Component: NAVY

Title: Automated Configuration Deployment and Auditing

Acquisition Program: PEO-IWS5: Surface ASW Combat System Integration, Surface ASW System Improvement

ITAR: The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 3.5 of the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop an architecture that automates capabilities within Naval Control Systems (NCS) to minimize operator-associated cybersecurity vulnerabilities and streamline rapid fielding of modular capability updates.

DESCRIPTION: Naval Control Systems (NCSs) are comprised of a complex combination of hardware systems, operating systems, and software elements. The installation and configuration of the tactical software, to include operating system, middleware, and applications, is currently a time-consuming, operator-intensive, and error-prone process. Current commercially available solutions do not meet the standards necessary. The Navy needs an innovative process to automate installation, configuration, application deployment, auditing, and reporting of system status within a complex NCS. This process will need to align with the Navy’s desire to deploy incremental capability improvements to ships at sea in a manner that maintains secure cyberspace posture and weapons safety. It is envisioned that the solution will include software and an architectural construct.

The current operator-intensive installation process can result in the introduction of cybersecurity vulnerabilities or misconfigurations that affect the performance and effectiveness of the NCS due to inadvertent operator error or the reduction of security controls during the execution of administrative tasks associated with installation. The possibility of operator error also introduces configuration uncertainty. This configuration uncertainty prohibits rapid introduction of modular capability updates.

Industry has demonstrated significant productivity improvements by migrating to automated tools such as Ansible [Ref. 1] to reduce complexity and enable DevOps initiatives. However, industry tools do not account for the rigor associated with weapons safety, with which the Navy must be concerned. Automated tools reduce the cybersecurity vulnerabilities associated with operator-intensive installation processes.

The desired innovation will be able to completely install and configure a tactical capability from a ‘bare-metal’ state while providing objective quality evidence (OQE) of the installation and periodic auditing of the configuration after installation. The desired innovation will utilize existing Navy-specified system and sub-system components to provide a fully functional operational capability with minimal operator involvement in an automated and repeatable process. The innovation desired should also demonstrate the capability to ingest a modular update to the NCS to allow agile deployment of capability improvements and bug fixes.

The correctness of the automated software deployment and auditing will be measured by objective assessment of proper operating systems configuration, configuration of software applications, and proper allocation of network device operating systems and configurations. By taking an ‘infrastructure as code’ approach [Refs. 2-5], the desired innovation will ensure the installed configuration is properly version controlled. The automated approach will reduce the need for operator-intensive interaction during installation and configuration, ensuring a repeatable process and reducing the opportunity to introduce cybersecurity vulnerabilities or misconfiguration.
The automated system will produce a logged record of the installation and therefore provide OQE of the installation results and auditing and reporting of current system configuration to permit identification of configuration drift. This will reduce costs associated with maintenance, manning, and operations associated with configuration management and cybersecurity.

The initial Naval Control System transition for this technology will be the AN/SQQ-89 Anti-Submarine Warfare Combat System Element, which fields with different Combat Systems on Cruisers, Destroyers, Frigates, and the Littoral Combat Ships. Testing of the automated system will take place under the cognizance of the Navy at the AN/SQQ-89 Prime Integrator site, currently LM RMS at Manassas, VA.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. Owned and Operated with no Foreign Influence as defined by DOD 5220.22-M, National Industrial Security Program Operating Manual, unless acceptable mitigating procedures can and have been be implemented and approved by the Defense Security Service (DSS). The selected contractor and/or subcontractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances, in order to perform on advanced phases of this contract as set forth by DSS and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material IAW DoD 5220.22-M during the advance phases of this contract.

PHASE I: Define and develop a concept for innovative software and its associated architecture that will enable the automated installation and configuration of all components of an example NCS. Demonstrate the feasibility of the concept in meeting the parameters in the Description by modeling and simulation or analysis. The Phase I Option, if exercised, will include the initial design specifications and capabilities description to build the prototype in Phase II.

PHASE II: Develop and deliver a prototype of the software and its architecture for automated installation and configuration of NCS capabilities. Demonstrate the prototype performance through the required range of desired performance attributes given in the Description. Testing and demonstration will occur at a Government-specified facility. It is probable that the work under this effort will be classified under Phase II (see Description section for details).

PHASE III DUAL-USE APPLICATIONS: Assist the Navy in transitioning the technology to Navy use. The prototype will provide support for Navy specified NCSs and the associated system engineering activities of the program.

The architecture developed has a high potential for dual use in systems that require a repeatable, automated installation and configuration process to reduce the introduction of potential cybersecurity vulnerabilities and misconfiguration in complex, critical systems, such as municipal infrastructure for power (nuclear, electrical) and connectivity. Automated installation and configuration that creates ‘infrastructure as code’ is of high interest to companies like Amazon and Google.

REFERENCES:
1. "Ansible is IT Automation." Ansible, 12 December 2018. ansible.com
4. "HashiCorp Packer." HashiCorp, 12 December 2018. packer.io
5. "HashiCorp Terraform." HashiCorp, 12 December 2018. terraform.io

KEYWORDS: Cybersecurity; Automated Software Deployment and Auditing; Agile Deployment; Naval Control Systems; Combat Systems; DevOps