Software and Supply Chain Risk Management Assurance Framework

Don O'Neill, Independent Consultant

Abstract. The DoD, the defense industrial base, and the nation's critical infrastructure all face challenges in Supply Chain Risk Management Assurance. These diverse challenges span infrastructure, trust, competitiveness, and austerity. Beginning with acquisition where Supply Chain foundations are laid, Supply Chain Risk Management Assurance extends into operations and sustainment.

Terms of Reference

Supply Chains are essential to global competitiveness and national security. Consequently, a Supply Chain Risk Management Assurance Framework will be produced, refined, and sustained. In addition its rollout and maturity of adoption will be measured. To encourage adoption and motivate maturity progress, appropriate public policy measures will be sought.

Supply Chains in the wild are intrinsically risky, vulnerable to Cybercrime and Cloud Computing risks as well as organizational neglect and unmet needs. The practice of risk management using smart and trusted tactics is necessary because software-based supply chains are inherently insecure, the risks and uncertainties are prolific, and vulnerabilities abound. The combination of unmet needs, industry neglect, and austerity coupled with the immature state of software, Cyber Security, and Cloud Computing infrastructure yield a rich environment of uncertainty and risk in establishing and maintaining infrastructure, being trusted, being competitive, and being austere.

The objective of rolling out the Supply Chain Risk Management Assurance Framework is to advance the assurance of smart and trusted risk management principles and practices useful and essential for military, government, critical industries, and commercial industry.

The benefit of the Supply Chain Risk Management Assurance Framework will be to elevate the expert application of risk management principles and practices in order to reduce uncertainty in the assurance of software-intensive Supply Chains through the use of smart and trusted tactics designed to deliver consequential outcomes in assuring Supply Chain trustworthiness, security, resilience, product integrity, coordination, control, and flexibility.

Specifically, adopters of the Supply Chain Risk Management Assurance Framework will be better able:

1. To systematically pinpoint the factors and sources of risk involved in Supply Chain Risk Management on software-intensive projects.

2. To identity concrete Supply Chain Risk Management objectives involved and consequential outcomes sought in meeting each of the goals associated with establishing and maintaining infrastructure, being trusted, being competitive, and being austere.

3. To visualize the operations of the Software and Supply Chain Risk Management Assurance and achievable Service Level Agreements through the use of assurance assertions based on goals and objectives and appropriate indicators, measures, metrics, and analytics.

4. To calculate Supply Chain assurance risks based on the factors evaluated for each goal, a count of factors that might serve as sources of problems in goal achievement, and a count of factors that represent objectives that are in a failed state. For each goal, the calculated risk is the number of problems divided by factors evaluated expressed as a percent.

5. To calibrate Supply Chain Risk Management Assurance rollout and maturity progress with military, government, critical infrastructure, and commercial industry peers useful in boosting brand value.

The criteria for success of the Supply Chain Risk Management Assurance Framework lies in the rate of adoption by Supply Chain owners and operators followed by their progressive advancement in Supply Chain Risk Management Assurance maturity. Five levels of maturity are envisioned spanning management, commitment, engineered flow control, process risk calculation, and global challenge strategies.

Framework Foundations

Software and Supply Chain Risk Management Assurance is the application of risk management principles and practices to reduce uncertainty in the assurance of software-intensive Supply Chains through the use of software-based smart and trusted tactics designed to deliver consequential outcomes in assuring Supply Chain trustworthiness, security, resilience, product integrity, coordination, control, and flexibility.

The purpose of the Supply Chain Risk Management Assurance Framework is not to prescribe or impose supply chain practice or methods. Instead the purpose of the Supply Chain Risk Management Assurance Framework is to encourage, stimulate, and incentivize supply chain owners and operators to positively and proactively assure the identification, mitigation, transfer, or acceptance of the sources of risk, problems, and factors that may impede the achievement of supply chain goals and objectives.

Descriptive not prescriptive, it is important to understand that the Supply Chain Risk Management Assurance Framework, by necessity, operates under three levels of indirection. First, it is a framework, a basic underlying structure. Second, it promises assurance, a positive declaration intended to inspire confidence. Third, it manages risk through the identification, elimination, mitigation, transfer, or acceptance of factors, sources of risk, and problems that may impede the achievement of supply chain goals and objectives.

1. As a framework, the Supply Chain Risk Management Assurance Framework focuses on the infrastructure of management, engineering, process, technology, and skills needed to acquire, field, and operate trusted, competitive, and austere software-based supply chains with intelligence and confidence.

