OFFICE OF

INFORMATION

SECURITY

Authorization Requirements

Standard Operating Procedures

Version 1.8

February 12, 2020

VA

U.S. Department of Veterans Affairs

Office of Information and Technology

Table of Contents

Document Revision History

Revision Date	Summary of Changes	Version	Author
7/22/19	Initial Draft	1.0	OIS
8/23/19	Second Draft	1.1	OIS
9/13/19	Third Draft	1.3	OIS
10/11/19	Fourth Draft	1.4	OIS
11/13/19	Updated Premier/VA Network and Platform sections	1.5	OIS
12/13/19	Updated Application Registration (section 3.2) Changed 'Secure Code Review' sections to 'Application Security Testing' for all applicable boundaries and updated the steps to complete the requirement Removed 'Quality Code Review' requirement Changed 'Secure Design Review' to 'Application Threat Modeling' for all applicable boundaries and updated the steps to complete the requirement Changed 'Status of Artifacts' to 'Status of Requirements' and added link to Status of Requirements template (Section 4) Added Security Impact Analysis (SIA) requirement for systems requiring a major change (Section 4)	1.6	OIS
1/13/20	Added link for SIA Q&A in Section 4 Updated 'Security Configuration Compliance Data' instructions in all SCCD sections Added Common Control Providers/System of Record (SOR) details (i.e., VA T1SOR, IO SOR, VA Area SOR) in Appendix D and updated SOR verbiage throughout the SOP Updated all 'Application Security Testing' sections with new details on how results are uploaded to eMASS	1.7	OIS

2/12/20	Created Appendix E – New Authorizing Official Guidelines	1.8	OIS

1 Purpose

To obtain and maintain a Department of Veterans Affairs' (VA) Authority to Operate (ATO), the authorization requirements included within the contents of this document must be completed. Enterprise Mission Assurance Support Service (eMASS), VA's Governance, Risk and Compliance (GRC) tool, is the authoritative management tool for VA's Assessment and Authorization (A&A) process and Risk Management Framework. All systems will be assessed in eMASS by the Risk Review team for an authorization recommendation to be submitted to the Authorizing Official (AO) for final ATO consideration. eMASS guidance documentation can be found in the eMASS VA Implementation Guide and eMASS User Guide located on the ***Help*** page within eMASS.

This is a living document based on current federal and VA security policies, standards and guidance, and is subject to change.

2 Scope

These procedures apply to systems that are required to obtain an ATO. These systems must be entered into eMASS and be evaluated for potential risk to VA.

3 Authorization Prerequisites and Registration

3.1 Application Prerequisites

Information System Owners (ISO) for a new information system looking for a determination on an ATO requirement or looking to begin the process to obtain an ATO can submit a request to the GRC Oversight Committee. Follow the steps below to complete the eMASS system pre-registration. For anFy questions regarding system registration, email the GRC Oversight Committee.

1. Fill out the eMASS pre-registration SharePoint request form by going to the eMASS Pre-Registration and clicking *new item*.
2. The GRC Committee will include the new information system request for discussion on the weekly meeting agenda, scheduled Thursdays at 12:00pm EST. During the meeting, the GRC Committee will approve or deny the information system or request additional information before a decision.
3. Once the GRC Committee approves the new information system request and an eMASS administrator approves the system, an email is automatically generated in eMASS to notify the System Owner or delegate of the approval. The System Owner or delegate must then complete the eMASS system registration. Access to eMASS is required to register a new system.
4. The System Steward completes the eMASS System Registration. The System Steward eMASS job aid can assist with the registration process. You may also reach out to the ISSO or the GRC Oversight Committee via email with any questions regarding system registration.

5. Once the eMASS system registration has been completed, the GRC Oversight Committee will approve it and the system project team can begin documentation for security controls and working through the RMF workflow towards an ATO. The ISO must complete the System Owner Responsibilities and the System Owner Attestation documents then upload both to the Artifacts tab within eMASS.

Note: For eMASS, the applicable system POCs must have their authorization package completed and progressed to **RMF Step 5 Authorize: Stage 4 Risk Review in the workflow no less than 45 calendar days** prior to the date they want their authorization decision to be made. Once the package has been progressed, a package snapshot will be taken within eMASS for the Risk Review team to analyze for an ATO. After progressing the system to RMF Step 5 Authorize: Stage 4 Risk Review, the system POCs should continue to work on the system requirements within eMASS. Any progress made after the package snapshot will be able to be viewed by the Risk Review team during their review.

3.2 Application Registration

Custom-developed VA applications, and sometimes Commercial Off The Shelf (COTS) and Software as a Service (SaaS) applications, are required to be registered with the VA Software Assurance Program Office. Registration is necessary to maintain an inventory of the total population of VA applications, by type and business line, according to the VA Common Application Enumeration (CAE) to ensure application-level security considerations are taken into account when determining readiness and performance.

Application registration guidance is provided below:

- VA application developers are responsible for registering custom-developed applications
- Custom-developed VA applications are required to be registered with software assurance
- COTS may be registered with software assurance at the direction of CSOC
- Software as a Service (SaaS) should follow COTS registration procedures
- Registration is required as a prerequisite to both software assurance application security testing validation and CSOC penetration test / application assessment testing
- This requirement is not applicable to VistA systems

Application registration completion steps:

1. Navigate to the Your IT Services portal using your web browser
2. Click on **Make a Request** on the home page
3. Click on the **Vulnerability Management** category
4. Click on **Software Assurance Request** item
5. Fill out the form and select **Application Registration** in the **Services Request** field

6. Fill out this PDF form and attach it to the request using the **Add attachments** link
7. Click on the **Submit** button
8. Make a note of your ticket's request number

After the request has been made, a VA Software Assurance Program team member will follow up. You can view this ticket, or any of your open tickets, through Your IT Services portal.

4 *Assessment and Authorization Requirements*

The Authorization Requirements SOP details the technical scans/testing and security documentation requirements for each boundary. Within each boundary section, details are provided for the required security artifacts, including security document requirements, technical/testing requirements, and Federal/VA guidelines. Additional information related to the parties/OIS organization(s) that can provide additional guidance or assistance for each artifact may also be provided. A Status of Requirements, which is located on the Knowledge Service eMASS Job Aids page, needs to be completed for each ATO package and indicate if a security document and/or technical/testing requirement is applicable or not applicable. The Status of Requirements should provide details on the latest security documentation and technical/testing requirement results or explain why each security document and/or technical/testing requirement is not applicable or not completed. Each security artifact uploaded to eMASS should be named using the following format: SystemNameORAcronym_ArtifactName. To clearly identify the latest technical scans/testing results, all technical scans/testing results that have been completed for an authorization package should be uploaded together in a zip file using the following format: SystemNameORAcronym_TechnicalScans. For a technical scan/testing result that's completed monthly or quarterly for continuous monitoring, the results should be put into a zip file and uploaded to the Artifacts tab in eMASS using the following format: SystemNameORAcronym_TechnicalScanName. Additionally, when the user initiates a new Assess and Authorize package/workflow, a *Package Name* is required. The *Package Name* should utilize the following format: SystemNameORAcronym_MMYYYY. Once the workflow completes, the package is added to the Historical Package Listing with the *Package Name*. Finally, security artifacts should not be password protected. eMASS limits access to personnel with a need to view the system details and security artifacts.

