weaknesses in the configuration management process, such as weak system configuration settings that may compromise the system's confidentiality, integrity, and availability.
- State and/or federal policies are not followed.
- Major documentation omissions and/or discrepancies.

C.6.1 Security and Privacy Control Technical Testing

The state grants user access to the application or system to permit security technical testing by assessor staff. The state system administrator establishes application-specific user accounts for the assessor that accommodate the different user types and roles. Because of this access and these accounts, an assessor can thoroughly assess the application or system and test any application and system security controls that might otherwise not be tested. The assessor should not be given a user account with a role that would allow access to PII/PHI in any application or database.

The assessor should attempt to expose vulnerabilities associated with gaining unauthorized access to the application or system resources. The assessor should select and employ tools and techniques that simulate vulnerabilities, such as buffer overflows and password compromises. The assessor must ensure against any inadvertent alteration of important settings that may disable or degrade essential security or business functions. Because many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the assessor must identify in the SAP all proposed tools that pose a risk to the computing environment.

The MES solution can be tested in a test environment or a pre-production environment, provided these environments host an instance of the production operational environment. The testing or pre-production environments should mirror the production environment to generate an accurate response. The assessor should properly document any deviations in these environments used for testing. States or vendors should certify and attest that all system vulnerabilities discovered in a security and privacy assessment conducted in a test or a pre-production environment will also be mitigated in the production environment.

[13] https://csrc.nist.gov/pubs/sp/800/53/a/r5/final

C.6.2 Network and Component Scanning

To ensure an understanding of the security posture of a network and component infrastructure, the SCA includes network-based infrastructure scans, database scans, web application scans, and penetration tests for all in-scope components, applications, and systems. This scope provides a basis for determining the extent to which the security controls implemented within the network meet security control requirements. The assessor evaluates the results of these scans in conjunction with the configuration assessment.

C.6.3 Configuration Assessment

The configuration assessment provides the assessor with another mechanism to determine if the state's security requirements are implemented correctly in the application or system, or if the system environmental components are implemented correctly within the boundary of the application or system. Performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the state's security and privacy requirements.
- Review access to the system and databases for default user accounts.
- Test firewalls, routers, systems, and databases for default configurations and user accounts.
- Review firewall access control rules against the state's security requirements.
- Determine consistency of system configuration with the state's documented configuration standards.

C.6.4 Documentation Review

The assessor should review all security and privacy documentation for completeness and accuracy and to determine the security and privacy posture of the application or system. Through this process, the assessor develops insight into the documented security and privacy controls in place to effectively assess whether all controls are implemented as described. The documentation review augments all testing: it is an essential element for evaluating compliance of the documented controls versus the actual implementation as revealed during technical testing, scanning, configuration assessment, and personnel interviews.

For example, if the specified control stipulates that the system's password must be eight characters, the assessor must review the state's password policy or the SSPP to verify compliance with this requirement. During the technical configuration assessment, the assessor confirms that passwords are configured as stated in the state's documentation. Table 5. Core Security and Privacy Documentation, presents security documentation examples for review.

Table 5. Core Security and Privacy Documentation

NIST / State Control Family	NIST / State Control Number	Document Name
Planning (PL)	PL-2: System Security and Privacy Plan	System Security and Privacy Plan (SSPP)
Configuration Management (CM)	CM-9: Configuration Management Plan	Configuration Management Plan (CMP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
	CP-4: Contingency Plan Testing and Exercises	CP Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
	IR-3: Incident Response Testing and Exercises	IRP Test Plan
Awareness and Training (AT)	AT-3: Security Training	Security Awareness Training Plan
	AT-4: Security Training	Training Records
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements (ISA)
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment (PIA) or other privacy documents
	AP-2: Purpose Specification	Privacy documents and notices, including, but not limited to, PIAs and agreements to collect, use, and disclose PII / PHI and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
	AR-2: Privacy Impact and Risk Assessment	Documentation describing the organization's privacy risk assessment process, and documentation of privacy risk assessments performed by the organization

C.6.5 Personnel Interviews

The assessor conducts personnel interviews to validate the implementation of security and privacy controls, confirm that state and/or MES solution vendor staff understand and follow documented control implementations, and verify the appropriate distribution of updated documentation to staff. The assessor interviews business, IT, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. The assessor will customize interview questions to focus on control assessment procedures applicable to individual roles and responsibilities and ensure that state staff are properly implementing and/or executing security and privacy controls.