2. As an assurance mechanism, the Supply Chain Risk Management Assurance Framework validates positive declarations intended to inspire confidence using assurance assertions and levels of confidence.

3. As a risk mechanism, the Supply Chain Risk Management Assurance Framework seeks to prudently assign the disposition of risks associated with factors, sources of risk, and problems and to calculate the risk associated with supply chain goals and objectives.

Setting goals is the first step in managing risk. Goals are attributes to be assured. Goals associated with smart and trusted Software and Supply Chain Risk Management Assurance include maintaining infrastructure, being trusted, being competitive, and being austere. Objectives associated with goals are factors with consequential outcomes, for example, performance, product integrity, mission, resilience, innovation, flexibility, efficiency, control, leadership, coordination, and risk. See Figure 1.

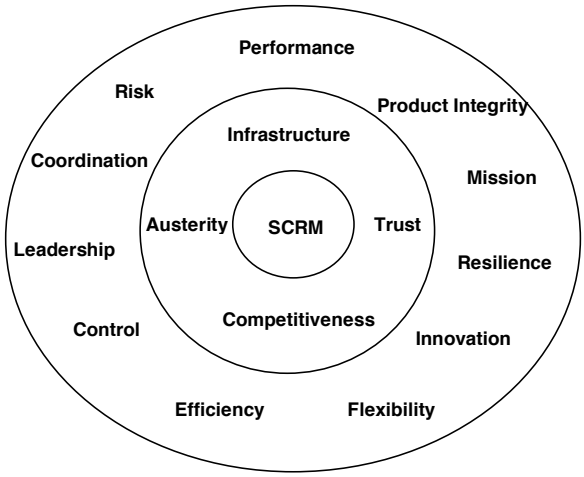

Figure 1. Strategic Goals and Tactical Objectives

Software and Supply Chain Risk Management Assurance involves the assessment of trust in the chain of custody of components, the detection of counterfeit and tainted components, and much more. The Supply Chain Risk Management Assurance Framework spans a wide range of goals, objectives, elements, issues, and factors associated with systems and software management, process, and engineering methods, practices, technologies, tools, and skills underlying acquisition and operations. See. Table 1.

Risk Management

Risk is uncertainty and the prospect for loss or gain depending on the outcome of an event. An industrial strength software risk management practice is one that treats risk as uncertainty, carefully distinguishes risks from the sources of risk and problems, and doesn't use risk management as an off ramp to avoid actually solving problems. Since risk is uncertainty, the challenge is to calculate the uncertainty of a risk and accept only those risks whose joint probability of occurrence and prospect for loss or gain are prudent choices. These are considered calculated risks.

Setting goals is the first step in managing risk. Goals are attributes to be assured. Goals associated with smart and trusted Software and Supply Chain Risk Management Assurance include maintaining infrastructure, being trusted, being competitive, and being austere. Objectives associated with goals are directed at consequential outcomes. Sources of risk are objective outcomes whose achievement is at risk and uncertain. Problems are objective outcomes that have failed. See Table 2 for a work in progress illustration.

Supply Chain assurance risk is calculated based on the factors evaluated for each goal, a count of factors that might serve as sources of problems in goal achievement, and a count of factors that represent objectives that are in a failed state. See Table 3 and Figure 2. Determining the level of confidence in assigning a failed state is assisted by evidence-based assurance assessment questions such as those in Table 4. For each goal, the calculated risk is the number of problems divided by factors evaluated expressed as a percent.

Overall Supply Chain assurance risk is determined by rule.

- R1- If infrastructure or Trust or Competitiveness or Austerity = High Risk, Then Supply Chain := High Risk