If a system undergoes a significant change or if there is a major change in the information collected or maintained, then the system is required to complete the authorization process prior to the change going into operation and complete a Security Impact Analysis (SIA). Details on completing an SIA can be found within the SIA Q&A on the Knowledge Service Job Aids page. All RMF Steps in eMASS must be completed and all security artifacts need to be updated to reflect the change. Additionally, the Major Change Notification Form, which can be found on the ATO Documents site, must be completed and included with the authorization package that must be uploaded to the Artifacts tab in eMASS.

4.1 Application hosted on Premier/VA Network

The Premier/VA Network includes applications that are VA managed and utilize an OS platform such as Window, UNIX, or Mainframe. A&A requirements for VAEC and other FedRAMP Cloud applications are addressed separately.

Applications on the Premier/VA Network may choose to inherit common control providers from the VA Tier 1 System of Record (T1SOR) and Infrastructure Operations (IO) SOR. Refer to Appendix D – Common Control Providers/System of Record (SOR) for complete details to help determine if the VA T1SOR or IO SOR is applicable.

4.1.1 Security Documentation

The following sections provide details for each of the required security artifacts including the document requirements, references, and the parties that can provide additional guidance for each artifact. If available, template locations for the applicable security artifacts/documents are provided.

An artifact that is generated through eMASS as part of the authorization package and is reviewed/approved by the ISO and/or Information System Security Officer (ISSO) in the eMASS workflow as part of the authorization package may not require signature(s) and may be valid without signature(s). Contact your ISSO with questions on how to complete the documentation.

4.1.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

Roles and Responsibilities

Currently, there's not a CMP template available. The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.

2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-2) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

4.1.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by OIS. Each year Emergency Preparedness & Response (EPR) will provide planning and testing guidance through an action item. DRP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item.
- The ISO or system steward works with the assigned ISSO to create or revise the DRP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS.
2. The ISO or system steward develops or revises the DRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the

FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change to the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.1.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.

3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.1.1.4 Information Security Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item. ISCP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- The ISO or system steward works with the assigned ISSO to create or revise the ISCP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. If yes, then the ISO or system steward will be required to upload the ISCP to eMASS.
2. The ISO or system steward develops or revises the ISCP using the applicable standards and guidelines.

3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.1.1.5 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The Business Requirements MOU/ISA Review Team will assess the documents for quality, content and security.
4. The Business Requirements Division (BRD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the BRD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the Business Requirements Division.

4.1.1.6 Minor Application Self-Assessment

Minor applications refer to information systems that rely on an underlying host information system for most of its security controls. A minor application must be associated with another system/application and cannot fall under a facility or a platform.

All minor applications are required to complete the Minor Application Self-Assessment. The Minor Application Self-Assessment must be uploaded to the Artifacts tab within eMASS under the associated system/Major Application.

4.1.1.7 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted

to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.1.1.8 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.

- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.1.1.9 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward completes the RMF steps in eMASS and develops POA&Ms for all CCIs marked Non-Compliant. eMASS will apply the user's N/A justification (test result) to automatically generate a POA&M item for all controls marked as Not Applicable.

4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.1.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the VA Handbook 6500 and BOD 19-02 (i.e.), Critical – 15 days; High – 30 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. A POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should also be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.1.2.1 Nessus Scan

A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. If the system receives a monthly predictive Nessus vulnerability scan from CSOC and the IP addresses that make up the system are all Windows based then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded, then proceed to Step 3.
    a. If the system receives a monthly predictive Nessus vulnerability scan from CSOC, and the IP addresses that make up the system are not all Windows based, then proceed to step 2, as all necessary Operating System information will not be captured in the predictive scans from CSOC.
    b. If the IP addresses that make up a system are outside of the VA network (Managed Services) and/or the system does not currently receive a monthly predictive Nessus vulnerability scan from CSOC, then proceed to Step 2.

2. The ISO or system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If its decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded.

3. Once the system's Nessus Scan data is accurately recorded, the ISO or system steward follows these steps:

    a. Browse to Information Central Analytics and Metrics Platforms (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.
    d. The ISO or system steward then uploads the mitigation/remediation report to the Artifacts tab within eMASS using the naming instructions identified in Section 4 Assessment and Authorization Requirements.
    e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Nessus scan.

5. A follow-up Nessus scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable system, then contact

the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.1.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

1. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, upload a word document to the Artifacts tab within eMASS explaining why a database scan is not applicable.
2. Once the Database scan is completed, the summary and raw results must be upload to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings and a POA&M must be created in eMASS to keep track of the remediation effort.
3. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.1.2.3 Penetration Test/Application Assessment

A Penetration Test or full Application Assessment (MASA/WASA) must be performed that includes automated and manual assessment tools and techniques for the following:

- A FISMA High and/or Internet facing system, considered a major or minor application.
- A FISMA Moderate or higher, that processes, uses, or hosts PII and/or financial data.
- For Internet facing applications, if the application utilizes multiple servers then a WASA and Penetration Test are required, regardless of the FIPS categorization. If the Internet facing application only uses one server then only a WASA is required.

- For systems that are not web-based or host a user presented web application but have middleware or APIs, a Penetration Test and WASA must be performed.
- If a Penetration Test / Application Assessment is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
- The Penetration Test / Application Assessment requirement is not applicable to the VistA authorization boundary.

Completion Steps

1. Systems with custom code must be registered with OIS Software Assurance and receive a "PASS" from the Code Review process prior to requesting an application assessment (MASA/WASA).
2. A system utilizing a COTS product still must register with OIS Software Assurance.
3. The ISO or system steward can request a penetration test/application assessment by completing the CSOC Penetration Test Questionnaire/ CSOC Mobile Application Security Assessment (MASA) Questionnaire/CSOC Web Application Security Assessment (WASA) Questionnaire. Additional scan details can be found at CSOC Scan Documents. Please allow 30 days for CSOC to schedule/conduct the penetration test/application assessment. Questions can be submitted to VA CSOC.
    a. CSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. CSOC must have visibility into all VA applications where an authorization decision is required, including systems behind firewalls. External systems must also have a recent CSOC penetration test/application assessment performed either remotely or by utilizing CSOC staff on-site to perform scans, when necessary.
4. CSOC will provide results to the ISO or system steward.
5. The ISO or system steward uploads the summary and raw results to the Artifacts tab in eMASS along with the mitigation / remediation plan for all findings.
    a. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-CSOC or as a separate document.
6. The ISO or system steward creates one finding and a response in the POA&M tab within eMASS for the Penetration Test/Application Assessment. Refer to the POA&M Management Guide for additional details.
7. Once the deficiencies have been mitigated, a follow-up Penetration Test/Application Assessment should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A CSOC Penetration Test/Application Assessment is required on an annual basis or when a major change to the system or data occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.1.2.4 Application Security Testing

Application Security Testing is conducted during the development or maintenance of a VA application. Close cooperation between OIS and the Office of Information Technology (OIT), including supporting contractors, is critical to achieving application security testing objectives and increasing the level of confidence that software developed for use at the VA is free from vulnerabilities.

