CYBER RESILIENCY SUMMIT: Ensure Resiliency in Federal Software Acquisition

**Topic:** Improving System Development & Sustainment Outcomes with Software Quality and Risk Measurement Standards

**Hosted by:** Consortium for IT Software Quality (CISQ) in cooperation with Object Management Group, Interoperability Clearinghouse, IT Acquisition Advisory Council

**Date:** 20 October 2016 from 0800 – 1230

**Location:** Army Navy Country Club, 1700 Army Navy Drive, Arlington, VA

**Agenda and Presentations:** [http://it-cisq.org/cyber-resilience-summit-2016/](http://it-cisq.org/cyber-resilience-summit-2016/)

---

**Event Background**

The Consortium for IT Software Quality (CISQ) held its semiannual Cyber Resilience Summit at the Army Navy Country Club in Arlington, Virginia in cooperation with the IT Acquisition Advisory Council (IT-AAC) and other IT leadership organizations. “Titans of Cyber” from the U.S. Federal Government attended the Summit to share critical insights from the front lines of the cyber risk management battle. The program focused on standards and best practices for measuring risk and quality in IT-intensive programs from the standpoint of productivity, software assurance, overall quality and system/mission risk. The discussion addressed proven methods and tools of incorporating such standard metrics into the IT software development, sustainment and acquisition processes.

**Discussion Points**

**John Weiler, IT-AAC Vice Chair** and **Dr. Bill Curtis, CISQ Executive Director** opened the Summit.

Dr. Curtis gave an overview of CISQ, explaining that it was co-founded in 2009 by the Software Engineering Institute (SEI) at Carnegie Mellon University and Object Management Group (OMG) and is currently managed by OMG. The Consortium is chartered to create international standards for measuring the size and structural quality of software. Its mission is to increase the use of software product measures in software engineering and management. Dr. Curtis developed the original Capability Maturity Model (CMM) while at the SEI and now directs CISQ. Current sponsors include CAST, Synopsys, Booz Allen Hamilton, Cognizant, others.

Significant CISQ contributions include:
- A standard for automating Function Points that mirrors IFPUG counting guidelines
- Four measures of structural quality to quantify violations of good architectural and coding practice:
  - Reliability
  - Performance Efficiency
  - Security
Maintainability

- It is important to note that most measures of reliability assess system availability or downtime, which are behavioral measures. The CISQ measures assess flaws in the software that can cause operational problems. Thus, the CISQ measures provide pre-release indicators for operational or cost of ownership risks.

CISQ measures can be used to track software performance against agreed targets, as well aggregated into management reports to track vendor performance. The continuing stream of multi-million dollar failures is causing an increased demand for certifying software. Although CISQ will not provide a certification service, it will provide an assessment process to endorse technologies that can detect the critical weaknesses that comprise the CISQ Quality Characteristic measure standards.

The Security measure effort was led by the next speaker, Robert Martin, who oversees the Common Weakness Enumeration Repository maintained by MITRE Corporation. This repository contains over 800 known weaknesses that hackers exploit to gain unauthorized entry into systems.

Robert Martin, Senior Principal Engineer at MITRE, gave a presentation on: Defending Against Exploitable Weaknesses When Acquiring Software-Intensive Systems.

- Mr. Martin’s main themes were:
  - We are more dependent upon software-enabled cyber technology than ever
  - Hardware and software are highly vulnerable so the possibility of disruption is greater than ever
  - Software in end items (ex. Cars, fighter jets, etc.) is growing at an exponential rate
  - Almost everything is cyber connected and co-dependent during operations and/or other phases of life
  - Today up to 90% of an application consists of third party code

Mr. Martin’s main question was how do we track and measure all the code characteristics that are flowing into software development? How do we determine and track what is really important?
Mr. Martin then described how to establish assurance by using an Assurance Case Model (Safety Case Tooling) with the elements of Claim/Sub-claim, Argument, and Evidence. He pointed out that this evidence-based assurance is an emerging part of NIST SPs 800-160 (draft) and 800-53 Rev 4.

- This technique is good for capturing complicated relationships
- Tying the evidence to supported claims can be an ongoing part of creating and maintaining the system
- It is useful for Mission Impact Analysis and Cyber Risk Remediation Analysis

Mr. Martin also identified the Common Weakness Scoring System (CWSS) and the Common Weakness Risk Analysis Framework (CWRAF) that applies to the SANS Top 25 list. He then identified the benefits of using multiple detection methods, as some are good at finding cause, while others are good at finding effect. We can use multiple detection methods to collect evidence through all phases of development from design review through red teaming – all the while considering the most important common weaknesses.

