


## Addendum C – Authorization Requirements Quick Reference Guide

Authorization Requirements		
Requirement	Roles / Responsibilities	References
Technical/Testing Requirements		
<input type="checkbox"/> <b>Nessus Scan</b> <ul style="list-style-type: none"> <li>A <u>credentialed</u> vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws.</li> <li>Actual scan results must be provided for analysis.</li> <li>All Critical and High deficiencies should be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan.</li> <li>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 and should be documented.</li> <li>Refer to the Threat &amp; Vulnerability Manager (TVM) guidance material located on the OIS portal at <a href="#">Training and Brown Bag Materials</a> for detailed information on how to access TVM within RiskVision.</li> </ul>	<b>If the system's Nessus Scan data is currently displayed in TVM within RiskVision:</b> <ul style="list-style-type: none"> <li>Browse to <a href="#">Nessus Enterprise Web Tool (NEWT)</a> and use the Remediation Effort Entry Form (REEF) to document your manual remediation effort. For each deficiency identified from the scan, the System Owner or delegate 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.</li> <li>Once all manual remediation has been documented within REEF, run this report <a href="https://spsites.cdw.va.gov/sites/FODW_PVT/Progress%20Reports/Progress_ReportbyRegion_Chart.rdl">https://spsites.cdw.va.gov/sites/FODW_PVT/Progress%20Reports/Progress_ReportbyRegion_Chart.rdl</a> within NEWT.</li> <li>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.</li> <li>System Owner or delegate then uploads the report from step 3 above to the Documents tab within RiskVision. Mitigation information can also be provided in the Vulnerabilities tab within RiskVision.</li> <li>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.</li> </ul>	<ul style="list-style-type: none"> <li>Contact the Office of Cyber Security (OCS) at: <a href="mailto:CertificationPMO@va.gov">CertificationPMO@va.gov</a> with any questions.</li> <li>TVM guidance material located on the OIS portal at <a href="#">Training and Brown Bag Materials</a></li> </ul>

		<p>Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.</p> <p><b>If the system's Nessus Scan data is not currently displayed in TVM within RiskVision:</b></p> <ul style="list-style-type: none"> <li>• : If Nessus Scan data is not currently provided in TVM for the system and instead raw Nessus Scan results exist from NSOC, the System Owner or delegate shall upload the actual Nessus Scan results to the Documents tab in RiskVision; along with a mitigation strategy for each finding. Also, within NEWT, if the ISO/System Owner 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 accreditation boundary to add it to NEWT to pull the report.</li> <li>• <u>System Owner or delegate</u> creates one finding and a response in the Findings tab within RiskVision for the Nessus scan to serve as a reminder to resolve the deficiencies.</li> </ul>	
	<p><b>Quality Code Review</b></p> <ul style="list-style-type: none"> <li>• Quality code reviews of custom developed VA applications using the approved VA static code analysis tool should be conducted to identify code quality issues within VA applications.</li> <li>• Applications written in languages that are not supported, such as MUMPS, shall be targeted for manual review of testing with other applicable tools; notify the VA Software Assurance (SwA) Program Office if this is the case at: <a href="mailto:OISSwASupportGroup@va.gov">OISSwASupportGroup@va.gov</a>.</li> </ul>	<p><b>V&amp;V Quality Code Reviews</b></p> <ul style="list-style-type: none"> <li>• <u>VA Application Developers</u> open a NSD ticket [(855) NSD-HELP] to request VA static code analysis tools in order to perform scans according to the procedures in the VA Quality Code Review SOP and guidance materials.</li> <li>• <u>VA Application Developers</u> scan their own application source code.</li> <li>• <u>VA Application Developers</u> open a NSD ticket [(855) NSD-HELP] to request validation of a final V&amp;V quality code review.</li> <li>• <u>VA Application Developers</u> deliver the scan results to the VA SwA Program Office at: <a href="mailto:OISSwASupportGroup@va.gov">OISSwASupportGroup@va.gov</a> for review, work with the VA SwA Program Office to schedule the validation, and coordinate with them to resolve any issues identified during validation. <ul style="list-style-type: none"> <li>• The scan results are reviewed to ensure that minimum</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• For detailed instructions on the code reviews process, reference the VA Quality Code Review SOP and guidance materials, which are posted on the <a href="#">VA SwA Program Office Resource Site</a>.</li> </ul>

