



SUMMARY

CYBER RESILIENCE SUMMIT: Strategies to Modernize & Secure Government IT

March 20, 2018 in Reston, VA

We were honored to have garnered such robust support again from thought leaders in the White House, Pentagon, Executive Branch, and leading industry groups for our bi-annual event. The quality of our attendees was almost as good as our distinguished speakers, providing one of the most dynamic and interactive programs available! Thank you for engaging in discussion.

For those who were unable to join in person, we felt it important to highlight key points made regarding cybersecure software and insights from those responsible for developing the "Strategies to Modernize and Secure Government IT" as detailed in FITARA, IT MGT Act, EO 13800 and the President's just released Management Plan.

CISQ STANDARDS

- CISQ is currently engaged in extending its [quality characteristic measures](#) to cover [embedded](#) software. The team updating the measures reports that embedded software has become more like enterprise software, with differences primarily focused on real-time aspects. CISQ anticipates releasing a draft of the updated quality standards later this year. CISQ has recently completed development of an OMG® standard for measuring [Technical Debt](#) that provides a correlate of the corrective maintenance costs remaining in an application. Regarding deployment, several federal agencies have begun referencing the CISQ quality standards.

CYBERSECURITY

- Speakers discussing cybersecurity argued that attack surfaces have become extremely broad given the extensive interconnections between applications. IT must assume attackers have penetrated weak points in the application chain and therefore must ensure internal protections for critical data. Defense is the best offense. IT cannot assume external software and libraries are secure. Ron Ross, NIST's Risk Management lead, stressed that cybersecurity must begin with design engineering, and that we need to evaluate cyber-risk "below the waterline", that is, the IT support system that resides below the visible applications. Since software has become a primary source of business risk in most organizations, CISQ proposed developing a 'Trustworthy Systems Manifesto' that guides executives in the practices they should require as part of their governance responsibilities.

MODERNIZATION

- On modernizing and securing legacy systems, agencies and contractors will need to reach deeper into commercial standards and innovations, recognizing that the Federal IT sector is less than 2% of the \$4T Global IT market. Grant Schneider, White House CISO filling in for Rob Joyce, and Ron Ross from NIST, emphasized the need for greater attention to improving both speed and rigor in IT modernization decision-making in terms of cyber vulnerabilities, supply chain risks, cost realism and business value. Traditional approaches have created the current situation - insecure and unmanageable legacy systems

that are a target of our adversaries. Agency heads who embrace Risk Management standards and Agile Acquisition (see CISQ software quality standards: <http://it-cisq.org/standards/> and ICH's Acquisition Assurance Method: <http://it-cisq.org/wiki/cyber-resilience-summit-knowledge-repository/#itaac>) are much more likely to gain access to new funds, while avoiding past failure patterns that have undermined the public trust.

You are encouraged to visit the Cyber Resilience Summit Knowledge Repository to download the presentations and sustentative materials: <http://it-cisq.org/wiki/cyber-resilience-summit-knowledge-repository/>

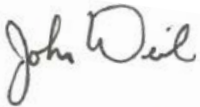
Thank you to CISQ corporate sponsors [CAST](#), [CGI](#), [Cognizant](#), [ISHPI](#), [Northrop Grumman](#), [Synopsys](#) and [Tech Mahindra](#) for supporting this work - as well as our lunch sponsor, [Bugcrowd](#).

CISQ and IT-AAC are offering on-site learning seminars and mentoring programs for agencies looking to bootstrap their IT modernization and software resilience efforts. Contact us for details.

Sincerely, from program chairs,



Dr. Bill Curtis
Executive Director
Consortium for IT Software Quality
bill.curtis@it-cisq.org



John Weiler
Vice Chair
IT Acquisition Advisory Council
john@it-aac.org