Mr. Martin then discussed program protection planning for prioritization/criticality analysis, using the assurance case to tie claims to supporting evidence. He also introduced the concept of “trustworthiness” that is a combination of factors like safety, privacy, security, reliability, and resilience. For example, a security “false-positive” may be a safety or reliability issue.

Finally, Mr. Martin pointed out that we can manage assurance cases with claims and the association of evidence to claims and that the evidence is articulated using structures related to common weaknesses. This accounts for all types of threats including human error, system faults, and environmental disruptions. Assurance cases can also be exchanged and integrated to aid extended system analysis.

CISQ is a standard for measuring security, safety and reliability in a consistent and computable way.

Next, the Titans of Cyber panel was led by Dr. Marv Langston, Principal, Langston Associates.

Dr. Marv Langston introduced the members:
• **Dr. Ray Letteer**, of the USMC stated the Marine Corps cyber concerns are for operational working metrics using standards. The need is for technical details not a “trust me” plan of action and milestones.

• **Kevin Dulany**, of DIAP, (a protégé of Dr. Letteer) stated that networks are “hard on the outside but soft in the middle.” Attacks today are data driven – inside the networks but current risk management frameworks (RMFs) are based on traditional constructs of IT. Procedures require them to use these RMFs but the mitigations do not actually apply. Embedded computing drives the need for a different approach with new mitigations. Kevin also noted that some levels of security tend to be categorized at a lower level because of the lack of resources.

• **Chris Page** of ONI stated that we do have superiority because of our great technology, citing that the Navy pub, “Design for Maintaining Naval Superiority” is a message (warning) to our adversaries.

• **Martin Stanley** of DHS said that their focus is on securing high-value assets. Their process assesses the security posture, applies measures for a year, and then reassesses with lessons learned. He went on to say that root causes are related to basic IT practices and ways the organization must operate systems. His organization is producing enterprise architecture (EA) guidance that is unusual for cyber because it attempts to address root causes.

• **Dr. J. Michael Gilmore** of DoD OT&E said that our systems are not designed with cyber security as a priority. He gave an example of a supporting network to an aircraft that was not considered in recovery and was also tied to a vendor network. He explained that capabilities need to be secured from both the government and contractor sides. Mike also cited that people can be major conduit for bad cyber – especially worldwide partners. Finally he added that the Joint Regional Security Stacks (JRSS) is essential for DoD but that people in the field are not fully trained and don’t understand its use or vulnerabilities.

• Dr. Marv Langston kicked off the discussion by stating:
  - We test and deliver *but don’t look back*. Why don’t we do cyber tests on operational systems – on a daily basis?
  - **Dr. Gilmore** – We have a limited project to do and are facing resource constraints so we push back on current cyber authorities. The commercial sector does continuous red teaming but the Government is resisting – deploy and forget.
  - **Dr. Letteer** – Testing must be continuous. The USMC has established “White Teams” to do continuous scans, coordinating with red teams. In addition, we have cyber protection teams to help put in mitigations. This is not as widespread as we would like but we are making progress. The USAF has a similar program.
  - **Mr. Stanley** – Many agencies are working with DHS on continuous monitoring. The traditional Certification and Authorization (C&A) process has a place but continuous monitoring is supplemental. Overall compliance is more important than continuous monitoring, and this must change.
  - **Mr. Dulany** – We used to have high emphasis on system security engineering but with too much reliance on contractors. Today we look at controls but that does not get us down into useable specifications or standards. The RMF is a good tool but we have problems keeping up with technologies. We cannot use tools in certain environments, so continuous RMF would help to reinforce compliance.

• Dr. Langston – I’m concerned that we will wear ourselves out with all these processes but will miss the critical checks like the daily cyber check
  - **John Weiler** – The software market is constantly refreshing but we still have 1985 software weapon systems.
  - **Dr. Gilmore** – We resist processes that are not spelled out in specifications. What percent of this good stuff are actually in RFPs? So, we will get resistance to innovative metrics because they are not in the specs.
Dr. Letteer – I agree, we are trying to get cyber security measures in RFPs but this is hard with any specifications. We are used to doing cyber (requirements) in general but cannot do it in the specifications. Because of this, cyber security is not a mandated function.