		<p>VA standards have been met. The VA SwA Program Office determines whether additional analysis is needed, and works with the VA Application Developers to ensure that they understand how to meet the standards required.</p> <ul style="list-style-type: none"> <li>• <u>System Owner or delegate</u> uploads full test results to the Documents tab in RiskVision.</li> <li>• <u>System Owner or delegate</u> creates a response for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated for each deficiency identified from the V&amp;V quality code review. Also, include the scheduled completion date and status of each deficiency. Information should be provided in Excel or Word format; refer to the OCS preferred template located on the OIS Portal at A&amp;A Home Documents. System Owner or delegate uploads the aforementioned document to the Documents tab in RiskVision.</li> <li>• <u>System Owner or delegate</u> creates one finding and a response in the Findings tab within RiskVision for the V&amp;V quality code review to serve as a reminder to resolve the deficiencies.</li> </ul>	
	<p><b>Secure Code Review</b></p> <ul style="list-style-type: none"> <li>• V&amp;V secure code reviews of custom developed VA applications must be conducted according to the VA Secure Code Review SOP located at</li> </ul> <p><a href="#">VA SwA Program Office Resource</a></p> <ul style="list-style-type: none"> <li>• V&amp;V secure code reviews are conducted by the VA Application Developers.</li> <li>• Applications written in languages that are not supported, such as MUMPS, shall be targeted for manual review or testing with other applicable tools (notify OCS if this is the case at: <a href="mailto:OISSwASupportGroup@va.gov">OISSwASupportGroup@va.gov</a>).</li> </ul>	<p><b>V&amp;V Secure Code Reviews</b></p> <ul style="list-style-type: none"> <li>• <u>VA Application Developers</u> open a NSD ticket [(855) NSD-HELP] to request VA static code analysis tools; they scan their own application source code; open a NSD ticket to request validation of a final V&amp;V secure code review; deliver the scan results to the VA SwA Program Office at <a href="mailto:OISSwASupportGroup@va.gov">OISSwASupportGroup@va.gov</a> for review; work with the VA SwA Program Office to schedule the validation; and coordinate with them to resolve any issues identified during validation.</li> <li>• <u>System Owner</u> or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the secure code review results to RiskVision under Entity Details: Documents tab.</li> <li>• <u>System Owner</u> or delegate creates one finding and a response in the Findings tab within RiskVision for the</li> </ul>	<ul style="list-style-type: none"> <li>• Contact the NSD Help Desk [(855) NSD-HELP] to request tools (Fortify), reviews, or technical support</li> </ul>

		secure code review to serve as a reminder to resolve the deficiencies.	
<input type="checkbox"/>	<b>Penetration Test/Application Assessment</b> <ul style="list-style-type: none"> <li>A full penetration test/application assessment must be performed that includes automated and manual assessment tools and techniques on Internet Facing and/or High Impact Systems.</li> <li>Actual test results must be provided for analysis.</li> <li>All Critical and High deficiencies should be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan.</li> </ul>	<ul style="list-style-type: none"> <li><u>System Owner or delegate</u> contacts CPO at <a href="mailto:CertificationPMO@va.gov">CertificationPMO@va.gov</a> to request penetration test/application assessment from NSOC.</li> <li><u>NSOC</u> conducts penetration test/application assessment and provides results to system POCs. Please allow 30 days for NSOC to schedule/conduct the penetration test/application assessment.</li> <li><u>System Owner</u> or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the test results to RiskVision under Entity Details: Documents tab.</li> <li><u>System Owner</u> or delegate creates one finding and a response in the Findings tab within RiskVision for the penetration test/application assessment to serve as a reminder to resolve the deficiencies.</li> </ul>	<ul style="list-style-type: none"> <li>Contact OCS at: <a href="mailto:CertificationPMO@va.gov">CertificationPMO@va.gov</a> with any questions</li> </ul>
