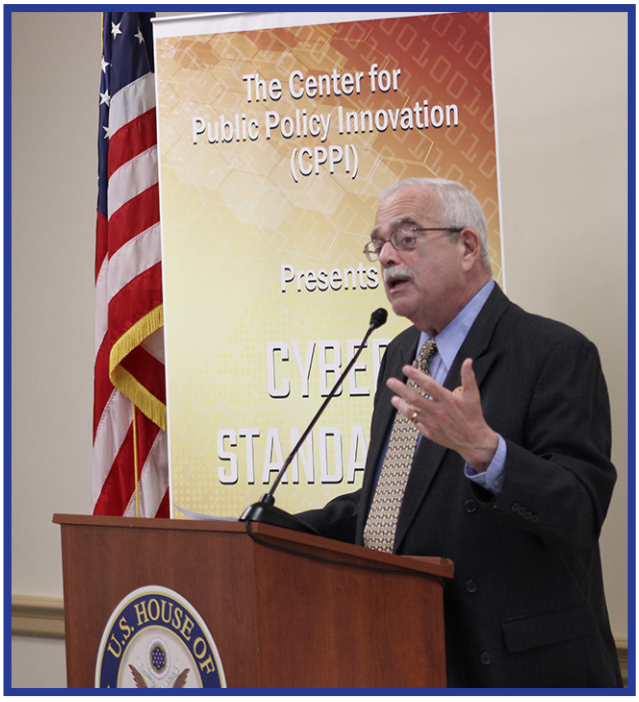
Cyber Standards for Modern IT

The Case for Standards in Software Development and Acquisition

On May 1 in Washington, DC, CISQ presented at *Cyber Standards for Modern IT*, an event co-hosted with the Homeland Security Dialogue Forum and Center for Public Policy Innovation. The purpose of the meeting was to educate members of Congress and their staff on standards developed by CISQ to reduce risk and improve outcomes in IT. CISQ described how to use the standards in software development to build better systems (DevSecOps), and in contracts with vendors to ensure the software being put into place is secure, resilient, and sustainable. This comes at a time of increased Congressional oversight and legislation for IT modernization and cybersecurity practices in government, including the Federal IT Acquisition Reform Act (FITARA), Modernizing Government Technology (MGT) Act, and Executive Order (EO) 13800 for Cybersecurity.

Congressman Gerry Connolly (D-VA) delivered a keynote in support of FITARA, signed into law in 2014, calling for the measurement of Federal agency IT outcomes in the FITARA Scorecard. The FITARA Scorecard has categories to measure agencies in the areas of: transparency and risk management, data center consolidation, software licensing, IT modernization (MGT Act roll-out), and more. Categories in the FITARA Scorecard are iterative to drive outcomes that strengthen IT. Connolly also called for improvements to FedRAMP, a government IT procurement program designed to accelerate cloud computing technology by pre-approving vendors.

Dr. Bill Curtis, Founding Executive Director of CISQ, continued by describing why software projects fail. He explained the technical advances being made in software engineering to automate detection of severe weaknesses in software-intensive systems and reviewed international standards produced by CISQ for analyzing the security and reliability of software. A panel of stakeholders discussed how the standards can be inserted into acquisition policy and practices to reduce the operational and security risk of government systems. The panelists (discussed the work being done at the Department of Homeland Security (DHS), Government Accountability Office (GAO), General Services Administration (GSA), Office of Management and Budget (OMB) and Consortium for IT Software Quality (CISQ).



Key Takeaways from the Panel Discussion

Dave Powner, Director of Strategic Engagement and Partnerships at MITRE and former Director of IT Issues at GAO:

- FITARA helps us modernize IT and measure digital capability. Measurement drives improvement. 50% of agencies were using an incremental approach to development; now 89% are using an incremental approach with 6-month deliveries. These are huge outcomes to populate the MGT bucket.
- Advice for FITARA 2.0 is to include metrics of mission-effectiveness, such as the CISQ metrics.

Beth Killoran, Deputy CIO at GSA:

- In government IT, there is a merger of Commercial-off-the-shelf (COTS) solutions and coding. We use a DevSecOps approach at GSA for velocity and security.
- The early result of using CISQ standards in contracts has been positive. It makes the conversation easier.
- There is a balance between compliance to standards and risk-based assessment.

