EXECUTIVE SUMMARY

Event: Cyber Resilience Summit: Modernizing and Securing Government IT

Topic: Reducing Modernization Risk through Compliance to Software and Risk Management Standards

Hosts: Consortium for IT Software Quality (CISQ) in cooperation with the Object Management Group (OMG) and IT Acquisition Advisory Council (IT-AAC)

Date and Location: October 19, 2017 at Army Navy Country Club, Arlington, VA

Program: http://it-cisq.org/cyber-resilience-summit-oct-2017

Knowledge Repository: http://it-cisq.org/wiki/cyber-resilience-summit-knowledge-repository/

Thank you SOF Intelligence Solutions and Bogart Consulting for taking meeting notes

EVENT BACKGROUND

The Consortium for IT Software Quality held its 4th annual Cyber Resilience Summit at the Army Navy Country Club in Arlington, Virginia with co-host IT Acquisition Advisory Council (IT-AAC). “Titans of Cyber” from the U.S. Federal Government attended to discuss Federal IT policy, directives, and recommendations for securing and modernizing critical IT infrastructure. The cyber risk standards community briefed on standards and best practices for achieving these goals.

Photo: Cyber Resilience Summit Opener with John Weiler, Donald Freese, Greg Smithberger, and Tony Scott

KEY POINTS

Modernization initiatives provide a unique opportunity to improve the cyber security and resilience of government IT systems.

- For IT acquisition, work on simplifying requirements to align to modern components and cloud-based architectures, focus on buying outcomes rather than resources, and add standard metrics to IT project proposals to control the risk of software delivered to government. (See GSA and State Department acquisition examples based on CISQ metrics)
- For development, leverage DevSecOps. Quoting Marc Jones, CISQ Director of Public Sector Outreach, "Modern agile development techniques around container-driven development, supported by automated tool chains to assess and build systems, can easily be extended to include software tools that evaluate all releases and builds for compliance with common sense standards like CISQ."

Government IT policy is converging around these key areas:

- Cyber security and risk management
- Strategic IT modernization funding
- Cloud computing and shared digital services
- Faster delivery of capabilities and new technologies
- Acquisition reform to be more iterative and affordable
- Empowering courageous and accountable leaders

Two items flagged by Tony Scott, President Obama's Federal CIO, as not being addressed fully by the government:

- The Human Resources (HR) issue. There is a tremendous number of people leaving the government in the next five years who are the only ones who know how to run ancient systems. It's like another Y2K creeping up on us. Not enough resources are available to migrate to new systems that are required. Mr. Scott is in favor of Congressman Will Hurd's plan to create a Cyber National Guard with industry partners to accelerate change.
- No design decision yet. An attempt to "lift and shift" legacy systems to modern infrastructure is not the answer as this still leaves us with silos. To quote Mr. Scott, "Don't throw an org chart at the problem."

IT Modernization sound bites:

- Cannot get resiliency at a component level, it's only achieved at end-to-end architectural level – and the org chart gets in the way. – Smithberger
- It takes more than a year's budget to move from legacy to shiny and new, and budgets are always one year. Congress is looking at a pool of investment money for this purpose (IT MGT Act), which will be tremendously helpful. – Eisensmith
- In commercial settings, measures of structural quality in applications have been correlated with the number and cost of incidents. – Curtis
- Technical debt and its components of principal, interest, liabilities, and opportunity cost provide a powerful metaphor for explaining the cost of quality to non-IT folks. – Curtis
- CISQ's Automated Technical Debt Measure has been finalized as an OMG standard. It provides an estimate of future corrective maintenance costs. – Curtis
- Plan, plan, plan. Don't just "lift and shift" to cloud infrastructure. Re-think what you need for the next level of performance rather than updating toolsets. – Mosley
- Get senior-level buy-in early and have a plan with wins along the way to keep leaders engaged. Decouple massive problems and break into smaller pieces. – Wilmer
- Modern software architecture is now microservices-based. Cyber processes must change to recognize this new architecture. – Bible

- It's becoming more important that Government IT program managers become smart and educated on commercial software licensing. This is just as important as skills on the technology side. – Bible
- When using open source software, be aware of support, patches, maintenance and license structure. – All
- Code complexity is not your friend. Things should be simple and transparent to reduce risk. – Eisensmith
- Commercially supported open source can strike a good balance. – Wilmer
- Adversaries are looking to attack architecture design traits. – Stempfley
- Security must me managed through the entire software supply chain since modern apps are a stack of technologies coming from different places and each possibly including open source or third-party components. – Curtis, Jarzombek
- States must take the initiative in securing their systems and the law in Texas regarding measurement of state system development is a start – Krasner, Jones

4. Cyber Security is not possible without software quality. Get to the data later.

- The focus used to be on securing systems. Now we know we should build it right the first time. – Jones
- Operate at the data layer for scalability and flexibility. – Arrieta
- Elasticity is gone if you only protect the perimeter. – Bible
- Majority of toolsets are based on perimeter protection and not on the data layer. We need to migrate. – Mosley
- We realized that no matter how much we protected our systems, something could happen. Navy created the Cyber Safe team to focus on securing mission-critical systems. – Lang

DISTINGUISHED SPEAKERS

- Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ)
- John Weiler, Vice Chair, IT Acquisition Advisory Council (IT-AAC)
- Tony Scott, former Federal Chief Information Officer
- Greg Smithberger, CIO/CTO, NSA
- Donald Freese, FBI Deputy Assistant Director for Information Technology
- Dr. Thresa Lang, Deputy Director, Navy Cybersecurity/Deputy Director, Department of the Navy Deputy Chief Information Officer
- Dr. Edward E. Amoroso, CEO, Tag Cyber LLC
- Jeffrey Eisensmith, CISO, DHS OCIO
- Sara Mosley, Acting Director for the Office of the Chief Technology Officer, DHS CS&C
- Jack Wilmer, Cyber lead for American Technology Council, White House OSTP
- Ken Bible, Deputy CIO, U.S. Marine Corps
- Dr. Ron Ross, Computer Scientist and Fellow, NIST
- Roberta Stempfley, Director of SEI's CERT Division
- Herb Krasner, University of Texas at Austin (ret.), Texas IT Champion
- Marc Jones, Director of Public Sector Outreach (Vol), Consortium for IT Software Quality (CISQ)
- Therese Firmin, Principal Director, DCIO (CS) and Deputy Chief Information Security Officer, Department of Defense
- Jose Arrieta, Director, Office of IT 70 Schedule Contract Operations, GSA
- Brigadier General (ret) Greg Touhill, former U.S. CISO; President of Cyxtera Federal Group
- Matt Conner, CISO, National Geospatial-Intelligence Agency
- Joe Jarzombek, Global Manager, Synopsys Software Integrity Group
- Emile Monette, Senior Cybersecurity Strategist and Acquisition Advisor, DHS OCISO
- Shon Lyublanovits, IT Security Category Manager and Director of the Security Services Division for the Office of Integrated Technology Services (ITS) in GSA's Federal Acquisition Service (FAS)
- David Duma, Acting Director, Operational Test and Evaluation, Department of Defense
- Don Davidson, Chief, Lifecycle Risk Management & Cybersecurity/Acquisition Integration Division, Department of Defense (DoD-CIO)

SPONSORS

PARTNERS

CONTACTS

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

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

Tracie Berardi
Program Manager
Consortium for IT Software Quality (CISQ)
tracie.berardi@it-cisq.org