Successful completion of the software assurance validation of developer-performed scans is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

The following guidance should be considered for the Application Security Testing:

- VA application developers are responsible for conducting application security testing
- Custom-developed VA applications are required to undergo application security testing
- Application security testing must be conducted using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) tool
- Testing results must be validated by software assurance for correctness and completeness
- Production source code is required to be provided along with audited scans and supporting analysis, including a text file named "resubmission.txt" explaining changes since any prior validation, using the application's restricted software assurance file share on the VA network
- Successful completion of the application security testing validation process is required as a prerequisite to a CSOC penetration test / application assessment
- This requirement is not applicable to VistA systems
- Findings should be created in eMASS for vulnerabilities that are not mitigated

Office of Information Security (OIS) Staff will upload application security testing validation report results (code scans) to eMASS. Subsequent to the upload of scan results to eMASS, the system POC(s) will receive a notification.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for

creating at least one POAM per scan to document remediation and mitigation activities.

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Application Security Scan Validation** in the **Services Request** field.
6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

Successfully completing the software assurance validation of developer-performed scans requires obtaining an overall passing verdict, repeating the process as necessary if failing verdicts are returned.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- For teams that are using automation for continuous integration and delivery (CI/CD), potentially continuous deployment, successful completion of the software assurance validation of scans is required after the initial release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).
- For teams that are not using automation for CI/CD, successful completion of the software assurance validation of scans is required after the initial release on either

release or calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).

Successful completion of the software assurance validation of scans is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning application source code for potential vulnerabilities using the Fortify tool can be found on the software assurance developer support site.

4.1.2.5 Application Threat Modeling

Application Threat Modeling is required for all custom developed systems/applications. The following guidance should be considered for the Application Threat Modeling:

- VA application developers are responsible for performing application threat modeling
- Custom-developed VA applications are required to have documented threat models
- The latest version of the Microsoft Threat Modeling Tool must be used
- Sample VA application threat models may be requested from software assurance
- A POA&M item should be created in eMASS for potential threats that are not mitigated
- This requirement is not applicable to VistA systems

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Threat Model Samples** in the **Services Request** field.
6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on the software assurance developer support site.

4.1.2.6 Security Control Assessment (SCA)

The SCA section is in the process of being updated to incorporate the use of eMASS.

4.2 Application hosted in Managed Service

Managed Service (also known as external systems) are systems that are managed outside the VA network. Technical scans and/or security documents should be provided (as applicable) for each Managed Service.

4.2.1 Security Documentation

4.2.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

Roles and Responsibilities

Currently, there's not a CMP template available. The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-2) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

4.2.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by OIS. Each year Emergency Preparedness & Response (EPR) will provide planning and testing guidance through an action item. DRP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item.
- The ISO or system steward works with the assigned ISSO to create or revise the DRP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS.
2. The ISO or system steward develops or revises the DRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change to the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.2.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the

FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.2.1.4 Information Security Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item. ISCP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- The ISO or system steward works with the assigned ISSO to create or revise the ISCP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. If yes, then the ISO or system steward will be required to upload the ISCP to eMASS.
2. The ISO or system steward develops or revises the ISCP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the

FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.2.1.5 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The Business Requirements MOU/ISA Review Team will assess the documents for quality, content and security.
4. The Business Requirements Division (BRD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the BRD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the Business Requirements Division.

4.2.1.6 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.

2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.2.1.7 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.

3. By default, the Risk Assessment tab will only show Non-Compliant Controls but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.2.1.8 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward completes the RMF steps in eMASS and develops POA&Ms for all CCIs marked Non-Compliant. eMASS will apply the user's N/A justification (test result) to automatically generate a POA&M item for all controls marked as Not Applicable.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.2.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the VA Handbook 6500 and BOD 19-02 (i.e.), Critical – 15 days; High – 30 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. A POA&M item should be created in

eMASS for each of the applicable scans to track the remediation progress. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should also be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.2.2.1 Nessus Scan

A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. If the system receives a monthly predictive Nessus vulnerability scan from CSOC and the IP addresses that make up the system are all Windows based then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded, then proceed to Step 3.
    a. If the system receives a monthly predictive Nessus vulnerability scan from CSOC, and the IP addresses that make up the system are not all Windows based, then proceed to step 2, as all necessary Operating System information will not be captured in the predictive scans from CSOC.
    b. If the IP addresses that make up a system are outside of the VA network (Managed Services) and/or the system does not currently receive a monthly predictive Nessus vulnerability scan from CSOC, then proceed to Step 2.

2. The ISO or system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If its decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded.

3. Once the system's Nessus Scan data is accurately recorded, the ISO or system steward follows these steps:

a. Browse to Information Central Analytics and Metrics Platforms (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
c. Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.
d. The ISO or system steward then uploads the mitigation/remediation report to the Artifacts tab within eMASS using the naming instructions identified in Section 4 Assessment and Authorization Requirements.
e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Nessus scan.

5. A follow-up Nessus scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems and Managed Services. External systems / Managed Services must have a recent CSOC Nessus scan conducted either via remote connection or by utilizing CSOC staff on-site to perform scans, when necessary.

4.2.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

1. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, upload a word document to the Artifacts tab within eMASS explaining why a database scan is not applicable.
2. Once the Database scan is completed, the summary and raw results must be uploadd to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings and a POA&M must be created in eMASS to keep track of the remediation effort.
3. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.2.2.3 Application Security Testing

Application Security Testing is conducted during the development or maintenance of a VA application. Close cooperation between OIS and the Office of Information Technology (OIT), including supporting contractors, is critical to achieving application security testing objectives and increasing the level of confidence that software developed for use at the VA is free from vulnerabilities.

Successful completion of the software assurance validation of developer-performed scans is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

The following guidance should be considered for the Application Security Testing:

- VA application developers are responsible for conducting application security testing
- Custom-developed VA applications are required to undergo application security testing
- Application security testing must be conducted using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) tool
- Testing results must be validated by software assurance for correctness and completeness
- Production source code is required to be provided along with audited scans and supporting analysis, including a text file named "resubmission.txt" explaining changes

since any prior validation, using the application's restricted software assurance file share on the VA network
- Successful completion of the application security testing validation process is required as a prerequisite to a CSOC penetration test / application assessment
- This requirement is not applicable to VistA systems
- Findings should be created in eMASS for vulnerabilities that are not mitigated

Office of Information Security (OIS) Staff will upload application security testing validation report results (code scans) to eMASS. Subsequent to the upload of scan results to eMASS, the system POC(s) will receive a notification.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for creating at least one POAM per scan to document remediation and mitigation activities.

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Application Security Scan Validation** in the **Services Request** field.
6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

Successfully completing the software assurance validation of developer-performed scans requires obtaining an overall passing verdict, repeating the process as necessary if failing verdicts are returned.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- For teams that are using automation for continuous integration and delivery (CI/CD), potentially continuous deployment, successful completion of the software assurance validation of scans is required after the initial release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).
- For teams that are not using automation for CI/CD, successful completion of the software assurance validation of scans is required after the initial release on either release or calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).

Successful completion of the software assurance validation of scans is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning application source code for potential vulnerabilities using the Fortify tool can be found on the software assurance developer support site.

4.2.2.4 Application Threat Modeling

Application Threat Modeling is required for all custom developed systems/applications. The following guidance should be considered for the Application Threat Modeling:

- VA application developers are responsible for performing application threat modeling
- Custom-developed VA applications are required to have documented threat models
- The latest version of the Microsoft Threat Modeling Tool must be used
- Sample VA application threat models may be requested from software assurance
- A POA&M item should be created in eMASS for potential threats that are not mitigated
- This requirement is not applicable to VistA systems

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Threat Model Samples** in the **Services Request** field.

6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on the software assurance developer support site.