<input type="checkbox"/>	<b>Security Control Assessment (SCA) (if applicable)</b> <ul style="list-style-type: none"> <li>An SCA will be required only upon request from OCS.</li> <li>If an SCA is required, all Critical and High POA&amp;Ms should be mitigated with documented mitigation evidence provided, and Moderate and Low POA&amp;Ms should be mitigated or have a documented mitigation plan.</li> </ul>	<ul style="list-style-type: none"> <li>Once notified by OCS that an SCA is required, the appropriate <u>audit team</u> will be notified by <u>OCS</u> to schedule the assessment.</li> <li>The assigned <u>audit team</u> will conduct the SCA.</li> <li><u>OCS</u> will create a SCA program for the appropriate entity in GRC that was audited.</li> <li>The <u>audit team lead</u> will upload the deliverables, to include the SCA report and import the POAMs, <u>within 4 weeks</u> of completion of the audit.</li> <li><u>System Owner or delegate</u> creates responses to the POAMs/findings within <u>15 days</u> of the POAMs uploaded.</li> </ul>	<ul style="list-style-type: none"> <li>Contact OCS at: <a href="mailto:CertificationPMO@va.gov">CertificationPMO@va.gov</a></li> </ul>
<input type="checkbox"/>	<b>Security Configuration Compliance Data</b> <ul style="list-style-type: none"> <li>Compliance data must be obtained for all IP addresses that make up a system and must check against VA approved hardening guidance for all Operating Systems, Databases, Networks, and Security Devices, where guidance exists.</li> </ul>	<b>For systems with IP address ranges internal to the VA that have the IBM Endpoint Manager (IEM) agent installed:</b> <ul style="list-style-type: none"> <li><u>System Owner or delegate</u> contacts CPO at <a href="mailto:CertificationPMO@va.gov">CertificationPMO@va.gov</a> to request compliance reports for the IP addresses that make up their system(s).</li> <li><u>System Owners/Administrators</u> should input IP address ranges for their system(s) by following the compliance scan 'Report' request process on the OIS Portal at</li> </ul>	<ul style="list-style-type: none"> <li>Contact OCS at: <a href="mailto:CertificationPMO@va.gov">CertificationPMO@va.gov</a> and NSOC, or the Enterprise Visibility Team at: <a href="mailto:OISEVSupportGroup@va.gov">OISEVSupportGroup@va.gov</a> with any questions</li> <li>Internal Compliance reports location:</li> </ul>



		<p><a href="#">Compliance Scan Report Request.</a></p> <ul style="list-style-type: none"> <li>• <a href="#">CPO</a> provides directions on how to retrieve the compliance reports for these systems. New compliance reports will be available daily as compliance configuration data changes. System Owners/Administrators will be required to go to this location:  <a href="http://dashboard.tic.va.gov/ibmcognos/cgi-bin/cognosisapi.dll">http://dashboard.tic.va.gov/ibmcognos/cgi-bin/cognosisapi.dll</a> to pull the compliance reports for their system(s). <ul style="list-style-type: none"> <li>• <a href="#">System Owner or delegate</a> uploads the Compliance Trending and Checklist Trending reports to the Documents tab in RiskVision. The Compliance Trending and Checklist Trending reports can be found at <a href="https://dashboard.tic.va.gov/s/28U/">https://dashboard.tic.va.gov/s/28U/</a> and <a href="https://dashboard.tic.va.gov/s/28T/">https://dashboard.tic.va.gov/s/28T/</a> respectively.</li> <li>• <a href="#">System Owner or Delegate</a> creates one finding and a response in the Findings tab within RiskVision for the compliance scan to serve as a reminder to resolve the deficiencies.</li> <li>• <a href="#">System Owner or Delegate</a> continues to remediate deficiencies identified from the Compliance Trending and Checklist Trending reports.</li> <li>• <a href="#">System Owner or Delegate</a> uploads new Compliance Trending and Checklist Trending reports to Documents tab within RiskVision as evidence to show the remediation progress.</li> </ul> </li> </ul> <p><b>For systems with IP address ranges external to the VA that do not have the IBM Endpoint Manager (IEM) agent installed:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">System Owners or delegate</a> must submit a 'Supplemental Scan Request' form found at <a href="#">A&amp;A Home Documents</a> to CPO at <a href="mailto:CertificationPMO@va.gov">CertificationPMO@va.gov</a>. Ensure that the 'Compliance' check box is checked.