Dr. Gilmore – We used to get in response to cyber security “There are no formal requirements for cyber security in DoD requirements.” The Joint Staff is working on cyber Key Performance Parameters (KPPs) but we are not there yet. All we have so far is a document that describes acceptable degradations after a cyber-attack. As of yet, there are no cyber security requirements blessed by the JRCC.

Mr. Page – Also, we see people shopping around for a threat profile to fit the security they implemented.

Questions from the audience:

- Question – Aren’t there software assurance metrics language that could be adapted to programs?
  - Panel – Sounds good to us, but we do not tend to use the most modern tools like the Google desktop.

- Question – Today’s cyber activities seemed to be aimed at the whole stack but not at individual levels.
  - Panel – This relates to how we cement Government – Industry partnerships. We are good at sharing high-level information but not at collaborating on the details. How do we change what we do across the environment? We can look at the kill chain concept to identify our weak points. However, we must look at needed capabilities first then look at tools.

- Question – Relating to cyber KPPs, we are trying to work with operators on how we manage risk. We need new commercial standards and it is important to work with industry.
  - Panel – Agree, but we are disappointed that this is taking two years. In addition, we are not sure we have PMO experience to understand cyber security engineering architectures. There is also more emphasis on getting complex mobile IT networks to function in the field. This has analogies in the commercial market but not specifics. Therefore, we struggle to get them to work and to facilitate links to supporting entities who can address failures. Common sense cyber controls would cause the (mobile) system to fail – not sure what we can do about this.

- Question – The scale of nodes is moving from millions to billions, what does the panel think of this?
  - Panel – Going to IPV6 will help drive this complexity. Of course, our mobile devices have access to our networks. We have to focus on the assets we really want to protect, not everything. We must be prepared for continuous surprise. We need to keep up with bad actors, but the solution is not necessarily to modify the RMF. This is a continual slog that we continue to do over the years.

BREAK

Keynote speaker Dr. David Bray, CIO of the FCC, presented: Charting Cyber Terra Incognita: A CIO’s Perspective and Challenges.
Dr. Bray began his presentation by emphasizing the exponential growth in IT, human participants, and networked devices. His Terra Incognita (unknown land) is the combination of complex legacy infrastructure, the explosive growth of internet-connected systems, all with human actors and behaviors. This complexity and human interaction make it impossible not to have cyber issues and we must strive for resiliency. He said that cyber threats will run like infectious diseases across borders and that the public, private sector, public sector, academia, and non-profits must all build bridges to deal with this. Fortune 500 CEOs cite having one cyber security engineer for each $1B of data. In addition, threats are over classified so it is often hard to make the case for cyber security support. Dr. Bray mentioned “DIY” and the “internet of everything” that is outpacing cyber controls, citing examples such as industrial controls (moving to the internet with weak security, but consumers are not willing to pay for more) and capabilities for grass root entrepreneurs – pioneering civic and social innovation (but could be exploited by terrorists). He also described a greater reliance on IT with machine learning as an essential complement to human activities. Exponential growth in technology is also spilling over into bio warfare with DNA engineered bugs. Everything in cyber could be in bio within 5 years. He cited the example of the FCC that was a sitting target for cyberattacks but then went to 100% public cloud – from premise to off premise. In the briefing, Dr. Bray then described the giant leap from IPV4 to IPV6; addressing numbers from $2^{32}$ to $2^{128}$. This is like moving from the volume of a beach ball to the volume of the sun! Dr. Bray talked about the importance of “Public Service” (21st century) Vs governance (20th century). He ended by emphasizing the need for more “change agents” in these exponential times.

At the conclusion of Dr. Bray’s presentation, John Weiler (IT-AAC) asked, “What do we see as the difference between (big) agile acquisition and agile development?”

**Dr. Bray** – We should not be in the code writing business. We are trying to procure IT capabilities in 6-9 months so agile acquisition should be an “a la carte” method with selectable modules.

**Leo Garciga, Joint Improvised Threat Defeat Agency (JIDO)** – In this commoditized environment, why do we still build custom stuff? Even standards are commoditized.
Dr. Bray – The commodity approach is good. Instead of Business Process Engineering, we should just keep it simple and draw on the board “how do you want to work”. In the FCC, we tried to automate an on-line form with an initial estimate of $17M but found we could do it for $450K using the commodity approach.

