# CYBER SECURITY INITIATIVES AT THE OBJECT MANAGEMENT GROUP, CONSORTIUM FOR IT SOFTWARE QUALITY AND INDUSTRIAL INTERNET CONSORTIUM

## Object Management Group: Cyber Security Initiatives

Cyber threats facing a nation's critical infrastructure, mission-critical systems, or any Internet of Things (IoT) system, demand a cyber infrastructure that matches their combined enormity and complexity.

There are many front-line applications and systems that employ services which need protection from cyber-attacks based on the sensitivity (classified, private, confidential, and legal significance) of the data and algorithms they process. Implementation of cyber protection for these systems often requires multiple layers of protection to insure that their mission execution can be completed under cyber-attack.

Front-line systems used by military and/or first responders are characterized as:

- sea-, air- and land-based
- static or mobile deployments
- manned or un-manned
- surveillance and/or weapon deployment tracking and/or defending technical and resource constraints (e.g., power, weight, and size)

The Consultation, Command, Control, Communications, and Intelligence (C4I) Domain Task of the Object Management Group® (OMG®) focuses on systems that support crisis response operations, emergency management, public safety, and military operations. Such systems are commonly called C4I systems and are taken to include surveillance and reconnaissance together with sustaining disciplines (such as logistics, weather, and air traffic control, etc.).

The OMG and, specifically, its C4I Domain Task Force, issued an RFI titled "Cyber Security Protection for Front-Line Real-Time Systems" to seek ideas, comments, discussions, user needs and experiences, and product information on:

a) how to develop standards to move the tool/integration community forward to reduce costs and focus on higher-quality system development
b) what area of standards can be addressed to reduce cost in developing cyber security solutions and designs for systems and
c) what can be done to integrate current standards that will allow standards-based tools to better support design, development and life-cycle support to reduce and control costs.

## Consortium for IT Software Quality: Cyber Security Initiatives

Recent security breaches such as the ones at SWIFT and Target are entering the realm of nine-digit defects, where damages can exceed $100 million. This makes the security of business applications a board room issue. Many of these headline-grabbing breaches are the result of poor coding and architectural practices that can be exploited for unauthorized entry.

OMG responded to this need by co-founding the Consortium for IT Software Quality™ (CISQ™) along with the Software Engineering Institute (SEI) at Carnegie Mellon University.

CISQ is a neutral, open forum in which customers and suppliers of IT application software can develop code quality standards that detect and quantify critical violations of good coding and architectural practice in software. CISQ measures include standards recently approved by OMG for: Automated Function Points, Automated Enhancement Points, Reliability, Security, Maintainability and Performance Efficiency.

In particular, the CISQ Automated Source Code Measure for Security assesses the risk of security weaknesses due to poor coding and architectural practices. Security problems have been studied extensively by the software assurance community and have been codified in the Common Weakness Enumeration (CWE) at **cwe.mitre.org.**

If you're interested in improving code and system-level quality, then join CISQ's community of system integrators, outsourced service providers, and software technology vendors. Learn more about CISQ at **www.it-cisq.org**.

## Industrial Internet Consortium: Cyber Security Initiative

The Industrial Internet Consortium® (IIC®) is an open membership organization, formed to accelerate the development, adoption and wide-spread use of inter-connected machines and devices, intelligent analytics and people at work. The IIC focuses on testbed cases to prove out theories, plans and objectives before going to market. IIC Working Groups coordinate and establish the priorities and enabling technologies of the Industrial Internet in order to accelerate market adoption and drive down the barriers-to-entry. Learn more about IIC and its mission at **www.iiconsortium.org**.

The IIC published the Industrial Internet Framework Technical Report. For more information go to **www.iiconsortium.org/IISF.htm**.

## Cyber Security Resources

- Read the Cyber Security Protection for Front-Line Real-Time Systems RFI *(closed for responses)* at **www.omg.org/cgi-bin/doc.cgi?c4i/2016-10-1**
- Listen to the Cyber Security Work at OMG Webinar *(recorded)* at **www.omg.org/brighttalk-flyer**
- Download the Cybersecurity flyer at **www.omg.org/hot-topics/Cybersecurity-flyer.pdf**
- Download "Thinking Forward About Federal Civilian Cybersecurity" *(MITRE technical paper)* at **www.omg.org/mitre-flyer**
- Download the Industrial Internet Consortium Industrial Internet Security Framework Technical Report at **www.iiconsortium.org/IISF.htm**

## Want to learn more?

We are happy to discuss how OMG membership will benefit your organization! Feel free to explore our website at **www.omg.org** and when you are ready, please contact **bd-team@omg.org** or call + 1-703-231-6335 to get started.

## About OMG

The Object Management Group® (OMG®) is an international, open membership, not-for-profit computer industry standards consortium with representation from government, industry and academia. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries. OMG's modeling standards enable powerful visual design, execution and maintenance of software and other processes. Visit **www.omg.org** for more information.

OMG® OBJECT MANAGEMENT GROUP®

industrial internet® CONSORTIUM

CISQ™ Consortium for IT Software Quality™

For a listing of all OMG trademarks, visit **www.omg.org/legal/tm_list.htm**. All other trademarks are the property of their respective owners.