</li> <li>• <a href="#">CPO</a> will submit this form to the NSOC and an NSOC POC will contact the System Owner/Administrator to schedule the compliance scan.</li> <li>• <a href="#">NSOC</a> will submit compliance results/reports to system</li> </ul>	<p><a href="http://dashboard.tic.va.gov/ibmcognos/cgi-bin/cognosisapi.dll">http://dashboard.tic.va.gov/ibmcognos/cgi-bin/cognosisapi.dll</a></p> <ul style="list-style-type: none"> <li>• OCS preferred template location on the OIS Portal at <a href="#">A&amp;A Home Documents</a></li> <li>• Supplemental Scan Request form location <a href="#">A&amp;A Home Documents</a></li> </ul>
--	--	--	--

		<p>POCs for compliance scans that are conducted.</p> <ul style="list-style-type: none"> <li>• <u>System Owner or delegate</u> uploads the Compliance Trending and Checklist Trending reports to the Documents tab in RiskVision. The Compliance Trending and Checklist Trending reports can be found at <a href="https://dashboard.tic.va.gov/s/28U/">https://dashboard.tic.va.gov/s/28U/</a> and <a href="https://dashboard.tic.va.gov/s/28T/">https://dashboard.tic.va.gov/s/28T/</a> respectively.</li> <li>• <u>System Owner or Delegate</u> creates one finding and a response in the Findings tab within RiskVision for the compliance scan to serve as a reminder to resolve the deficiencies.</li> <li>• <u>System Owner or Delegate</u> continues to remediate deficiencies identified from the Compliance Trending and Checklist Trending reports.</li> <li>• <u>System Owner or Delegate</u> uploads new Compliance Trending and Checklist Trending reports to Documents tab within RiskVision as evidence to show the remediation progress.</li> </ul>	
Requirement		Roles / Responsibilities	References
Security Documentation Requirements			
<input type="checkbox"/>	<p><b>System Security Plan (SSP)</b></p> <ul style="list-style-type: none"> <li>• The SSP is developed within RiskVision.</li> <li>• All required diagrams and confirmation of the security authorization boundary to include all devices and supporting software architecture should be included.</li> <li>• All controls must be addressed. A finding will need to be created in RiskVision for every control that is not in place.</li> </ul>	<ul style="list-style-type: none"> <li>• <u>System Steward</u> completes the assessments in RiskVision and develops findings and responses in the <b>Findings</b> tab for controls not in place.</li> <li>• <u>ISO</u> validates information added by the System Steward in RiskVision.</li> <li>• <u>The ISO, System Owner or delegate/System Steward</u> exports the SSP from RiskVision and uploads the document to the Documents tab in RiskVision.</li> </ul>	<ul style="list-style-type: none"> <li>• NIST SP 800-18 and VA Handbook 6500.3</li> <li>• Additional guidance for completion of the SSP can be provided by OCS</li> </ul>
<input type="checkbox"/>	<p><b>Minor Application Self-Assessment</b></p> <ul style="list-style-type: none"> <li>• Minor Application Self-Assessment must be completed for all minor applications.</li> </ul>	<ul style="list-style-type: none"> <li>• <u>The ISO, Project team, and the SS</u>, working in conjunction should prepare the Minor Application Security Control Summary and provide implementation detail for all applicable security controls and upload the Self-Assessment to GSS/MA Documents repository in RiskVision.</li> </ul>	<ul style="list-style-type: none"> <li>• Minor Application Self Assessment SOP (<a href="#">Appendix D</a>)</li> </ul>

<input type="checkbox"/>	<b>Signatory Authority</b> <ul style="list-style-type: none"> <li>The Signatory Authority must be signed and dated by the appropriate parties.</li> </ul>	<ul style="list-style-type: none"> <li><u>System Owner or delegate</u> completes the Signatory Authority using the template provided at <a href="#">A&amp;A Home Documents</a> and uploads the Signatory Authority to RiskVision under Entity Details: Documents tab.</li> </ul>	<ul style="list-style-type: none"> <li>NIST SP 800-18</li> <li>Additional guidance for completion of the Signatory Authority can be provided by OCS</li> </ul>