Question from audience – What should we do about weapon systems and cyber vulnerabilities?

Dr. Bray – We must balance availability and protection. Sometimes we rule out cloud-based solutions by asking ourselves “do I want this on the internet?”

John Weiler – What are services that can be on the internet?

Dr. Bray – We can move to limited public and Government internets (Taiwan and Australia do this.)

Question from audience – How do we retrofit TCPIP to be more secure in flight?

Dr. Bray – 1. Trust but verify (red teams). 2. Focus on Mission (what do you really need?)

Next, Leo Garcia, J6 Chief / CIO, JIDO and Ryan Skousen, Software Engineer, Booz Allen Hamilton presented: Integration of Security and Agile/DevOps Processes.

The presentation began with a review of JIDO’s mission as a quick reaction capability – to bring timely solutions to war fighters. The J6’s mission for IT is to:

- Built a Big Data analytic platform, “Catapult,” and tool suite based on real-time, tactical needs
• Embed with users worldwide to understand data available, analytic methodologies, & capability/data gaps
• Provide solutions required same day at times

JIDO has been doing Agile SDLC for five years. Continuous integration is already implemented with nightly security scans. Release management with traditional CM/CCB is still hard. Agile alone is not enough.
• Quick reaction capability to emerging threats
• Quicker than standard DoD process; seeing agility and speed
• Length of time to approve is standard
• Intel fusion system with focus on how to change and when we need to change

JIDO started DevOps evolution in 2015. Security and compliance is built in upfront. JIDO’s goal is to completely automate deployments from code to production. We think this is a great capability.
• Focus on managing risk and not compliance
• Small changes
• No manual/human review gate
• Affordable by other agencies

Security /accreditation – ongoing authorization is secure agile + DevOps + continuous monitoring. JIDO has also developed an automated ongoing authorization pipeline.
• Think through C&A before writing code
• Adopt mission focus
• Security accreditation (per NIST SP 800-37) can be automated to a large extent and should help to implement decisions by continuous monitoring instead of one-by-one inspection of packets – sort of an “ongoing authorization”

JIDO is still working to transition capability. This is hard to do but we are working to make it transferable to other agencies

Major takeaways:
• Secure design and planning throughout SDLC
• Containers for standardized deployment packaging
• Secured, transparent DevOps pipeline.
  o Prohibits tampering, provides monitoring, and traceability.
  o Escalation based on code triggers (code delta, coverage)
• Type-accredited platform to receive and run containers
• It is like having a trusted candy factory, packaging goodies into bulletproof briefcases, transporting through a point-to-point hyperloop, delivering to candy shops with turrets – Really need to lick every lollipop?

Question from audience – How long will it take to fully implement JIDO Agile/DevOps process?

JIDO – We are now in full deployment across the classified and unclassified environment. We still have some staff education issues, but technically, we are up and running by working out CM problems.

John Weiler – In the DevOps world, speed is sacrificing some assurance issues. How do we recognize and incorporate engineering needs for safety/security?

JIDO – DevOps cannot be used for new ground up systems. Our process incorporates assurance by having daily scrums.
John Weiler – Security engineering cannot be determined by engineering. We must force rigorous engineering of systems with knowledge infusion.

JIDO – Yes, we do that by scanning in real time.

Question from audience – How do you characterize the tech challenge vs. the people challenge?

JIDO – This is a HUGE cultural change. We initially had a lot of push back with people worried about their rules.

The second panel, Standards of Practice for IT Modernization and Software Assurance, was led by Dr. Bill Curtis, CISQ Executive Director.

Don Davidson, DoD kicked off the panel with a short presentation on DoD cyber resilience:

- Cyber resilience is to ensure that DoD missions (and their critically enabled systems) are dependable in the face of cyber warfare by a capable cyber adversary.
- The DoD cybersecurity campaign:
  - Cybersecurity discipline implementation plan
  - Cybersecurity scorecard
  - Culture and compliance
- The campaign covers these cybersecurity disciplines:
  - Strong authentication for access
  - Device hardening with configuration management / SW patching
  - Reduction of attack surface
Monitoring and diagnostics

- Mission appropriate cybersecurity balances risks vs. additional security (beyond cybersecurity discipline) for trusted systems.
- Approach incorporates fundamental basis of supply chain risk management and addresses compliance through policy.