4.2.2.5 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e. servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online at YourIT.
2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. The ISO or System Steward

must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.

3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO and/or System Steward uploads the Checklist Trending and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 aboveAssessment and Authorization Requirements.
5. The ISO and/or System Steward creates a POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. Please refer to the POA&M Management Guide for instructions on creating a POA&M item in eMASS.
6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.2.2.6 Security Control Assessment (SCA)

The SCA section is in the process of being updated to incorporate the use of eMASS.

4.3 Application hosted in FedRAMP cloud (VAEC)

Once approval from the GRC Committee has been received and the system has been registered in eMASS with the recognition that it utilizes the VA Enterprise Cloud (VAEC), the System Owner or delegate should work with the VAEC cloud team to ensure all VAEC requirements are met. Information regarding the requirements can be found at the VAEC main page. The Security Documentation and Technical/Testing requirements listed below are a guideline for the typical requirements to receive an ATO. If the Security Documentation or Technical/Testing requirements is not applicable for the eMASS authorization package, then a word document detailing the reasons why it's not applicable must be uploaded to the Artifacts tab within eMASS.

VA OIS leadership has established the VA Tier 1 SOR (T1SOR) as Common Control Providers (e.g. Hosting Facilities, Organizational Policy Records, etc.) to facilitate the automated establishment of inheritance relationships. VA T1SOR is available for applications in the VAEC. Instructions for applying VA T1SOR for VAEC AWS or Microsoft Azure can be found on the VAEC site. Refer to Appendix D – Common Control Providers/System of Record (SOR) for additional details on the VA T1SOR.

4.3.1 Security Documentation

4.3.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

Roles and Responsibilities

A CMP template for VAEC AWS and VAEC Azure can be found at the VAEC main page. The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-2) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

4.3.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by OIS. Each year Emergency Preparedness & Response (EPR) will provide planning and testing guidance through an action item. DRP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item.
- The ISO or system steward works with the assigned ISSO to create or revise the DRP. A DRP template for VAEC AWS and VAEC Azure can be found at the VAEC main page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS.
2. The ISO or system steward develops or revises the DRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions)

within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change to the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.3.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP. An IRP template for VAEC AWS and VAEC Azure can be found at the VAEC main page.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.

2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.3.1.4 Information Security Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item. ISCP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- The ISO or system steward works with the assigned ISSO to create or revise the ISCP. An ISCP template for VAEC AWS and VAEC Azure can be found at the VAEC main page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. If yes, then the ISO or system steward will be required to upload the ISCP to eMASS.
2. The ISO or system steward develops or revises the ISCP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.3.1.5 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.

- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The Business Requirements MOU/ISA Review Team will assess the documents for quality, content and security.
4. The Business Requirements Division (BRD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the BRD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the Business Requirements Division.

4.3.1.6 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22

- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.3.1.7 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.3.1.8 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward completes the RMF steps in eMASS and develops POA&Ms for all CCIs marked Non-Compliant. eMASS will apply the user's N/A justification (test result) to automatically generate a POA&M item for all controls marked as Not Applicable.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.3.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the VA Handbook 6500 and BOD 19-02 (i.e.), Critical – 15 days; High – 30 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. A POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should also be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.3.2.1 Nessus Scan

A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. If the system receives a monthly predictive Nessus vulnerability scan from CSOC and the IP addresses that make up the system are all Windows based then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded, then proceed to Step 3.
    a. If the system receives a monthly predictive Nessus vulnerability scan from CSOC, and the IP addresses that make up the system are not all Windows based, then proceed to step 2, as all necessary Operating System information will not be captured in the predictive scans from CSOC.
    b. If the IP addresses that make up a system are outside of the VA network (Managed Services) and/or the system does not currently receive a monthly predictive Nessus vulnerability scan from CSOC, then proceed to Step 2.

2. The ISO or system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If its decided that the authentication

information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded.

3. Once the system's Nessus Scan data is accurately recorded, the ISO or system steward follows these steps:

    a. Browse to Information Central Analytics and Metrics Platforms (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.
    d. The ISO or system steward then uploads the mitigation/remediation report to the Artifacts tab within eMASS using the naming instructions identified in Section 4 Assessment and Authorization Requirements.
    e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Nessus scan.

5. A follow-up Nessus scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities

potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems. External systems must have a recent CSOC Nessus scan conducted either via remote connection or by utilizing CSOC staff on-site to perform scans, when necessary.

4.3.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

1. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, upload a word document to the Artifacts tab within eMASS explaining why a database scan is not applicable.
2. Once the Database scan is completed, the summary and raw results must be uploadd to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings and a POA&M must be created in eMASS to keep track of the remediation effort.
3. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.3.2.3 Penetration Test/Application Assessment

A Penetration Test or full Application Assessment (MASA/WASA) must be performed that includes automated and manual assessment tools and techniques for the following:

- A FISMA High and/or Internet facing system, considered a major or minor application.
- A FISMA Moderate or higher, that processes, uses, or hosts PII and/or financial data.
- For systems residing in a cloud environment or external to the VA network, connections must be in place through the Trust Internet Connection (TIC) prior to assessment to facilitate connectivity from the CSOC internal testing servers.
- For Internet facing applications, if the application utilizes multiple servers then a WASA and Penetration Test are required, regardless of the FIPS categorization. If the Internet facing application only uses one server then only a WASA is required.

- For systems that are not web-based or host a user presented web application but have middleware or APIs, a Penetration Test and WASA must be performed.
- If a Penetration Test / Application Assessment is not applicable, upload a word document to the Artifacts tab within eMASS explaining why a Penetration Test / Application Assessment is not applicable.
- The Penetration Test / Application Assessment requirement is not applicable to the VistA authorization boundary.

Completion Steps

1. Systems with custom code must be registered with OIS Software Assurance and receive a "PASS" from the Code Review process prior to requesting an application assessment (MASA/WASA).
2. A system utilizing a COTS product still must register with OIS Software Assurance.
3. The ISO or system steward can request a penetration test/application assessment by completing the CSOC Penetration Test Questionnaire/ CSOC Mobile Application Security Assessment (MASA) Questionnaire/CSOC Web Application Security Assessment (WASA) Questionnaire. Additional scan details can be found at CSOC Scan Documents. Please allow 30 days for CSOC to schedule/conduct the penetration test/application assessment. Questions can be submitted to VA CSOC.
    a. CSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. CSOC must have visibility into all VA applications where an authorization decision is required, including systems behind firewalls. External systems must also have a recent CSOC penetration test/application assessment performed either remotely or by utilizing CSOC staff on-site to perform scans, when necessary.
4. CSOC will provide results to the ISO or system steward.
5. The ISO or system steward uploads the summary and raw results to the Artifacts tab in eMASS along with the mitigation / remediation plan for all findings.
    a. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-CSOC or as a separate document.
6. The ISO or system steward creates one finding and a response in the POA&M tab within eMASS for the Penetration Test/Application Assessment. Refer to the POA&M Management Guide for additional details.
7. Once the deficiencies have been mitigated, a follow-up Penetration Test/Application Assessment should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A CSOC Penetration Test/Application Assessment is required on an annual basis or when a major change to the system or data occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.3.2.4 Application Security Testing

Application Security Testing is conducted during the development or maintenance of a VA application. Close cooperation between OIS and the Office of Information Technology (OIT), including supporting contractors, is critical to achieving application security testing objectives and increasing the level of confidence that software developed for use at the VA is free from vulnerabilities.