<input type="checkbox"/>	<b>Risk Assessment (RA)</b> <ul style="list-style-type: none"> <li>The RA is developed within RiskVision.</li> </ul>	<ul style="list-style-type: none"> <li><u>System Steward</u> completes the assessments in RiskVision.</li> <li><u>ISO</u> validates information added by the System Steward in RiskVision.</li> <li>The <u>ISO, System Owner or delegate/System Steward</u> exports the RA from RiskVision and uploads the document to the Documents tab in RiskVision.</li> </ul>	<ul style="list-style-type: none"> <li>NIST SP 800-30</li> <li>Additional guidance for completion of the RA can be provided by the Office of Risk Management and Incident Reporting (RMIR)/OCS</li> </ul>
<input type="checkbox"/>	<b>Configuration Management Plan (CMP)</b> <ul style="list-style-type: none"> <li>The CMP should include processes for managing configuration and change management.</li> <li>The CMP should include infrastructure devices and baseline configurations (e.g., switches, routers, firewalls).</li> <li>The CMP should include a configuration file for each operating system(s), database(s), application(s), and network device(s) to validate compliance with baseline configuration.</li> </ul>	<ul style="list-style-type: none"> <li><u>System Owner or delegate</u> completes the CMP using the template provided at <a href="#">A&amp;A Home Documents</a> and uploads the CMP as evidence to RiskVision under Entity Details: Documents tab.</li> </ul>	<ul style="list-style-type: none"> <li>NIST SP 800-70 and VA Handbook 6500</li> <li>Additional guidance for completion of the CMP can be provided by OCS</li> </ul>
<input type="checkbox"/>	<b>Incident Response Plan (IRP)</b> <ul style="list-style-type: none"> <li>The IRP must be created using RA and SSP.</li> <li>The IRP must meet the following standards: <ul style="list-style-type: none"> <li>Information Access and Privacy Program</li> <li>NIST Special Publication 800-61 - Computer Security Incident Handling Guide</li> <li>VA Handbook 6500.3, Certification and Accreditation of Federal Information Systems</li> </ul> </li> <li>Each site is responsible for developing local level procedures incorporating VA-NSOC areas of responsibility.</li> </ul>	<ul style="list-style-type: none"> <li><u>System Owner</u> works with the assigned <u>ISO</u> to create the IRP.</li> <li><u>System Owner or designee</u> uploads the signed IRP into RiskVision once completed and tested.</li> </ul>	<ul style="list-style-type: none"> <li>NIST SP 800-61</li> <li>Useful tools and websites: <ul style="list-style-type: none"> <li><a href="#">Agilience RiskVision Enterprise Operations GRC Instance</a></li> <li><a href="#">Agilience RiskVision National Release GRC Instance</a></li> <li><a href="#">Office of Cyber Security (OCS) Portal</a></li> </ul> </li> </ul>
<input type="checkbox"/>	<b>Information Security Contingency Plan (ISCP)</b> <ul style="list-style-type: none"> <li>The ISCP must be created using following inputs: <ul style="list-style-type: none"> <li>Preliminary Information System Contingency Plan</li> <li>Primary Site System Security Plan</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><u>System Owner or delegate</u> develops or revises the Information System Contingency Plan.</li> <li><u>System Owner or designee</u> uploads the Information System Contingency Plan into RiskVision.</li> </ul>	<ul style="list-style-type: none"> <li>Additional guidance for completion of the ISCP can be provided by the OBC</li> <li>Useful tools and websites:</li> </ul>

	<ul style="list-style-type: none"> <li>• Backup Site System Security Plan</li> <li>• The ISCP must meet the following standards: <ul style="list-style-type: none"> <li>• NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems</li> <li>• Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures</li> <li>• VA Handbook 6500.8, Information System Contingency Planning</li> </ul> </li> </ul>		<ul style="list-style-type: none"> <li>• <a href="#">Agilience RiskVision Enterprise Operations GRC Instance</a></li> <li>• <a href="#">Agilience RiskVision National Release GRC Instance</a></li> <li>• <a href="#">Business Continuity Portal</a></li> <li>• <a href="#">Office of Cyber Security (OCS) Portal</a></li> <li>• <a href="#">Technical Services Project Repository (TSPR)</a></li> </ul>
