#	Responsibility	Designee	Completed?	
1.	Develop in RiskVision: - SSP - Risk Assessment - Configuration Management Plan (CMP) - Incident Response Plan (IRP) - Information System Contingency Plan (ISCP) - Disaster Recovery Plan (DRP) - Privacy Impact Assessment (PIA) - Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU).	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
2.	Review and update the SSP as required by OCS and when a significant change to the system occurs.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
3.	Review, update and test the system contingency plan as specified in the SSP and when a significant change to the system occurs.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
4.	Ensure risk assessments are accomplished per the SSP, regularly reviewed/updated, and when there is a major change to the system, reviewed and updated as required.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
5.	Conduct PIA with the assistance of the PO, as required.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
6.	Develop and maintain an IT system Configuration, Change, and Release Management Plan.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
7.	Ensure that technical testing is coordinated with the appropriate organizational entities and completed as scheduled (i.e., Nessus scans, secure code reviews, penetration test/application assessments, security control assessments (SCA), and security configuration compliance data).	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
8.	Ensure each system has developed a secure baseline of security controls by scoping, tailoring, compensating, and supplementing the controls as outlined in the VA Handbook 6500.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
9.	Ensure each system secure baseline configuration outlined above is documented in	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

	the SSP and approved by the VA CIO (as the AO) or designee prior to implementation.			
10.	Provide appropriate access to VA systems (including types of privileges or access), in coordination with VA managers and ISOs.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
11.	Ensure the development and maintenance of SSPs and contingency plans are in coordination with local information owners, the local system administrators, ISO, and functional "end user" for nationally deployed systems.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
12.	Ensure system users and support personnel receive required security training.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
13.	Assist the local system administrators in the identification, implementation, and assessment of security controls.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
14.	Ensure the information system receives authorization prior to operational deployment, is reauthorized when a significant change in the system or a major change in the data occurs, and is continuously monitored.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
15.	Assist other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the plan of action and milestones (POA&M) and updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
16.	Ensure continuous monitoring activities are performed.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
17.	Notify the responsible VA ISO, PO, VA Network Security Operations Center (VA-NSOC) and the OIG as appropriate per VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), of any suspected incidents immediately upon identifying that an incident has occurred and	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

	assisting in the investigation of incidents, as necessary.			
18.	Ensure compliance with the Enterprise and Security Architecture throughout the system life cycle.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
19.	Charter, organize, and maintain VA's Patch and Vulnerability Team (PVT) Program.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
20.	Collaborate with VA Identity Safety Service to monitor for identity theft, when appropriate.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
21.	Nominate a COR for all contracts impacted by this directive and ensuring CORs complete the required COR training.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
22.	Ensure security requirements and security specifications are explicitly included in VA contracts, as appropriate.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
23.	Work with the ISO and PO to ensure contracts contain the required security language necessary for compliance with FISMA and 38 U.S.C. 5721-5728 and to provide adequate security for information and information systems used by the contractor, including the requirement for signing the VA Contractor ROB.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
24.	Ensure contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
25.	Ensure contractors complete VA's security and privacy awareness training and any additional role-based training, as outlined in the contract.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
26.	Monitor the contract to ensure that security requirements are met, consulting the ISO and PO as necessary.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
27.	Ensure compliance with Federal security requirements and VA security policies.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

28.	Participate in self-assessments, external and internal audits of system safeguards and program elements, including A&A of the system.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
29.	Evaluate proposed technical security controls to assure proper integration with other system operations.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
30.	Identify requirements for resources needed to effectively implement technical security controls.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
31.	Ensure the integrity in implementation and operational effectiveness of technical security controls by conducting technical control testing.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
32.	Serve as owner for all local systems (e.g., tenant systems, guest networks) for which he/she is assigned, establishing standards (based on Federal requirements and VA security policies) for operating the systems within a VA facility, and removing non-compliant systems from use at the VA facility.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
33.	Periodically repeat selected test procedures from the system's security authorization to ensure the security controls continue to operate effectively at the proper levels of assurance per NIST guidance and over the life cycle of the system.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
34.	Assist other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M; updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
35.	Collaborate with VA Identity Safety Service to provide training on identity theft and fraud prevention and mitigation and to assist in the prevention and mitigation of potential identity theft and fraud.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

36.	Consult with the AO or designee, the local CIO and ISO when establishing or changing system boundaries. Additional guidance regarding the determination of system boundaries is outlined in NIST SP 800-37 and should be used if there are questions regarding a system's boundary.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
37.	In coordination with Information Owners and the ISO, categorize information systems as low-, moderate-, or high-impact for the security objectives of confidentiality, integrity, and availability.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
38.	Continue with VA's Risk Management Framework by: (1) selecting the initial baseline of security controls, (2) tailoring the initial baseline of security controls, and (3) supplementing the baseline controls as outlined in VA Handbook 6500.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
39.	Implement and test the security controls specified in the approved SSP.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
40.	Implement the VA-approved U.S. Government Configuration Baseline (USGCB) controls, formerly known as the Federal Desktop Core Configuration (FDCC), or Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG).	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
41.	Ensure assessors have access to the information system and environment of operation where the security controls are employed, and the appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
42.	Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated controls, as appropriate.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
43.	Prepare the POA&M based on the findings and recommendations of various security	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

	assessment reports excluding any remediation actions taken.			
44.	Assemble the security authorization package and submits the package to the AO for adjudication.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
45.	Follow the security authorization process defined in VA Handbook 6500.3.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
46.	Determine the security impact of proposed or actual changes to the information system and its environment of operation.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
47.	Conducts remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
48.	Update the SSP, security assessment report, and POA&M based on the results of the continuous monitoring process.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
49.	Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate VA officials on an ongoing basis in accordance with the monitoring strategy.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
50.	Follow VA Handbook 6500.1, Electronic Media Sanitization requirements when a system is removed from service.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
51.	Follow additional information regarding continuous monitoring in VA Handbook 6500.3.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
52.	Implement and follow additional System Owner/Steward responsibilities as outlined in the VA Handbook 6500's security control details.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

The list of System Owner responsibilities is subject to change as federal and VA security policies, standards and guidance are modified.