Successful completion of the software assurance validation of developer-performed scans is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

The following guidance should be considered for the Application Security Testing:

- VA application developers are responsible for conducting application security testing
- Custom-developed VA applications are required to undergo application security testing
- Application security testing must be conducted using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) tool
- Testing results must be validated by software assurance for correctness and completeness
- Production source code is required to be provided along with audited scans and supporting analysis, including a text file named "resubmission.txt" explaining changes since any prior validation, using the application's restricted software assurance file share on the VA network
- Successful completion of the application security testing validation process is required as a prerequisite to a CSOC penetration test / application assessment
- This requirement is not applicable to VistA systems
- Findings should be created in eMASS for vulnerabilities that are not mitigated

Office of Information Security (OIS) Staff will upload application security testing validation report results (code scans) to eMASS. Subsequent to the upload of scan results to eMASS, the system POC(s) will receive a notification.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for

creating at least one POAM per scan to document remediation and mitigation activities.

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Application Security Scan Validation** in the **Services Request** field.
6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

Successfully completing the software assurance validation of developer-performed scans requires obtaining an overall passing verdict, repeating the process as necessary if failing verdicts are returned.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- For teams that are using automation for continuous integration and delivery (CI/CD), potentially continuous deployment, successful completion of the software assurance validation of scans is required after the initial release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).
- For teams that are not using automation for CI/CD, successful completion of the software assurance validation of scans is required after the initial release on either

release or calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).

Successful completion of the software assurance validation of scans is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning application source code for potential vulnerabilities using the Fortify tool can be found on the software assurance developer support site.

4.3.2.5 Application Threat Modeling

Application Threat Modeling is required for all custom developed systems/applications. The following guidance should be considered for the Application Threat Modeling:

- VA application developers are responsible for performing application threat modeling
- Custom-developed VA applications are required to have documented threat models
- The latest version of the Microsoft Threat Modeling Tool must be used
- Sample VA application threat models may be requested from software assurance
- A POA&M item should be created in eMASS for potential threats that are not mitigated
- This requirement is not applicable to VistA systems

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Threat Model Samples** in the **Services Request** field.
6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on the software assurance developer support site.

4.3.2.6 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e. servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online at YourIT.
2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. They must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.
3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending and

Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).

4. The ISO and/or System Steward uploads the Checklist Trending and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 aboveAssessment and Authorization Requirements.
5. The ISO and/or System Steward creates a POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. Please refer to the POA&M Management Guide for instructions on creating a POA&M item in eMASS.
6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.3.2.7 Security Control Assessment (SCA)

The SCA section is in the process of being updated to incorporate the use of eMASS.

4.4 Application hosted in FedRAMP cloud (Non-VAEC)

Once approval from the GRC Committee has been received and the system has been registered in eMASS with the recognition that it utilizes a FedRAMP cloud but not the VAEC, the System Owner or delegate must work to ensure all the Security Documentation and Technical/Testing requirements listed below are completed and included with the eMASS authorization package. If the Security Documentation or Technical/Testing requirements is not applicable for the eMASS authorization package, then a word document detailing the reasons why it's not applicable must be uploaded to the Artifacts tab within eMASS.

4.4.1 Security Documentation

4.4.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

Roles and Responsibilities

Currently, there's not a CMP template available. The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-2) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

4.4.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by OIS. Each year Emergency Preparedness & Response (EPR) will provide planning and testing guidance through an action item. DRP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item.
- The ISO or system steward works with the assigned ISSO to create or revise the DRP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems

- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS.
2. The ISO or system steward develops or revises the DRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change to the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.4.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.

- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.4.1.4 Information Security Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item. ISCP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.

- The ISO or system steward works with the assigned ISSO to create or revise the ISCP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. If yes, then the ISO or system steward will be required to upload the ISCP to eMASS.
2. The ISO or system steward develops or revises the ISCP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.4.1.5 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection

between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The Business Requirements MOU/ISA Review Team will assess the documents for quality, content and security.
4. The Business Requirements Division (BRD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the BRD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the Business Requirements Division.

4.4.1.6 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.4.1.7 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.4.1.8 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward completes the RMF steps in eMASS and develops POA&Ms for all CCIs marked Non-Compliant. eMASS will apply the user's N/A justification (test result) to automatically generate a POA&M item for all controls marked as Not Applicable.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.4.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the VA Handbook 6500 and BOD 19-02 (i.e.), Critical – 15 days; High – 30 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. A POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should also be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.4.2.1 Nessus Scan

A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. If the system receives a monthly predictive Nessus vulnerability scan from CSOC and the IP addresses that make up the system are all Windows based then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded, then proceed to Step 3.

a. If the system receives a monthly predictive Nessus vulnerability scan from CSOC, and the IP addresses that make up the system are not all Windows based, then proceed to step 2, as all necessary Operating System information will not be captured in the predictive scans from CSOC.
b. If the IP addresses that make up a system are outside of the VA network (Managed Services) and/or the system does not currently receive a monthly predictive Nessus vulnerability scan from CSOC, then proceed to Step 2.

2. The ISO or system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If it's decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded.

3. Once the system's Nessus Scan data is accurately recorded, the ISO or system steward follows these steps:

    a. Browse to Information Central Analytics and Metrics Platforms (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.
    d. The ISO or system steward then uploads the mitigation/remediation report to the Artifacts tab within eMASS using the naming instructions identified in Section 4 Assessment and Authorization Requirements.
    e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Nessus scan.

5. A follow-up Nessus scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems. External systems must have a recent CSOC Nessus scan conducted either via remote connection or by utilizing CSOC staff on-site to perform scans, when necessary.

4.4.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

4. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, upload a word document to the Artifacts tab within eMASS explaining why a database scan is not applicable.

5. Once the Database scan is completed, the summary and raw results must be uploadd to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings and a POA&M must be created in eMASS to keep track of the remediation effort.

6. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.4.2.3 Penetration Test/Application Assessment

A Penetration Test or full Application Assessment (MASA/WASA) must be performed that includes automated and manual assessment tools and techniques for the following:

- A FISMA High and/or Internet facing system, considered a major or minor application.
- A FISMA Moderate or higher, that processes, uses, or hosts PII and/or financial data.
- For systems residing in a cloud environment or external to the VA network, connections must be in place through the Trust Internet Connection (TIC) prior to assessment to facilitate connectivity from the CSOC internal testing servers.
- For Internet facing applications, if the application utilizes multiple servers then a WASA and Penetration Test are required, regardless of the FIPS categorization. If the Internet facing application only uses one server then only a WASA is required.
- For systems that are not web-based or host a user presented web application but have middleware or APIs, a Penetration Test and WASA must be performed.
- If a Penetration Test / Application Assessment is not applicable, upload a word document to the Artifacts tab within eMASS explaining why a Penetration Test / Application Assessment is not applicable.
- The Penetration Test / Application Assessment requirement is not applicable to the VistA authorization boundary.