<input type="checkbox"/>	<p><b>Disaster Recovery Plan (DRP)</b></p> <ul style="list-style-type: none"> <li>• The DRP must be created using following inputs: <ul style="list-style-type: none"> <li>• Primary Site System Security Plan</li> <li>• Backup Site System Security Plan</li> </ul> </li> <li>• The DRP must meet the following standards: <ul style="list-style-type: none"> <li>• Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <u>System Owner or designee</u> develops the DRP as the entry point for the creation of both the facility and data center plans.</li> <li>• <u>System Owner or designee</u> uploads the DRP into RiskVision once completed and tested.</li> </ul>	<ul style="list-style-type: none"> <li>• Additional guidance for completion of the ISCP can be provided by the OBC</li> <li>• Useful tools and websites: <ul style="list-style-type: none"> <li>• <a href="#">Agilience RiskVision Enterprise Operations GRC Instance</a></li> <li>• <a href="#">Agilience RiskVision National Release GRC Instance</a></li> <li>• <a href="#">Business Continuity Portal</a></li> <li>• <a href="#">Office of Cyber Security (OCS) Portal</a></li> </ul> </li> </ul>



	<p><b>Privacy Impact Assessment (PIA)</b></p> <ul style="list-style-type: none"> <li>• A complete PIA must have: <ul style="list-style-type: none"> <li>• A previously completed Privacy Threshold Analysis (PTA). <ul style="list-style-type: none"> <li>• Been completed in the most up-to-date and Privacy Services approved template for both the PTA and PIA. The PTA and PIA template can be found at <a href="#">A&amp;A Home Documents</a></li> </ul> </li> <li>• Been completed in coordination with the VA Privacy Services Office.</li> <li>• Been signed by the System Owner, Privacy Officer, and ISO.</li> <li>• Been re-submitted whenever there are major changes to the system or within 3 years.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <u>System Owner, Privacy Officer, and ISO</u> work together to submit a PTA, which is reviewed by the Privacy Services Office. After review and determination by analysts, the PTA must be signed by the System Owner, Privacy Officer, ISO, and any other relevant stakeholders and re-submitted to the Privacy Services Office via <a href="mailto:PIASupport@va.gov">PIASupport@va.gov</a>. If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed and submitted to the Privacy Services Office and then comments by the analysts, if any, must be incorporated.</li> <li>• <u>Privacy Services</u> verifies PIA and provides results.</li> <li>• <u>System Owner or delegate</u> re-submits the PIA as a PDF file with the signatures of the System Owner, Privacy Officer, ISO, and any other relevant stakeholders to <a href="mailto:PIASupport@va.gov">PIASupport@va.gov</a>.</li> <li>• <u>System Owner or delegate</u> uploads the PIA to RiskVision under Entity Details: Documents tab.</li> </ul>	<ul style="list-style-type: none"> <li>• Authority is found in E-Government Act of 2002, OMB Circular 03-22, VA Directive 6502, VA Directive 6508, and VA Handbook 6508.1</li> <li>• Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to <a href="mailto:PIASupport@va.gov">PIASupport@va.gov</a></li> </ul>
	<p><b>Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU)</b></p> <ul style="list-style-type: none"> <li>• An ISA/MOU must be provided for all external interconnections.</li> </ul>	<ul style="list-style-type: none"> <li>• <u>System Owner</u> in coordination with the entities identified in NIST SP 800-47 will complete the ISA/MOU using the latest template provided at: OIS Portal or A&amp;A Home Documents.</li> <li>• <u>ISO</u> will upload all final draft MOU/ISA documents to the MOU/ISA Review Submissions SharePoint site for a review prior to requesting signatures.</li> <li>• <u>VA review team</u> will assess the documents against a checklist for quality and content.</li> <li>• <u>Reviewer and the ISO</u> will work collaboratively to correct deficiencies found in the documentation.</li> <li>• <u>Reviewer</u> will notify the ISO via email informing them that the document is ready for signatures.</li> <li>• <u>ISO</u> will process the document for signature.</li> <li>• <u>ISO</u> will upload the document to the Enterprise Document SharePoint upon receipt of the completed and signed MOU/ISA document,.</li> <li>• The finalized document should also be added to the existing A&amp;A artifacts in RiskVision.</li> </ul>	<ul style="list-style-type: none"> <li>• NIST SP 800-47, VA Handbook 6500, and <a href="#">FSS Bulletin#269</a></li> <li>• Additional guidance can be provided by the Health Information Security Division at <a href="mailto:vafsshisd@va.gov">vafsshisd@va.gov</a> or the OIT ERM CRISP Team at <a href="mailto:Sharon.mcallister@va.gov">Sharon.mcallister@va.gov</a></li> </ul>