The SCA test plan identifies the designated state and/or MES solution vendor SMEs to interview. These SMEs should have specific knowledge of overall security and privacy requirements and a detailed understanding of the application or system operational functions. The staff selected for conducting interviews may have the following roles:

- Business Owner(s).
- Application Developer.
- Configuration Manager.
- Contingency Planning Manager.
- Database Administrator.
- Data Center Manager.
- Facilities Manager.
- Firewall Administrator.
- Human Resources Manager.
- Information System Security Officer.
- Privacy Program Manager.
- Privacy Officer.
- Media Custodian.
- Network Administrator.
- Program Manager.
- System Administrator(s).
- System Owner.
- Training Manager.

Although the initial identification of interviewees is determined when the SAP is prepared, additional staff may participate as interviewers during the SCA process.

C.6.6 Penetration Testing

A penetration test is a comprehensive way to test an organization's cybersecurity vulnerabilities and its compliance with the adopted security and privacy standards. Penetration testing views the network, application, device, and physical security from the standpoint of a malicious actor as well as an experienced cybersecurity expert to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities.

At a minimum, penetration testing includes the tests found in subsection 3.2, The Streamlined Modular Certification Process, based on the OWASP Top 10. The Security and Privacy Controls Assessment Test Plan should document the tools, methods, and processes for penetration testing. The test plan should clearly account for and coordinate any special requirements or permissions for penetration testing during the SCA.

C.7 Security and Privacy Assessment Reporting

At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to the state's Business Owner, who is then responsible for providing the report to CMS. The SAR's structure and content must be consistent with the assessment objectives. The SAR structure allows the assessor to communicate the assessment results to several audience

levels, ranging from executives to technical staff.

The SAR is not a living document; the assessor should neither add findings to nor remove findings from the SAR.

C.7.1 SAR Content

The SAR content may include, but is not limited to, the following information:

- System Overview.
- Executive Summary Report.
- Detailed Findings Report.
- Scan results consist of Infrastructure Scan, Database Scan, and Web Applications Scan.
- Penetration Test Report.
- Penetration Test and Scan Results Summary.

The SAR presents the results of all testing performed, including technical testing, scans, configuration assessment, documentation review, personnel interviews, and penetration testing. Results from multiple testing sources may be consolidated into one finding if closely related. The findings of the assessment should be annotated in detail, along with the remediation recommendations for the weaknesses and deficiencies found in the implementation of system security and privacy controls. To reduce the risks posed to this important healthcare service and to protect the sensitive information of the citizens who use this service, the assessment team must assign business and system risk levels to each specific finding. The assignment of these risk levels should follow the methodology in NIST SP 800-30 Rev. 1, Appendices G, H, and I.[14] A sample SAR can be modeled after one used by FedRAMP.[15]

C.8 Incident and Breach Reporting Procedures

CMS considers a security or privacy incident[16] or breach[17] of beneficiary PII/PHI to be a serious matter. Therefore, state agencies that are out of compliance with the privacy or security requirements presented in this appendix can be suspended or denied FFP for their information systems, as well as other penalties under federal and state laws and regulations.

[14] NIST 800-30 Rev.1, Appendices G, H, and I. Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[15] FedRAMP SAR Template. Available at: https://www.fedramp.gov/templates/.

[16] OMB Memorandum M-17-12 defines "incident" or "security incident" as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (OMB Memorandum M-17-12, Preparing for or Responding to A Breach of Personally Identifiable Information, January 3, 2017. Located at: http://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-17-12.pdf.

[17] OMB Memorandum M-17-12 defines "breach" as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for anything other than an authorized purpose.

