Development, Security, and Operations (DevSecOps) Application Lifecycle Management (ALM) Tools Usage Policy for Agency Software Development

The NRC has completed the implementation of various ALM tools within the DevSecOps pipeline. The Office of the Chief Information Officer (OCIO) ensures that the usage of the agency's approved ALM tools and processes are instituted with a policy that provides consistent usage and standards for the Continuous Integration (CI) and Continuous Delivery (CD) throughout agency's system/application lifecycle. NRC DevSecOps pipeline also includes system and application development, testing, production, and monitoring phases, and is designed to support and further develop the agency's adoption of agile-based software development practices. The paragraphs below provide a high-level description of policy, concepts, processes, requirements, and tools surrounding NRC's ALM capabilities and DevSecOps methodologies.

There are two methods for developing software at the NRC:

1. Developing an application off-site on vendor provided infrastructure, or
2. Developing an application on-site in the Enterprise Development and Test Environment (EDTE).

Either scenario requires application's source code to be **maintained** in a repository in the agency's Source Control Management (SCM) solution and tool. Also, there must be a defined compile/build process for each software component in the SCM repository and CI tool. This practice:

- Ensures that the software component's source code is continuously validated in the respective project repositories.
- Facilitates and ensures traceability to determine what approved software component source code is running in the Production Operating Environment (POE).
- Identifies enhancements in development or bugs to be fixed.
- Supports and promotes the adoption of agile-based software development concepts as well as the agency's DevSecOps methodology.
- Ensures source code vulnerability analysis has been completed at specified intervals.

Once the application development team onboards their compile/build processes into the agency's SCM tool, the NRC's ALM team will orchestrate the specific automated deployment processes required by each application in order to deploy required artifacts across the pre-production and production environments using the current approved CD tool.

Additionally, NRC requires developers to utilize approved security and functional testing tools early and throughout the development process to assist in minimizing security vulnerabilities, thereby avoiding delays at the end of the development process. The use of these tools also orchestrates functional and performance testing for all applications across NRC's enterprise.

System/Application Deployments:

To deploy the application artifacts from the compile/build onto any NRC production system, the following requirements and artifacts are necessary:

1. A clean security code analysis report, and static/dynamic application security scan or test result.
2. A set of release notes providing all relevant information regarding enhancements and bugs being deployed.
3. A test and rollback plan.

The artifacts are required as part of any change request submission to the Change Control Board (CCB) so the CCB members can make educated decisions on approvals of the changes to be deployed into the production environment.

NRC DevSecOps Tools:

The following are brief descriptions of the type of functions supported by various industry leading tools the agency has adopted to support the ALM process. They will help ensure the delivery of quality work products and services in support of NRC mission requirements for application software development:

Change Management

The agency has deployed an official tool used for issue tracking and overall project management functions. The tool dashboard act as the user's central dashboard for tracking all activities in their project. Each team has an initial choice of using three standard workflows (Simple, Standard and Complex) that can be customized for specific needs or business processes. There is traceability to source control and software builds to identify what code changes were made for each issue, bug, or improvement. All application technical documentation must be stored in the agency's approved application technical documentation repository.

Collaboration

The agency provides a tool for ALM workspaces where project teams share knowledge and collaborate on projects. It allows project teams to create, capture, and collaborate on any project or idea and provides visibility into institutional knowledge and access to the information needed.

SCM

The agency provides an official source code repository tool. All production source code must be actively updated in these repositories as software is being developed and released to production. The SCM system is Git-based, the most widely used standard for source control management. It also provides a Git client that allows users to push and clone source control

repositories to developers' workstations. Additionally, the tool provides issue, commit, and build traceability to the other agency ALM tools.

Build Management/CI

The agency provides an official build management/CI tool used to orchestrate software builds and releases across the agency's environment lifecycle. The tool organizes the development team's source code builds into plans and orchestrates source code builds, automated testing, and deployments from a single console.

Automated Deployment/CD

The agency provides an official automated deployment/CD tool that orchestrates the deployment of software release artifacts across the agency's environment lifecycle. The software release lifecycle is dev (EDTE), test, User Acceptance Testing (UAT)/Pre-production (pre-prod), then production (prod). Each application is broken up into components and delivered incrementally through the lifecycle.

Automated Testing

The agency deployed automated testing tools used to orchestrate functional and performance testing for all applications across the agency. A browser automation tool is provided that allows the user to record specific functional tests for web applications. A desktop tool is provided that can be configured to test web applications for performance based on usage. A studio desktop application tool is also provided that can test desktop, web, and mobile applications. These tools integrate with build management/CI tools to allow for traceability across the entire suite of agency ALM tools.

Automated Provisioning and Configuration Management

The agency provides an automated provisioning and configuration management tool for cloud governance. The tool is used to implement Infrastructure as Code & Compliance as Code to standardize the application server configuration across all environments. It also orchestrates middleware installations and configuration upon instance creation in a cloud-based environment.

Dynamic Web Application Security Testing

The agency provides an automated, yet fully configurable, dynamic application security testing tool that enables users to scan websites, web applications, and web services, to identify security vulnerabilities and application flaws. The tool can scan all types of web applications, regardless of the platform or the language with which they are built.