Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

NAVSEA #2020-0476

Topic # N171-050

Software-based Modular and Extensible Cybersecurity Framework for Combat Systems

Real-Time Innovations

WHO

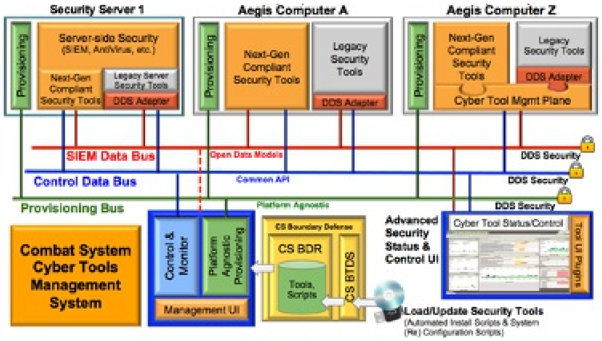
SYSCOM: NAVSEA

Sponsoring Program: AEGIS - IWS 1.0

Transition Target: AEGIS - IWS 1.0

TPOC:
(202)781-5326

Other transition opportunities: All DoD systems that are currently hampered by cyber tool vendor lock. Our TRL-9 based solution adopts an open system architecture and open data models ensuring Navy/DoD ownership of the interfaces, facilitating future extensibility. The transition value will increase with the scale/size of the target system.



Cyber Framework Architecture Overview, Real-Time Innovations

Notes: Our project centers around data models, provisioning, and adapters for various cyber tools identified by the Navy and LMCO as applicable to the target system. The data and control for these components will be carried by DDS. DDS is a mature, open standard and our implementation is a TRL-9 product already in use by the Navy, other DoD entities, and commercial industry.

WHEN

Contract Number: N68335-19-C-0290 **Ending on:** April 1, 2022

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Integration into Land-based Test System	Low	The successful integration, testing, and evaluation of the framework into a land-based test system.	6	April 2021
Integration into target DoD System	Low	Deploy the framework into the target DoD system and evaluate success metrics.	7	April 2022

WHAT

Operational Need and Improvement: U.S. Navy Combat Systems employ cybersecurity capabilities that detect, prevent and react to cyber threats in todays cyber environment. Two common challenges associated with these capabilities are 1) the complicated and unique interfaces they use, and 2) the need to update capabilities frequently to maintain their effectiveness against threats. A framework that could provide a simple and consolidated interface and the ability to update with little or no impact to the combat system will help ensure a more effective Defense-in-Depth cybersecurity solution. Most of these capabilities offer vendor-specific (known as vendor-lock) client-server architectures that assume computing environments with synchronous update cycles under a single programmatic authority. Such solutions present challenges. Adoption of vendor-specific technologies typically locks the combat system into the expertise and capabilities of that single vendor or solution, making it challenging to leverage the unique strengths of various companies across different domains.

Specifications Required: The approach shall be modular with the ability to update with little or no impact to the combat system performance. It should have a simple and consolidated interface. To prevent vendor-lock it should be a communication standard solution to allow plug-and-play of new capabilities in the framework.

Technology Developed: While cyber tool vendors are paying lip service to vendor interoperability, there is no concerted effort to actually realize this. By leveraging RTI’s commercially mature, standards-based communications technology, already deployed within the entire combat fleet, we are able to quickly develop and deploy an openly extensible, scalable, and secure solution at very low cost.

Our approach builds out common, openly extensible application programming interfaces (APIs) and data models that will enable cyber tool interoperability across product versions and vendors. This breaks vendor lock. While we encourage direct vendor support of these APIs, our agile approach can be easily integrated and used with both binary executable products and open source cyber tool solutions.

Our architecture facilitates loose coupling – new upstream and downstream tools can be added during system operation. Cyber tools can be readily deployed, tested, and verified before previous versions are removed. Our solution is platform and operating system agnostic.

HOW

Projected Business Model: We intend to standardize the approach and data model for cyber communication. The approach uses the Data Distribution Service (DDS) standard. We are the largest producer of a framework based on this standard, though alternatives exist that are commercially available or open. Any revenue would be increased license sales of Connext Pro (our implementation of the DDS framework).

Company Objectives: As systems become more interconnected, they become more difficult to extend, adapt, and engineer if they remain tightly coupled. DDS removes the tight coupling of distributed systems, making them more component oriented. Our implementing of DDS is the most widely used as we consistently provided top tier support to development teams, provide the most feature rich DDS software development kit (SDK), and our implementation is extremely performant.

Potential Commercial Applications: Any distributed system or IT environment that has a cyber tool infrastructure, which is to say nearly all of them, would benefit from an open cyber tool communication framework. We intend to provide such a standard and hope that cyber tool vendors will both use and extend it.

Contact: Jason Upchurch, Principal Research Scientist
jason@rti.com 443-223-9488