Software and Supply Chain Risk Management (SCRM) Factors	Acquisition/Operations	Goal: Infrastructure, Trust, Competitiveness, Austerity
Supply Chain Risk Management (SCRM)	Acquisition, Operations	Infrastructure
Risk Management (RM)	Acquisition, Operations	Infrastructure
Assurance Assertion Management (AAM)	Acquisition, Operations	Infrastructure
Capability Maturity Model Integration (CMMI)	Acquisition, Operations	Infrastructure
State of Austerity	Acquisition, Operations	Infrastructure, Austerity
State of Software	Acquisition, Operations	Infrastructure, Trust, Competitiveness
State of Security	Acquisition, Operations	Infrastructure, Trust
State of Cloud Security	Acquisition, Operations	Infrastructure, Trust
NIST Cloud Computing Reference Architecture (CCRA)	Acquisition, Operations	Infrastructure, Trust, Austerity
NIST Cloud Service Level Agreements (SLA)	Acquisition, Operations	Infrastructure, Trust
NIST Cyber Framework (CF)	Acquisition, Operations	Infrastructure, Trust
Cyber Tactics (CT)	Operations	Trust
Software Assurance (SA)	Acquisition, Operations	Trust
Trusted Chain of Custody (TCC)	Acquisition, Operations	Trust
Counterfeit and Tainted Component Detection (CTCD)	Acquisition, Operations	Trust
Software Product Engineering (SPE)	Acquisition	Trust
Trustworthy Software Engineering (TSE)	Acquisition	Trust
Technical Debt (TD)	Acquisition, Operations	Trust, Austerity
Software Project Management (SPM)	Acquisition	Austerity
Earned Value Management (EVM)	Acquisition	Austerity
Fixed Price Contracting (FPC)	Acquisition	Austerity
Offshore Outsourcing (OO)	Acquisition	Competitiveness, Austerity
Cost Return Ratio (CRR)	Acquisition	Competitiveness, Austerity
Next Generation Software Engineering (NGSE)	Acquisition	Competitiveness, Austerity
Frequency of Release (FR)	Acquisition, Operations	Competitiveness, Trust
Global Software Competitiveness (GSC)	Acquisition, Operations	Competitiveness
Science, Technology, Engineering, Mathematics (STEM)	Acquisition, Operations	Competitiveness
Team Innovation Management (TIM)	Acquisition	Competitiveness

Table 1. Supply Chain Risk Management Factors

- R2- If infrastructure or Trust or Competitiveness or Austerity = Moderate Risk and not High Risk, Then Supply Chain := Moderate Risk
- R3- If infrastructure and Trust and Competitiveness and Austerity = Low Risk, Then Supply Chain := Low Risk

Goal	Objective	Source of Risk	Problem	Indicator
Maintain infrastructure	SSCRM Framework Risk Management Assertion Mgt. Austerity risk Software risk Internet risk Cloud risk	SSCRM Framework Risk Management Assertion Mgt.	 Austerity risk Software risk Internet risk Cloud risk	Adoption rate Assertions met Assertions made Unmet needs Neglect, defects Incidents SLA mix
Be trusted	Reputation Build Security In Completeness Correctness Consistency Software Product Eng. Quality Technical Debt Cyber Security Cyber Tactics Trustworthiness Security Resilience Chain of Custody Counterfeit High Assurance Survivability Mission compliant	Reputation Completeness Correctness Consistency Software Product Eng. Quality Cyber Tactics Trustworthiness Chain of Custody Counterfeit High Assurance Survivability Mission compliant	Build Security In Technical Debt Cyber Security Security Resilience	Customer loyalty Vulnerabilities Defects, traceability Defects Defects Defects, Complexity Defects, complexity Neglect Incidents Defects Unmet need, defects Incidents Unmet need,Incidents Traceability Incidents Unmet need, Failures Unmet need, Failures Mission failure
Be competitive	Control work force STEM Control customers Control competition Control event threats Sustainability of wages	Control work force Control customers Control competition Sustainability of wages	 STEM Control events	Open requisitions STEM Customer satisfaction Win/loss ratio Unmet need Wage metrics
Be austere	Economics NGSE Fixed Price Software Project Mgt. Earned Value Offshore Outsourcing CMMI Cloud Computing	Economics NGSE Software Project Mgt. Earned Value Offshore Outsourcing CMMI Cloud Computing	 Fixed Price	Cost Adoption rate Adoption rate Schedule, cost var. EVM adoption rate Cost Return Ratio CMMI Maturity Level Adoption rate

Table 2. Supply Chain Risk Management, Assurance Goal, Objective, Source of Risk, Problem, and Indicator Table

Goals	Factors Evaluated	Sources of Problems	Problems	Calculated Risk	Risk by Rule
Infrastructure	7	3	4	57.7%	High
Trust	18	13	5	27.7%	Moderate
Competitiveness	6	4	2	33.3%	Moderate
Austerity	8	7	1	12.5%	Low
Supply Chain	39	27	12		High (R1)