Completion Steps

1. Systems with custom code must be registered with OIS Software Assurance and receive a “PASS” from the Code Review process prior to requesting an application assessment (MASA/WASA).
2. A system utilizing a COTS product still must register with OIS Software Assurance.
3. The ISO or system steward can request a penetration test/application assessment by completing the CSOC Penetration Test Questionnaire/ CSOC Mobile Application Security Assessment (MASA) Questionnaire/CSOC Web Application Security Assessment (WASA) Questionnaire. Additional scan details can be found at CSOC Scan Documents. Please allow 30 days for CSOC to schedule/conduct the penetration test/application assessment. Questions can be submitted to VA CSOC.
    a. CSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. CSOC must have visibility into all VA applications where an authorization decision is required, including systems behind firewalls. External systems must also have a recent CSOC penetration test/application assessment performed either remotely or by utilizing CSOC staff on-site to perform scans, when necessary.
4. CSOC will provide results to the ISO or system steward.

5. The ISO or system steward uploads the summary and raw results to the Artifacts tab in eMASS along with the mitigation / remediation plan for all findings.
    a. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-CSOC or as a separate document.
6. The ISO or system steward creates one finding and a response in the POA&M tab within eMASS for the Penetration Test/Application Assessment. Refer to the POA&M Management Guide for additional details.
7. Once the deficiencies have been mitigated, a follow-up Penetration Test/Application Assessment should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A CSOC Penetration Test/Application Assessment is required on an annual basis or when a major change to the system or data occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.4.2.4 Application Security Testing

Application Security Testing is conducted during the development or maintenance of a VA application. Close cooperation between OIS and the Office of Information Technology (OIT), including supporting contractors, is critical to achieving application security testing objectives and increasing the level of confidence that software developed for use at the VA is free from vulnerabilities.

Successful completion of the software assurance validation of developer-performed scans is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

The following guidance should be considered for the Application Security Testing:

- VA application developers are responsible for conducting application security testing
- Custom-developed VA applications are required to undergo application security testing
- Application security testing must be conducted using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) tool
- Testing results must be validated by software assurance for correctness and completeness
- Production source code is required to be provided along with audited scans and supporting analysis, including a text file named "resubmission.txt" explaining changes since any prior validation, using the application's restricted software assurance file share on the VA network

- Successful completion of the application security testing validation process is required as a prerequisite to a CSOC penetration test / application assessment
- This requirement is not applicable to VistA systems
- Findings should be created in eMASS for vulnerabilities that are not mitigated

Office of Information Security (OIS) Staff will upload application security testing validation report results (code scans) to eMASS. Subsequent to the upload of scan results to eMASS, the system POC(s) will receive a notification.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for creating at least one POAM per scan to document remediation and mitigation activities.

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Application Security Scan Validation** in the **Services Request** field.
6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

Successfully completing the software assurance validation of developer-performed scans requires obtaining an overall passing verdict, repeating the process as necessary if failing verdicts are returned.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- For teams that are using automation for continuous integration and delivery (CI/CD), potentially continuous deployment, successful completion of the software assurance validation of scans is required after the initial release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).
- For teams that are not using automation for CI/CD, successful completion of the software assurance validation of scans is required after the initial release on either release or calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing).

Successful completion of the software assurance validation of scans is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning application source code for potential vulnerabilities using the Fortify tool can be found on the software assurance developer support site.

4.4.2.5 Application Threat Modeling

Application Threat Modeling is required for all custom developed systems/applications. The following guidance should be considered for the Application Threat Modeling:

- VA application developers are responsible for performing application threat modeling
- Custom-developed VA applications are required to have documented threat models
- The latest version of the Microsoft Threat Modeling Tool must be used
- Sample VA application threat models may be requested from software assurance
- A POA&M item should be created in eMASS for potential threats that are not mitigated
- This requirement is not applicable to VistA systems

Completion Steps

1. Navigate to the Your IT Services portal using your web browser.
2. Click on **Make a Request** on the homepage.
3. Click on the **Vulnerability Management** category.
4. Click on **Software Assurance Request**.
5. Fill out the form and select **Threat Model Samples** in the **Services Request** field.

6. Click on the **Submit** button.
7. Make a note of your ticket's request number.

After the request has been made, a VA Software Assurance Program team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on the software assurance developer support site.

4.4.2.6 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e. servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online at YourIT.
2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. They must ensure all

hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.

3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO and/or System Steward uploads the Checklist Trending and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 aboveAssessment and Authorization Requirements.
5. The ISO and/or System Steward creates a POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. Please refer to the POA&M Management Guide for instructions on creating a POA&M item in eMASS.
6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.4.2.7 Security Control Assessment (SCA)

The SCA section is in the process of being updated to incorporate the use of eMASS.

4.5 Facility

Facility authorizations describe the local processes that differ from enterprise standards, including security control requirements provided by Contingency Planning, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, and System and Information Integrity. Facility authorization boundaries include IT Hardware (i.e., servers, printers, scanners, peripheral devices, desktop computer systems) and any operating systems (OS) software specific to the facility.

Facilities may choose to inherit common control providers from the VA T1SOR, IO SOR, or VA Area SOR. Refer to Appendix D – Common Control Providers/System of Record (SOR) for complete details to help determine if the VA T1SOR, IO SOR, or VA Area SOR is applicable.

4.5.1 Security Documentation

4.5.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

Roles and Responsibilities

Currently, there's not a CMP template available. The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-2) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change occurs.

4.5.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by OIS. Each year Emergency Preparedness & Response (EPR) will provide planning and testing guidance through an action item. DRP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item.
- The ISO or system steward works with the assigned ISSO to create or revise the DRP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS.
2. The ISO or system steward develops or revises the DRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.5.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change occurs.

4.5.1.4 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The Business Requirements MOU/ISA Review Team will assess the documents for quality, content and security.

4. The Business Requirements Division (BRD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the BRD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the agreement as documented, please contact the Business Requirements Division.

4.5.1.5 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.5.1.6 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.5.1.7 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward completes the RMF steps in eMASS and develops POA&Ms for all CCIs marked Non-Compliant. eMASS will apply the user's N/A justification (test result) to automatically generate a POA&M item for all controls marked as Not Applicable.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.5.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the VA Handbook 6500 and BOD 19-02 (i.e.), Critical – 15 days; High – 30 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP.

4.5.2.1 Nessus Scan

A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations for the facility IP addresses must be conducted to identify security flaws.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. If the system receives a monthly predictive Nessus vulnerability scan from CSOC and the IP addresses for the facility are all Windows based then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded, then proceed to Step 3.

    a. If the system receives a monthly predictive Nessus vulnerability scan from CSOC, and the IP addresses that make up the system are not all Windows based, then proceed to step 2, as all necessary Operating System information will not be captured in the predictive scans from CSOC.
    b. If the IP addresses that make up a system are outside of the VA network (Managed Services) and/or the system does not currently receive a monthly predictive Nessus vulnerability scan from CSOC, then proceed to Step 2.

2. The ISO or system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If its decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then please provide the IP Ranges to ISRM, so the applicable Nessus data can be recorded.

3. Once the system's Nessus Scan data is accurately recorded, the ISO or system steward follows these steps:

    a. Browse to Information Central Analytics and Metrics Platforms (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.
    d. The ISO or system steward then uploads the mitigation/remediation report to the Artifacts tab within eMASS using the naming instructions identified in Section 4 Assessment and Authorization Requirements.
    e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise

mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Nessus scan.
5. A follow-up Nessus scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: Facility boundaries should identify physical specifics and identify hardware/software applicable to each Facility.

4.5.2.2 Enterprise Discovery Scan (EDS)

If required by OIS, an Enterprise Discovery Scan (EDS) against all instances of the operating system and desktop configurations must be conducted to identify security flaws. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings, and a POA&M must be created in eMASS to keep track of the remediation effort.

