1.0 PROJECT TITLE:

Prototype DevSecOps pipelines

2.0 SUMMARY:

Our work within certain security contexts requires diligent enforcement and guarantees of system behavior and accessibility. A robust Development / Security / Operations (DevSecOps) pipeline that incorporates static code analysis, vulnerability scanning, code quality assessment, test coverage, and dependency tracking is needed to enable the accreditation process for deploying our software to operational field sites. This work will investigate the best tools to use for this DevSecOps pipeline and integrate them together for a working sequence that takes code from check-in to vetted deliverable.

3.0 BACKGROUND:

MIT Lincoln Laboratory (MIT-LL) is helping our sponsors realize their vision of an Open Architecture information infrastructure that reaches across all levels of its data enterprise. In this context, an open architecture has many benefits. It allows for rapid deployment of capabilities vs. large infrequent software upgrades; it reduces costs due to leveraging of open source software components, and it lowers barrier to entry, which empowers non-traditional contractors to provide best-of-breed solutions. To achieve this, we must be able to quickly deploy prototypes to enlisted end-users to obtain feedback and iterate on our designs. This, in turn, requires that we have a solid foundation for our software development, security, and deployment process.

MIT Lincoln Laboratory builds and deploys software systems, also known as software testbeds, to sites in support of program-based events and demonstrations. These software systems are designed for use in secure environments, and must conform to strict configuration requirements. Our goal is to streamline the process for vetting our code and system configurations so that developers can focus on writing application code.