Table 3. Calculated Risks

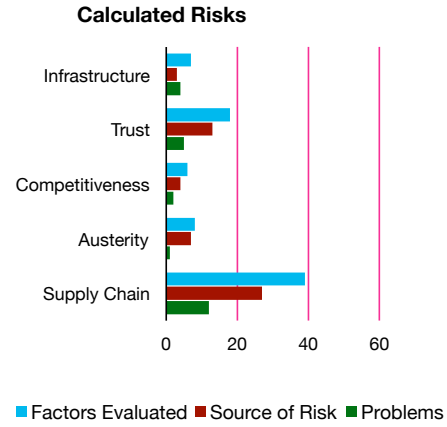

Figure 2. Calculated Risks

Specific findings:

1. Maintaining infrastructure is considered high risk due to the failed or immature state of austerity, software, Internet, and Cloud.
2. Being trusted is considered moderate risk due to the failed or immature state of Build Security In, Technical Debt, Cyber Security, Security, and Resilience.
3. Being competitive is considered moderate risk due to the failed or immature state of STEM and control of event threats.
4. Being austere is considered low risk due to the failed or immature state of fixed price contracting.

Recommendations:

1. Supply Chain success depends on maintaining an infrastructure of austerity, software, Internet, and Cloud. Very high priority attention and investment in management and engineering are recommended.

2. Supply Chain success depends on being trusted. High priority attention and investment in management, engineering, and process in the factors of Build Security In, Technical Debt, Cyber Security, Security, and Resilience are recommended.

3. Supply Chain success depends on being competitive. Priority attention and investment in STEM and control of event threats are recommended.

4. Supply Chain success depends on being austere. Attention and investment in management, engineering, and process in the factor of fixed price contracting is recommended.

Conclusion

With austerity as the context and contemporary software and security as unmet challenges, the Software and Supply Chain Risk Management Assurance Framework focuses on the infra-

Software and Supply Chain Risk Management (SCRM) Factors	Evidence-based Assurance Assertion Argument Assessment Questions
Cloud Computing (CC)	1. Has the Cloud vendor's reputation been assessed and found to be acceptable? 2. Does the Cloud vendor comply with the NIST Cloud Computing Reference Architecture (CCRA)? 3. Does the Cloud vendor accept a Service Level Agreement to protect and safeguard proprietary data and information? 4. Have the possibility and security risks of multi-tenancy been assessed and found to be acceptable?
Software Assurance (SA)	1. Are build security in practices followed? 2. Are known security vulnerabilities understood, monitored, and avoided? 3. Are known security weaknesses understood, monitored, and avoided?
Trusted Chain of Custody (TCC)	1. Is the chain of custody identified? 2. Is the accountability of permissible access maintained, updated, and reviewed? 3. Is the chain of custody unbroken? 4. Are access logs kept, maintained, and reviewed for evidence of tampering?
Counterfeit and Tainted Component Detection (CTCD)	1. Does the organization have the capability to apply Static Analysis of source code? 2. Does the organization have the capability to apply Function Extraction of object code? 3. Does the organization have the capability to apply rigorous software inspections process of source code?
Science, Technology, Engineering, Mathematics (STEM)	1. Are STEM workforce requirements known and understood? 2. Are outstanding personnel requisitions periodically reviewed by senior management? 3. Are alternate sourcing measures including offshore outsourcing identified, understood, monitored, and activated as necessary?
Offshore Outsourcing (OO)	1. Is a cost return ratio calculated during planning and recalculated periodically? 2. Are control points established for the global enterprise? 3. Are control points established for the outsource vendor? 4. Does a trusted pipe architecture feature an in-country control point connected by high speed, secure line to an out-country control point with defined capabilities and protocols. 5. Do intelligent middlemen possess necessary hard and soft skills? 6. Are outsourcing risks understood, monitored, and controlled?
Global Software Competitiveness (GSC)	1. Are suppliers understood, monitored, and controlled? 2. Are customers understood, monitored, and controlled? 3. Are competitors understood, monitored, and controlled? 4. Are event threats understood, monitored, and controlled?
Fixed Price Contracting (FPC)	1. Is the organization committed to Fixed Price Contracting? 2. Is the organization committed to systems engineering and software engineering collaboration? 3. Are software development plans structured as incremental development with well specified design levels and cost accounts? 4. Is there strict accountability of cost accounts based on a work breakdown structure? 5. Are fixed price doctrine tenets for project management, process management, and product engineering adhered to in practice?