Completion Steps

1. Browse to the Information Central Analytics and Metrics Platform (ICAMP) and use the EDS input (EDSI) form to document your manual remediation effort. For each deficiency identified from the scan, the ISO or system steward creates a response within EDSI for mitigating the deficiencies and / or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within EDSI.
2. Once all the manual remediation has been documented within EDSI, run this report within ICAMP: https://spsites.cdw.va.gov//sites/FODW_PVT/Progress%20Reports/EDS_ATO_Mitigation.rdl
3. Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.
4. The ISO or system steward then uploads the report from step 3 above to the Artifacts tab within eMASS using the naming instructions identified in Section 4 Assessment and

Authorization Requirements. A mitigation plan should also be uploaded to the Artifacts tab within eMASS.

5. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the EDS to determine and document the findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or by the vendor should be documented as part of this analysis.
6. The ISO or system steward creates a POA&M and a response in the POA&M tab within eMASS for the EDS as outlined by the POA&M Management Guide.

Continuous Monitoring

CSOC conducts EDS on a quarterly basis. The quarterly results must be pulled in accordance with the guidance above to maintain an ATO. The EDS results must be provided when the tool used receives an upgrade or a major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.5.2.3 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e. servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online at YourIT.
2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. They must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g.,

"R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.

3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO and/or System Steward uploads the Checklist Trending and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 aboveAssessment and Authorization Requirements.
5. The ISO and/or System Steward creates a POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. Please refer to the POA&M Management Guide for instructions on creating a POA&M item in eMASS.
6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.5.2.4 Security Control Assessment (SCA)

The SCA section is in the process of being updated to incorporate the use of eMASS.

4.6 Medical Devices

Medical Devices are MRIs, Pacemakers, X-ray machines, etc. Generally, web applications are not Medical Devices. The Medical Devices boundary consists of required diagrams for all

devices (medical devices and special purpose systems (SPSs), where applicable), supporting software architecture, IP ranges, and documentation of all minor applications within the boundary. The ISSO should provide assistance to the ISO or System Steward with Medical Device authorization requirements.

4.6.1 Security Documentation

4.6.1.1 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The Business Requirements MOU/ISA Review Team will assess the documents for quality, content and security.

4. The Business Requirements Division (BRD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the BRD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the Business Requirements Division.

4.6.1.2 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change occurs, then a new PTA/PIA must be completed.

4.6.1.3 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change occurs.

4.6.1.4 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward completes the RMF steps in eMASS and develops POA&Ms for all CCIs marked Non-Compliant. eMASS will apply the user's N/A justification (test result) to automatically generate a POA&M item for all controls marked as Not Applicable.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change occurs.

4.6.2 Technical Scans/Testing Requirements

4.6.2.1 Security Control Assessment (SCA)

The SCA section is in the process of being updated to incorporate the use of eMASS.

4.7 Other Federal Agency (Non-eMASS Reciprocity)

An 'Other Federal Agency' system allows the VA to utilize a pre-existing ATO from a Federal Agency and grant a reciprocity based ATO so the VA can utilize the system. The system needs to be approved by the VA GRC Oversight Committee and entered into eMASS. A non-eMASS reciprocity ATO can be granted by the AO once a Risk Review of the system is completed. The review of security artifacts may take place in person by the Risk Review team at the 'Other Federal Agency' facility or virtually if online access can be granted to the Risk Review team. The Risk Review must ensure that the 'Other Federal Agency' ATO meets VA standards. Any VA

required security documentation, such as an ISA/MOU or PTA/PIA, must be completed and uploaded to the Artifacts tab within eMASS by the ISO, system steward, and/or ISSO.

4.8 Platform

The different Platform boundaries throughout the VA require an authorization decision; however, due to the nature of these platforms, there's a limited number of technical scans/testing requirements that can be completed. The following authorization requirements must be completed for IO Network Operations, IO Platform Support Mainframe, IO Platform Support UNIX, and IO Platform Support Windows.

Platforms may choose to inherit common control providers from the VA T1SOR and IO SOR. Refer to Appendix D – Common Control Providers/System of Record (SOR) for complete details to help determine if the VA T1SOR or IO SOR is applicable.

4.8.1 Security Documentation

4.8.1.1 Information Security Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item. ISCP guidance is provided below.

Roles and Responsibilities

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- The ISO or system steward works with the assigned ISSO to create or revise the ISCP.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

5. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. If yes, then the ISO or system steward will be required to upload the ISCP to eMASS.
6. The ISO or system steward develops or revises the ISCP using the applicable standards and guidelines.

7. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
8. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

Note: Questions about the planning process, plan templates, or testing process should contact the EPR team.

4.8.1.2 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The Business Requirements MOU/ISA Review Team will assess the documents for quality, content and security.
4. The Business Requirements Division (BRD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the BRD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the Business Requirements Division.

4.8.1.3 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.

- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.8.1.4 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.

2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.8.1.5 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward completes the RMF steps in eMASS and develops POA&Ms for all CCIs marked Non-Compliant. eMASS will apply the user's N/A justification (test result) to automatically generate a POA&M item for all controls marked as Not Applicable.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.8.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified

in the VA Handbook 6500 and BOD 19-02 (i.e.), Critical – 15 days; High – 30 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. A POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should also be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.8.2.1 Security Control Assessment (SCA)

The SCA section is in the process of being updated to incorporate the use of eMASS.

5 Appendix A – Acronyms/Definitions

Acronym	Description
A&A	Assessment and Authorization
AO	Authorizing Official
ATO	Authority to Operate
BRD	Business Requirements Division
CAE	Common Application Enumeration
CCI	Control Correlation Identifier
CIO	Chief Information Office
CMP	Configuration Management Plan
COTS	Commercial off the shelf
CSOC	Cyber Security Operations Center
DRP	Disaster Recovery Plan
EDS	Enterprise Discovery Scan
eMASS	Enterprise Mission Assurance Support Service
EPR	Emergency Preparedness & Response
FISMA	Federal Information Security Management Act
GRC	Governance, Risk, and Compliance
ICAMP	Information Central Analytics and Metrics Platform
IO SOR	Infrastructure Operations System of Record
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISCP	Information Security Contingency Plan
ISO	Information System Owner
ISRM	Information Security and Risk Management
ISSO	Information System Security Officer
MASA	Mobile Application Security Assessment
MOU	Memorandum of Understanding
OIS	Office of Information Security
OIT	Office of Information Technology
OPR	Office of Primary Responsibility
PDAS	Primary Deputy Assistant Secretary
PIA	Privacy Impact Assessment
POA&M	Plan of Actions and Milestones
PTA	Privacy Threshold Analysis
RAR	Risk Assessment Report
REEF	Remediation Effort Entry Form
RMF	Risk Management Framework
SaaS	Software-as-a-Service
SCA	Security Control Assessment

SCCD	Security Configuration Compliance Data
SIA	Security Impact Analysis
SSP	System Security Plan
SwA	Software Assurance
TIC	Trusted Internet Connection
VAEC	VA Enterprise Cloud
VASI	VA Systems Inventory
VA T1SOR	Veterans Affairs Tier I System of Record
WASA	Web Application Security Assessment

