CSIAC Success Story

CSIAC Assists AFRL to provide cross-enclave situational awareness and mission assurance using ARMOUR Adapter Exploration (AAE)

Customer:	Air Force Research Laboratory Information Systems Division (AFRL/RIS)
Challenge:	Automate information sharing of cyber defense information across enclaves, and provide an approach to automate remediation of threats by developing a capability to interface mission awareness platforms, specifically through the United States' Mission Awareness for Mission Assurance (MAMA) program and the Automated Computer Network Defence (ARMOUR) Technical Demonstrator (TD) project developed by the Defence Research and Development Canada (DRDC). The tasks pursued under this effort supported cyber C2 in demonstrating improved mission assurance and situation awareness.

Approach:	Under the ARMOUR Adapter Exploration (AAE) CAT, the CSIAC leveraged digital messaging technologies to create logical adapters to interface with the MAMA framework and the ARMOUR cyber defense framework, consistent with Unity Coalition Information Environment (UCIE) emerging standards. New cyber defense capabilities were demonstrated prototyping a common integration framework with standardized interfaces such that components developed by different partners – sensor feeds, data management and movement, analysis engines and metrics, incident and intrusion escalation recommendations and scoping information, course-of-action algorithms, and response mechanisms – are compatible and can be used together to provide the combined capabilities in a seamless fashion. Specific activities included: - **Mission Exemplars and Adapter Development & Integration Plan** - The identification and refinement of exemplar scenarios was a necessity in order to perform interface testing and demonstrate the capabilities and utility of the ARMOUR-MAMA adapter. Based on their importance to the effort, CSIAC performed a detailed evaluation of candidate mission scenarios to identify those most appropriate for these two systems/frameworks, as well as the cyber vulnerability sharing objectives of this effort. - **Adapter Software** – The primary objective for this task involved the development of the logical adapters to facilitate the bidirectional communications between the ARMOUR and MAMA frameworks. The developed software was provided to the government along with the final deliverables at the completion of this effort. - **Final Technical Report** - This documented the task's overall background and objectives, as well as the analyses performed and the conclusions reached. - **Final Demonstration** – On December 9th 2016, prior to the completion of this effort, the CSIAC provided a live demonstration of the ARMOUR-MAMA interface, identifying how the two systems are able to communicate and the utility of this capability in improving cyber defense mechanisms with international coordination. Despite the differences between the two systems' design and general purpose, the logical adapter supports bidirectional communications between the two, with automated rule set implementations identifying how to communicate potential threats and take steps to employ appropriate defenses. The slideshow and video presentation that accompanied the software demonstration was submitted along with the Final Technical Report.
Value:	CSIAC developed a capability to interface Coalition partners' mission awareness platforms via the automated sharing of cyber defense information across enclaves. The development of this interface shows that the successful adaptation of the common sensor environment will provide the following benefits: immediate situational awareness of the cyber threat; characterization of cyber effects; and ability to swiftly/effectively neutralize the impact against network enclaves and operational capabilities. This will increase operational resiliency, survivability and overall mission effectiveness in contested cyber environments.