Table 4. Examples of Evidence-based Assurance Assertion Argument Assessment Questions Useful in Determining Level of Confidence

structure of management, engineering, process, technology, and skills needed to acquire, field, and operate trusted, competitive, and austere software-based supply chains with intelligence and confidence.

Within the Software and Supply Chain Risk Management space uncertainties associated with vulnerabilities, threats, sources of risk, and problems abound. Beginning with infrastructure uncertainties including state of austerity, software, security, and Cloud Security, these uncertainties go on to include an uncertain industry state of readiness to develop and field trusted large scale software intensive systems with confidence.

Supply Chain security has emerged as a challenge calling for strategies to combat Cyber crime, economic espionage, military espionage, and Cyber warfare. Most notably the critical infrastructure needs to be trusted both with respect to economic security and public safety. What is the industry response to this challenge?

In short, Supply Chains must be trusted; Supply Chains must have integrity. Seeking trust, one approach in assuring integrity is a transparent certification regime based on a convincing demonstration and sufficient assurance assertion argument evidence. Rejecting trust, another approach in a different direction is indigenous innovation where no one trusts anyone and each country avoids foreign dependency and limits itself to domestic sourcing.

Even where trust is sought, there is the realistic acknowledgement of residual risk even in the presence of transparent, audited lifecycle processes for design, sourcing, and sustainment and the inclusion of a credible response and recovery process for event threats that may occur despite best efforts.

In conclusion, industry needs to evolve global standards for Supply Chain Risk Management Assurance. There needs to be transparency on how products are produced and distributed. Finally, flexibility must be a foremost objective so as not to stifle innovation, which is best achieved by focusing on the what not the how.

ABOUT THE AUTHOR

Don O'Neill served as the President of the Center for National Software Studies (CNSS) from 2005 to 2008. Following 27 years with IBM's Federal Systems Division (FSD), he completed a three-year residency at Carnegie Mellon University's Software Engineering Institute (SEI) under IBM's Technical Academic Career Program and has served as an SEI Visiting Scientist. A seasoned software engineering manager, technologist, independent consultant, and expert witness, he has a Bachelor of Science degree in mathematics from Dickinson College in Carlisle, Pennsylvania. His current research is directed at public policy strategies for deploying resiliency in the nation's critical infrastructure; disruptive game changing fixed price contracting tactics to achieve DoD austerity; smart and trusted tactics and practices in Supply Chain Risk Management Assurance; and a defined Software Clean Room Method for transforming a proprietary system into a Clean System devoid of proprietary information, copyrighted material, and trade secrets as well as investigating, confirming, verifying, and validating the results.