Under HIPAA standards, states must require contractors and other entities to protect PII/PHI privacy and security through business associate agreements if they perform claims processing, third-party, or other payment or reimbursement services on their behalf. States should ensure that their business associates update their procedures as necessitated by environmental or operational changes affecting security and privacy safeguards. The HIPAA Breach Notification Rule, 45 CFR 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI. Similar breach notification provisions implemented and enforced by the Federal Trade Commission apply to vendors of personal health records and their third-party service providers pursuant to Section 13407 of the HITECH Act.

The HHS HIPAA Breach Notification Rule website offers more information and guidance on the breach reporting requirements.[18] In addition to the foregoing HIPAA requirements, the state, in turn, should immediately report a security or privacy incident or breach, whether discovered by its own staff or reported by a contractor, to the CMS MES State Officer and CMS IT Service Desk at cms_it_service_desk@cms.hhs.gov. If a state is unable to report breaches to the CMS IT Service Desk via email, the state can contact the CMS IT Service Desk by phone at (800) 562-1963 or (410) 786-2580.

C.9 Summary

All states should perform either an internal state risk assessment to identify, address, and remediate security and privacy vulnerabilities or engage an industry-recognized security and privacy assessment organization to conduct an external third-party risk assessment (CMS's preferred method) of the MES implementation. Information security and privacy safeguards and continuous monitoring are dynamic processes that must be managed effectively and proactively to support organizational risk management decisions. An independent security and privacy assessment provides a mechanism to identify and respond to new vulnerabilities, evolving threats, and a constantly changing enterprise architecture and operational environment that can feature changes in hardware or software, as well as risks from the creation, collection, disclosure, access, maintenance, storage, and use of data. Through ongoing assessment and authorization, organizations can detect changes to the security and privacy posture of their IT systems and environment, which is essential to making well-informed, risk-based decisions about their system or module within the MES.

[18] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Appendix D. Acronyms

Term	Definition
ACA	Patient Protection and Affordable Care Act of 2010
APD	Advance Planning Document
APD-U	Advance Planning Document-Update
CEF	Conditions for Enhanced Funding
CFR	Code of Federal Regulations
CHIP	Children's Health Insurance Program
CIS	Center for Internet Security
CMCS	Centers for Medicaid and CHIP Services
CMS	Centers for Medicare & Medicaid Services
CP	Claims Processing
CP	Contingency Plan
CR	Certification Review
DDI	Design, Development, and Implementation
DSSDW	Decision Support System Data Warehouse
E&E	Eligibility and Enrollment
EPS	Encounter Processing System
EVV	Electronic Visit Verification
FedRAMP	Federal Risk and Authorization Management Program
FFP	Federal Financial Participation
FFS	Fee-For-Service
FM	Financial Management
HHS	Department of Health and Human Services
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act
IRL	Information Request Listing
IRP	Incident Response Plan
IT	Information Technology
KPI	Key Performance Indicator

Term	Definition
LSE	Large System Enhancement
LTSS	Long-Term Services and Supports
MAGI	Modified Adjusted Gross Income
MCO	Managed Care Organization
MCPIRS	Mechanized Claims Processing and Information Retrieval Systems
MES	Medicaid Enterprise Systems
MM	Member Management
MMIS	Medicaid Management Information System
NIST	National Institute of Standards and Technology
OAPD	Operational Advance Planning Document
OBC	Outcomes Based Certification
OMB	Office of Management and Budget
ORR	Operational Readiness Review
ORW	Operational Readiness Workbook
OWASP	Open Web Application Security Project
PBM	Pharmacy Benefit Management
PDMP	Prescription Drug Monitoring Program
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PM	Provider Management
RFP	Request for Proposal
SaaS	Software as a Service
SAP	Security and Privacy Controls Assessment Test Plan
SAR	Security and Privacy Assessment Report
SCA	Security Control Assessment
SMA	State Medicaid Agency
SMC	Streamlined Modular Certification
SMDL	State Medicaid Director Letter
SME	Subject Matter Expert
SOP	Standard Operating Procedures

Term	Definition
SP	Special Publication
SSPP	System Security and Privacy Plan
T-MSIS	Transformed Medicaid Statistical Information System
TPL	Third-Party Liability
UAT	User Acceptance Testing