Joe Jarzombek, Synopsys – We are starting to implement SW assurance systems to address low hanging fruit.

Tom Hurt, DoD – Layers of cybersecurity are like multiple Maginot Lines applying 95% of assets on 16% of problems. Software must be integrated into system engineering.

Emile Monette, DHS – We have challenges to interpret cases and do not cover them all. We have many weaknesses in thousands of categories and automation is difficult. System security measures we discussed today are useful, but we can also focus on human expertise and leave other forms of assurance to automation.

Mr. Jarzombek – It is about leadership, not technical issues. KPPs get diminished for functionality. We need to be more demanding on providers and have requirements that are more specific, MOEs, and testing. We can specify industry standards but we must also help providers work through issues.

Mr. Davidson – We need to write KPPs because there are baseline security requirements that cannot be traded away. CIOs and CISOs are always fighting – but it needs to be a healthy dialog.

At the Black Hat conference, we heard:
- Major breaches will continue for two years (bad for CISOs)
- Industry may have to provide software with warranties
- Software as a Service (SaaS) is a good model. Self-driving cars will lead to insuring software!
- Sourcing untrusted libraries may drive some away from COTS to in-sourcing

Mr. Hurt – For mission assurance, we can take successful attacks back through architects and engineers to analyze with tools including penetration. Why don’t we have red hat (penetration) tests as part of O&M?
- We could avoid vulnerabilities in development
- It always take more money to fix something after the fact

Dr. Curtis – 40% of software engineers are self-taught.

Panel members – We should ask if people and products we have are certified. We need (strong) leadership to avoid deploying dangerous products. This can be part of the RFI. One approach to vetting would be to have industry recommend proper controls, but other vendors may reject the recommendations.

Dr. Curtis – We need to know that a piece of software has some sort of certification. Education may help, but this is a complex issue and cyber courses in schools are not standardized. Institutions are now promoting cybersecurity basics in software engineering schools. We could approach this like a community “buyers’ club” – putting assurance in all Agency networks with requirements to build security into the software. This idea is emerging in industry such as the Vendor Security Alliance. These are models we could use to promote Government standards.

Mr. Hurt – The DoD Program Protection Plan requires use of assurance measures. We need assessments that are passed on to DT, OT, and O&M. We had a Joint Federation Information Assurance IOC in April 2016.

Dr. Curtis – How does cybersecurity work with agile? Agile is not incompatible with this and assumes activities are engaged with customers.
**Mr. Hurt** – For each sprint, we need a good set of allocated requirements and they must cover assurance – so we blend assurance into agile.

Question from audience – Do we need continuing education for cybersecurity professionals?

**Panel** – Yes, it is required for CISSPs. In addition, software engineers should be networked to work fixes to bugs. There are software development courses that cover cybersecurity but we still lack hard and fast requirements. The Government always asks for Project Management Professionals (PMPs) but rarely for cyber credentials.

Who is teaching “formerly verified code”? This is a great concept of merging AI with humans but we don’t know how mature it is or how long it would take to train someone.

Question from audience – What are we doing to give “tactical” hands on knowledge?

**Dr. Curtis** – Industry does not want to train and generally looks for experience. We have professional students vs. untrained practitioners. There is lots of pressure to push out code.

Question from audience – How does Government want industry to train? What certifications?

**Mr. Hurt** – New DoD 5000.2 will have software tools. We hope policy will move into guidance and best practices on websites. (DoD has 100,000 system engineers)

Question from audience – There is no certification in industry for security in software coding so we have to use contract (language) to govern security requirements. The FAR allows us to make suppliers fix bad software, but who exercises this? It does not seem to stand up in court.

**Mr. Garciga** – Scanning of software helps to deal with this. We should scan before acceptance. We must also get source code and software design description (SDD) to promote an organizational maturity. See White House.Gov on open source code that is forcing PMs to build document libraries of software with access to source code.

The Cyber Resilience Summit ended at 1230 with John Weiler (IT-AAC) and Dr. Curtis (CISQ) gave closing comments.

Join us at the next Cyber Resilience Summit on March 21, 2017 in Reston, Virginia.

Contact: Tracie Berardi, Program Manager, Consortium for IT Software Quality (CISQ)
tracie.berardi@it-cisq.org; 781-444-1132 x149