E-mail: oneilldon@aol.com

REFERENCES

1. "Hacksurfer Cybercrime Info- As Everything Becomes Outsourced, The Dangers to Business Increase", Hacksurfer, 23 September 2013
2. Sheffi, Yossi, "Supply Chain Strategy: Building a Resilient Supply Chain", Harvard Business Review, Volume 1 Number 8, October 2005
3. Goldratt, Eliyahu and Jeff Cox, "The Goals: A Process of Ongoing Improvement", North River Press, ISBN-10 0884271951, Revised Edition, June 1, 2012, 408 pages
4. Wieland, A., Wallenburg, C.M., 2012. Dealing with supply chain risks: Linking risk management practices and strategies to performance, International Journal of Physical Distribution & Logistics Management, 42(10).
5. O'Neill, Don, "Extending the Value of the CMMI to a New Normal", CrossTalk, The Journal of Defense Software Engineering, January/February 2012 <http://www.crosstalkonline.org/storage/issue-archives/2012/201201/201201-ONeill.pdf>
6. "Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness," Center for National Software Studies, May 2005, <http://www.cnsoftware.org/nss2report/NSS2FinalReport04-29-05PDF.pdf >
7. Resilient Military Systems and the Advanced Cyber Threat, Department of Defense Defense Science Board Task Force Report, January 2013
8. "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision Making", National Research Council of the National Academies, The National Academies Press, Washington DC, prepublication, 2013
9. Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, Cyberpower and National Security, National Defense University, ISBN 978-1-59797-423-3, Potomac Books, Inc., 2009, page 26
10. Badger, Lee, Tim Grance, Robert Patt-Comer, and Jeff Voss, Cloud Computing Synopsis and Recommendations, NIST Computer Security Division Special Publication SP 800-146, May 29, 2012
11. "Supply Chain Risk Management Practices for Federal Infomration Systems Organizations", Initial Oublic Draft, August 2013
12. O'Neill, Don, "Cyber Strategy, Analytics, and Tradeoffs: A Cyber Tactics Study", CrossTalk, The Journal of Defense Software Engineering, September/October 2011 <http://www.crosstalkonline.org/storage/issue-archives/2011/201109/201109-ONeill.pdf>
13. O'Neill, Don, "Peer Reviews", Encyclopedia of Software Engineering- Volume 2, Second Edition, Edited by John Marciniak, John Wiley & Sons, Inc., January 2002, pp. 929-945
14. Schulmeyer, G. Gordon, "Handbook of Software Quality Assurance", Artech House, Inc. 2008,,ISBN-13: 978-1-59693-186-2, 464 pages
15. Hevner, Alan R., Richard C. Linger, Rosann W. Collins, Mark G. Pleszkoch, Stacy J. Prowell, and Gwendolyn H. Walton, "The Impact of Function Extraction Technology on Next-Generation Software Engineering", Carnegie Mellon University CERT, CMU/SEI-2005-TR-015, July 2005
16. Wheeler, David A. and Gregory N. Larsen, "Techniques for Cyber Attribution", Institute for Defense Analysis, IDA paper P-3792, October 2003
17. Michels, William L., "Managing the Chain of Custody: Minimizing Your Risk and Exposure!", ADR America, LLC, 94th Annual International Supply Chain Conference, May 2009
18. Linger, R.C., H.D. Mills, B.I. Witt, "Structured Programming: Theory and Practice", Addison-Wesley Publishing Company, Inc., 1979
19. O'Neill, Don, "Technical Debt in the Code: Cost to Software Planning", Defense AT&L Magazine, March-April 2013 <http://www.dau.mil/pubscats/ATL%20Docs/Mar_Apr_2013/O%27Neill.pdf>
20. "Restructuring FTE Debt: The Role of Activism in a Firm", Ventureckpital, September 8, 2013
21. O'Neill, Don, "Preparing the Ground for Next Generation Software Engineering", IEEE Reliability Society, Annual Technology Report 2008, pp. 148-151, June 2009
22. O'Neill, Don, "Introduction to Global Software Competitiveness", CrossTalk, The Journal of Defense Software Engineering, Online Articles, October 2003 http://www.crosstalkonline.org/storage/issue-archives/2003/200310/200310-ONeill.pdf [Defense AT&L 12] "A Disruptive Game Changer to Achieve DOD Austerity", Defense AT&L Magazine, May-June 2012 <http://www.dau.mil/pubscats/ATL%20Docs/May_Jun_2012/O%27Neill.pdf>
23. Larman, Craig, "Agile & Iterative Development: A Manager's Guide", Pearson Education, Inc., ISBN 0-13-111155-8, 2008, 342 pages
24. O'Neill, Don, "Inside Track to Offshore Outsourcing Using the Trusted Pipe™: What Global Enterprises Look For in Offshore Outsourcing", Making the Business Case for Software Assurance Workshop, Carnegie Mellon CyLab, Pittsburgh, PA, September, 2008, pages 59-75
25. O'Neill, Don, "Team Innovation Management: Research into Practice", International Process Research Conference, Software Engineering Institute, CMU/SEI-2006-SR-001, January 2006, pages 60-71
26. Chenok, Dan, "Six Trends Driving Change in Government", IBM Center for the Business of Government, October 28, 2013 <http://www.businessofgovernment.org/blog/business-government/looking-ahead-key-challenges-and-opportunities-government>
27. Charney, Scott, Corporate Vice President, Trustworthy Computing, Microsoft, Keynote Speech at the Second Worldwide Cybersecurity Summit, London, June 2, 2011, "Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust", <http://www.youtube.com/watch?v=SEO_ieLXQ8o>
28. Goertzel, Karen Mercedes, "Integrated Circuit Security Threats and Hardware Assurance Countermeasures", CrossTalk, The Journal of Defense Software Engineering, November/December 2013 <http://www.crosstalkonline.org/storage/issue-archives/2013/201311/201311-Goertzel.pdf>
29. O'Neill, Don, "Meeting the Challenge of Assuring Resiliency Under Stress", CrossTalk, The Journal of Defense Software Engineering, September/October 2009 <http://www.crosstalkonline.org/storage/issue-archives/2009/200909/200909-ONeill.pdf>