Paul Seay, Northrop Grumman Technical Fellow and CISQ Governing Board Member:

- Standards provide a fair playing field. Standards help government and contractor sides to agree.
- In agreements, change "should" statements to "shall" based on an industry standard. Consider maintainability.

Lesley Field, Acting Administrator, Office of Federal Procurement Policy at OMB:

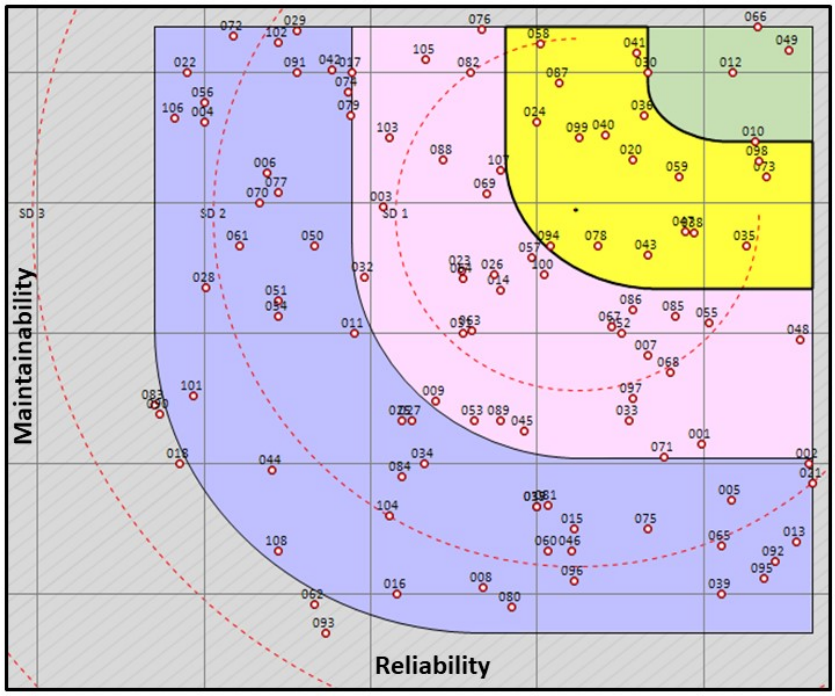
- There is an acquisition modernization system at OMB. We are working on acquisition language with various stakeholders. There is a Digital IT Acquisition Professionals Program.
- Using outcome-based standards can help enhance acquisition of purpose-built systems.

From left to right: Mr. Luke McCormack, Mr. David Powner (MITRE), Ms. Beth Killoran (GSA), Ms. Lesley Field (OMB), and Mr. Paul Seay (Northrop Grumman)

MITRE Study of Federal Systems

Software quality evaluation of 108 Federal systems regarding factors affecting operational and cost risk

Too high quality	- 5
Quality is good	- 17
Needs minor improvement	- 34
Needs major improvement	- 46
Outside range	- 6



Source: *The MITRE Corporation, John Marien, 2019*

Summary of major takeaways from the event:

- The U.S. spends $550B each year on federal contracts - $65B of that is for IT programs.
- New research from MITRE indicates nearly half of government IT systems are substandard for quality.
- Software quality measurement is critical to acquisition, technical risk, quality management, and acceptance.
- FITARA 2.0 should incorporate metrics of mission-effectiveness, with software quality standards helping to achieve better outcomes.
- The FedRAMP certification process should be made easier and more predictable for industry.
- In government IT contracting, standards provide a fair playing field for government and contractors.
- Identifying flexibility in the Federal Acquisition Regulation can improve the way government does procurement.

The standards written by CISQ enable organizations developing or acquiring software-intensive systems to measure the operational risk software poses to the business, as well as estimate the cost of ownership. The presentation from Dr. Bill Curtis with CISQ is available at this link. In addition, there are a multitude of other resources available on CISQ's website including the Trustworthy Systems Manifesto, webinars, and several papers with technical guidance.

"Most of the serious outages and security breaches are caused by badly engineered software.

There are now industry standards for software quality measurement that can be used and written into acquisition policy at the federal level to ensure reliability and security of IT systems."

- Dr. Bill Curtis, Founding Executive Director of CISQ