OVL Cyber Team Roles and Responsibilities

FUNCTION	TITLE	ROLE	RESPONSIBILITIES (AO DEFINED)
System Owners	Program Executive Officer (PEO)	Senior Acquisition Official	Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system/Capability.
	Information System Owner (ISO)	System Operational Owner	Primarily responsible for managing system development, operations, and maintenance at the program level. As part of these responsibilities, ISO must work with AOs, ISSMs, ISSEs, and PMs to ensure compliance for the systems which they own.
Assess & Authorize	Authorizing Official (AO)	Authorizing Official	Formally assumes responsibility for operating a system at an acceptable level of risk. Responsible for assessing and determining the Risk of Use for the system or capability and informing the stakeholders. The AO is responsible for authorizing or denying the operation (or the testing) of the information system by issuing an authorizing determination. The AO reviews the security authorization package, including supporting evidence and the recommendation of the CRA as a basis for determining risk.
	Authorizing Official Designated Representative (AODR)	AO Designated Representative	As defined by the AO, Acts on behalf of the authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process.
	Cyber Risk Assessors (CRA)	Independent Risk Assessor	Provides the AO, an independent (of the program) risk assessment of assigned systems, and an authorization recommendation to the AO.
Acquisition Program	Information System Security Manager (ISSM)	Program/ Cyber Lead	Primarily responsible for maintaining the overall security posture of the systems within their organization and are accountable for the implementation. The organization's Cybersecurity program is developed by ISSMs that includes Cybersecurity architecture, requirements, objectives and policies, Cybersecurity personnel, and Cybersecurity processes and procedures. ISSMs are also in charge of the continuous monitoring of systems within their purview to ensure compliance with Cybersecurity policies.
	Program Manager (PM)	Program Manager	The official responsible for and authority to accomplish program or system objectives for development, production and sustainment to meet the user's operational needs. Additionally, the PM serves as the focal point for the integration of cybersecurity into and throughout the system life cycle of an assigned IS and PIT system.

OVL Cyber Team Taskings

*Supporting Role

Role	Task
Authorizing Official	• Provides Assessment Criteria input and reviews the plan to assess the security requirements. • Final authorization determination • Review the reported security status of the IS (including the effectiveness of security requirements employed within and inherited by the IS) on an ongoing basis and in accordance with the continuous monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.
AODR	• Duties as assigned.
Information System Owner	• Categorize the information system and document the results in the AO Determination Brief. • Describe the information system (including system boundary) and document the description in the AO Determination Brief. • Register the IS with the appropriate organizational program management offices. • Assign qualified personnel to the OVL roles • Identify the security requirements provided by the organization as common requirements for organizational IS and document the requirements in the AO Determination Brief. • Select the security requirements for the IS (i.e., baseline, overlays, tailoring) and document the requirements in the AO Determination Brief. • Develop a system-level continuous monitoring strategy • Apply Overlays and tailor • Implement the security requirements specified in the AO Determination Brief. • Document the implementation as appropriate in the AO Determination Brief, providing a functional description of the implementation. • Conduct initial remedial actions based on findings and reassess remediated risk(s) as appropriate. • Prepare the Plan of Action and Milestones (POA&M) based on the findings and recommendations from the SAR, include any remediation actions taken. • Assemble and submit the Security Authorization Package (SAP) to the CRA. References are not part of the Security Authorization Package but must documented and made available. • Determine the security impact of proposed or actual changes to the IS and its environment of operation. • Conduct remediation actions based on the results of ongoing monitoring activities, assessment or risk, and outstanding items in the POA&M. • Update AO Determination Brief, SAR, and POA&M based on the results of the continuous monitoring process. • Report the security status of the IS (including the effectiveness of security requirements employed within and inherited by the IS) to the AO and other appropriate organizational officials on an ongoing basis and in accordance with the continuous monitoring strategy. • Implement an IS Decommissioning Strategy when needed which executes required actions when a system is removed from service.

OVL Cyber Team Taskings

Role	Task
PM/SM	• Register the IS with the appropriate organizational program management offices. • Assign qualified personnel to the OVL roles • Select the security requirements for the IS (i.e., baseline, overlays, tailoring) and document the requirements in the AO Determination Brief.* • Develop a system-level continuous monitoring strategy* • Apply Overlays and tailor* • Implement the security requirements specified in the AO Determination Brief.* • Document the implementation as appropriate in the AO Determination Brief, providing a functional description of the implementation.* • Prepare the Plan of Action and Milestones (POA&M) based on the findings and recommendations from the SAR, include any remediation actions taken. • Update AO Determination Brief, SAR, and POA&M based on the results of the continuous monitoring process.* • Implement an IS Decommissioning Strategy when needed which executes required actions when a system is removed from service.*
Cyber Risk Assessor	• Identify the security requirements provided by the organization as common requirements for organizational IS and document the requirements in the AO Determination Brief. • Develop a system-level continuous monitoring strategy* • Review the AO Determination Brief and Continuous Monitoring Strategy.* • Determine Assessment Criteria, develop, review, and create a plan to assess the security requirements.* • Assess the security requirements in accordance with the assessment procedures defined in the Security Assessment Plan. • Prepare the Security Assessment Report (SAR) • Conduct initial remedial actions based on findings and reassess remediated risk(s) as appropriate. • Assemble and submit the Security Authorization Package (SAP) to the AO. References are not part of the Security Authorization Package but must documented and made available.* • Assess a selected subset of security requirements employed within and inherited by the IS in accordance with the organization-defined monitoring strategy.

OVL Cyber Team Taskings

Role	Task
Information System Security Manager	• Identify the security requirements provided by the organization as common requirements for organizational IS and document the requirements in the AO Determination Brief. • Document the AO Determination Brief and Continuous Monitoring Strategy.* • Document the implementation as appropriate in the AO Determination Brief, providing a functional description of the implementation.* • Conduct initial remedial actions based on findings and reassess remediated risk(s) as appropriate.* • Prepare the Plan of Action and Milestones (POA&M) based on the findings and recommendations from the SAR, include any remediation actions taken.* • Assemble and submit the Security Authorization Package (SAP) to the CRA. References are not part of the Security Authorization Package but must documented and made available. • Assess a selected subset of security requirements employed within and inherited by the IS in accordance with the organization-defined monitoring strategy.* • Conduct remediation actions based on the results of ongoing monitoring activities, assessment or risk, and outstanding items in the POA&M.* • Update AO Determination Brief, SAR, and POA&M based on the results of the continuous monitoring process.* • Report the security status of the IS (including the effectiveness of security requirements employed within and inherited by the IS) to the AO and other appropriate organizational officials on an ongoing basis and in accordance with the continuous monitoring strategy.
Information Systems Security Engineer	• Identify the security requirements provided by the organization as common requirements for organizational IS and document the requirements in the AO Determination Brief. • Select the security requirements for the IS (i.e., baseline, overlays, tailoring) and document the requirements in the SSP. • Develop a system-level continuous monitoring strategy* • Apply Overlays and tailor* • Implement the security requirements specified in the AO Determination Brief.* • Document the implementation as appropriate in the AO Determination Brief, providing a functional description of the implementation.* • Determine the security impact of proposed or actual changes to the IS and its environment of operation.*