6 *Appendix B – Quick Reference Guide – Security Documentation Requirements*

Boundary	Security Document	Required Y/N
Application hosted on Premier/ VA Network	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Incident Response Plan	Y
	Information System Contingency Plan	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
Application hosted in Managed Service	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Incident Response Plan	Y
	Information System Contingency Plan	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
Application hosted in FedRAMP cloud (VAEC)	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Incident Response Plan	Y
	Information System Contingency Plan	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
Application hosted in FedRAMP cloud (Non-VAEC)	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Incident Response Plan	Y

	Information System Contingency Plan	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
Facility	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Incident Response Plan	Y
	Information System Contingency Plan	N
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
Medical Devices	Configuration Management Plan	N
	Disaster Recovery Plan	N
	Incident Response Plan	N
	Information System Contingency Plan	N
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
Other Federal Agency (Non-eMASS Reciprocity)	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Incident Response Plan	Y
	Information System Contingency Plan	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
Platform	Configuration Management Plan	N
	Disaster Recovery Plan	N

	Incident Response Plan	N
	Information System Contingency Plan	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y

7 Appendix C – Quick Reference Guide – Technical/Testing Requirements

Boundary	Technical / Testing Requirements	Required Y/N
Application hosted on Premier/ VA Network	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y – if applicable
	Application Security Testing	Y – if applicable
	Application Threat Modeling	Y – if applicable
	Security Configuration Compliance Data	N
	Security Control Assessment	Y – if applicable
Application hosted in Managed Service	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	N
	Application Security Testing	Y – if applicable
	Application Threat Modeling	Y – if applicable
	Security Configuration Compliance Data	Y – if applicable
	Security Control Assessment	Y – if applicable
Application hosted in FedRAMP cloud (VAEC)	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y – if applicable
	Application Security Testing	Y – if applicable
	Application Threat Modeling	Y – if applicable
	Security Configuration Compliance Data	Y – if applicable
	Security Control Assessment	Y – if applicable
Application hosted in FedRAMP cloud (Non-VAEC)	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y – if applicable
	Application Security Testing	Y – if applicable
	Application Threat Modeling	Y – if applicable
	Security Configuration Compliance Data	Y – if applicable
	Security Control Assessment	Y – if applicable

Facility	Nessus Scan	Y
	Database Scan	N
	Enterprise Discovery Scan	Y
	Penetration Test/Application Assessment	N
	Application Security Testing	N
	Application Threat Modeling	N
	Security Configuration Compliance Data	Y
	Security Control Assessment	Y – if applicable
Medical Devices	Nessus Scan	N
	Database Scan	N
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	N
	Application Security Testing	N
	Application Threat Modeling	N
	Security Configuration Compliance Data	N
	Security Control Assessment	Y – if applicable
Other Federal Agency (Non-eMASS Reciprocity)	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y – if applicable
	Application Security Testing	N
	Application Threat Modeling	N
	Security Configuration Compliance Data	Y – if applicable
	Security Control Assessment	Y – if applicable
Platforms	Nessus Scan	N
	Database Scan	N
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	N
	Application Security Testing	N
	Application Threat Modeling	N
	Security Configuration Compliance Data	N
	Security Control Assessment	Y – if applicable

8 Appendix D – Common Control Providers/System of Record (SOR)

VA Tier1 System of Record (VA T1 SOR), Infrastructure Operations System of Record (IO SOR), and VA Area SOR are common control providers identified as a System of Record (SOR) in the eMASS GRC. SORs are vehicles used to provide common assessment procedure inheritance to a collection of systems. SORs themselves are not actual systems; therefore, they are approved for use by an Authorizing Official, but not Authorized to Operate. Assessment procedures provided by an SOR are assessed in accordance with VA guidance. For additional information on inheritance, refer to the 'Management' section of the eMASS User Guide.

8.1.1.1 VA T1SOR

T1SOR is a common control provider in eMASS. T1SOR provides common assessment procedure inheritance for systems within the FISMA Inventory. T1SOR documents test results and test evidence for the assessment procedures that are implemented on an agency-wide basis as directed by OIS policy or other OIS organizations where the implementation applies at a Department level.

Process Providers include:

- VA Policy,
- Information Security Risk Management (ISRM),
- Software Assurance (SwA),
- Security Assessment and Vulnerability Division (SAVD), and
- Cybersecurity Operations Center (CSOC).

Applications on the Premier/VA Network, IO Platforms, and Facilities may choose to inherit from T1SOR. Although T1SOR is available for inheritance by the listed boundaries within eMASS, it is the responsibility of the requesting system to review each assessment procedure and determine if the T1SOR response appropriately describes the security controls in place for their system. As an example, the organization defined time periods cannot be made less stringent. There will be some CCIs that are hybrid, meaning the ISO can further define criteria (i.e., fields audited, devices inventoried, etc.). Depending on this outcome, System Stewards may choose to selectively inherit all or some of the CCIs provided for inheritance by T1SOR.

8.1.1.2 IO SOR

IO SOR is a common control provider in eMASS. IO SOR provides common assessment procedure inheritance for systems within the enterprise that utilize IO processes. IO SOR documents test results and test evidence for the assessment procedures that are implemented on an agency-wide basis by Infrastructure Operations.

IO Process Providers include:

- Business Office,
- Cybersecurity Management,
- Change Management,
- Network,
- Platform, and
- Unified Communications Infrastructure Support.

Applications on the Premier/VA Network, IO Platforms, and Facilities may choose to inherit from IO SOR. Although IO SOR is available for inheritance by the listed boundaries within eMASS, it is the responsibility of the requesting system to review each assessment procedure and determine if the IO SOR response appropriately describes the security controls in place for their system. Depending on this outcome, System Stewards may choose to selectively inherit all or some of the CCIs provided for inheritance by IO SOR.

8.1.1.3 VA Area SOR

VA Districts and Areas are organized into 5 Districts: North Atlantic, Southeast, Midwest, Continental, and Pacific. Within each district, sites such as Regional offices, medical centers, and cemeteries are organized and grouped by Area. The VA Area SOR addresses common processes that are utilized across all Areas.

VA Area SOR is a common control provider in eMASS. VA Area SOR provides common assessment procedure inheritance for VA Areas within the enterprise that utilize VA District Area processes. The VA Area SOR documents test results and test evidence for the assessment procedures implemented across all Areas within the VA.

At present, VA Area SOR includes common Area processes for Configuration Management; other security families will be examined for inclusion.

Areas may choose to inherit from VA Area SOR. Although VA Area SOR is available for inheritance by the listed boundaries within eMASS, it is the responsibility of the requesting system to review each assessment procedure and determine if the VA Area SOR response appropriately describes the security controls in place for their system. Depending on this outcome, System Stewards may choose to selectively inherit all or some of the CCIs provided for inheritance by VA Area SOR.

9 *Appendix E – New Authorizing Official (AO) Guidelines*

When an AO leaves the position or when a new AO starts, the systems under his/her purview require a review to continue the current ATO or grant a new ATO. The following steps should be used as guidance to ensure all systems receive an ATO review in a timely manner.

1. When an AO leaves or a new AO is recommended; the *Authorizing Official Appointments Memo* must be updated and signed by the CIO or PDAS prior to the new AO reviewing and providing risk decisions on any authorization packages.
2. The incoming AO to the authorization package will be required to review the package and determine if the system should continue with the current ATO or if a new full review, including a Risk Review, needs to be completed to provide a new ATO.
3. The new AO needs to use the eMASS RMF Step 5 workflow to show approval for the Authorization Boundary within 180 days of the previous AO leaving.