
Bibliography

- [ACM 2008] The Association for Computing Machinery (ACM) & IEEE Computer Society (IEEE-CS). "Computer Science Curriculum 2008: An Interim Revision of CS 2001." *Computing Curriculum Series*.
<http://www.acm.org/education/curricula/ComputerScience2008.pdf>(2008).
- [ACM 2009] The Association for Computing Machinery (ACM) & IEEE Computer Society (IEEE-CS). *Software Engineering Code of Ethics and Professional Practice (Version 5.2)*. ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices (SEEPP). <http://www.acm.org/about/se-code> (2009).
- [Alberts 2009] Alberts, Christopher & Dorofee, Audrey. A Framework for Categorizing Key Drivers of Risk (CMU/SEI-2009-TR-007). Software Engineering Institute, Carnegie Mellon University, 2009.
<http://www.sei.cmu.edu/library/abstracts/reports/09tr007.cfm>
- [Alberts 2011] Alberts, Christopher J.; Dorofee, Audrey J.; Creel, Rita; Ellison, Robert J.; Woody, Carol. "A Systemic Approach for Assessing Software Supply-Chain Risk." *Proceedings of the 44th Hawaii International Conference on System Sciences*. 2011. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05718996>
- [Alberts 2012a] Alberts, Christopher; & Dorofee, Audrey. *Mission Risk Diagnostic (MRD) Method Description* (CMU/SEI-2012-TN-005). Software Engineering Institute, Carnegie Mellon University, 2012.
<http://www.sei.cmu.edu/library/abstracts/reports/12tn005.cfm>
- [Alberts 2012b] Alberts, Christopher; Allen, Julia; & Stoddard, Robert. *Risk-Based Measurement and Analysis: Application to Software Security* (CMU/SEI-2012-TN-004). Software Engineering Institute, Carnegie Mellon University, 2012.
<http://www.sei.cmu.edu/library/abstracts/reports/12tn004.cfm>
- [Allen 2001] Allen, Julia. *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley, 2001.
<http://www.sei.cmu.edu/library/abstracts/books/020173723X.cfm>
- [Allen 2008] Allen, Julia; Barnum, Sean; Ellison, Robert J.; McGraw, Gary; Mead, Nancy R. *Software Security Engineering: A Guide for Project Managers*.
<http://www.sei.cmu.edu/library/abstracts/books/032150917X.cfm> (2008).
- [Allen 2010] Allen, Julia & Davis, Nooper. *Measuring Operational Resilience Using the CERT Resilience Management Model*. (CMU/SEI-2010-TN-030) Software Engineering

- Institute, Carnegie Mellon University, 2012.
<http://www.sei.cmu.edu/library/abstracts/reports/10tn030.cfm>
- [Amazon 2011] ReplyManager and Amazon Web Services Outage Report. *Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region*. [Online] April 21, 2011. [Cited: June 28, 2011.] <http://aws.amazon.com/message/65648>
- [Ambler 2013] Ambler, Scott. *Disciplined Agile Software Development: Definition*. <http://www.agilemodeling.com/essays/agileSoftwareDevelopment.htm> (2013).
- [Anderson 2013] Anderson, John. Home Page. <http://act-r.psy.cmu.edu/people/ja/> (2013).
- [Ardis 1989] Ardis, Mark A. & Ford, Gary. *SEI Report on Graduate Software Engineering Education (1989)* (CMU/SEI-89-TR-021). Software Engineering Institute, Carnegie Mellon University, 1989.
<http://www.sei.cmu.edu/library/abstracts/reports/89tr021.cfm>
- [Aviv 2010] Aviv, Adam J.; Gibson, Katherine; Mossop, Evan; Blaze, Matt; & Smith, Jonathan M. "Smudge attacks on smartphone touch screens." *Proceedings of the 4th USENIX conference on Offensive technologies*. USENIX Association, 2010.
http://static.usenix.org/events/woot10/tech/full_papers/Aviv.pdf
- [AWWA 2012] American Water Works Association. *US warns of cyber attacks on SCADA systems*. <http://www.nyruralwater.org/news/?p=399> (2012).
- [Barman 2002] Barman, Scott. *Writing Information Security Policies*, New Riders Publishing, 2002. <http://www.informit.com/store/writing-information-security-policies-9781578702640>
- [Beckers 2012] Beckers, Kristian; Faßbender, Stephan; Heisel, Maritta; Küster, Jan-Christoph; & Schmidt, Holger. "Supporting the Development and Documentation of ISO 27001 Information Security Management Systems through Security Requirements Engineering Approaches." *Engineering Secure Software and Systems: 4th International Symposium ESSoS 2012*. Eindhoven, The Netherlands, February 2012. Springer Berlin Heidelberg, 2012.
http://link.springer.com/chapter/10.1007/978-3-642-28166-2_2
- [Bellomo 2011] Bellomo, Stephany. *A Closer Look at 804: A Summary of Considerations for DoD Program Managers* (CMU/SEI-2011-SR-015). Software Engineering Institute, Carnegie Mellon University, 2011.
<http://www.sei.cmu.edu/library/abstracts/reports/11sr015.cfm>
- [Bellomo 2012] Bellomo, Stephany & Woody, Carol. *DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers* (CMU/SEI-2012-TN-024).

Software Engineering Institute, Carnegie Mellon University, 2012.
<http://www.sei.cmu.edu/library/abstracts/reports/12tn024.cfm?wt.ac=hpLibrary>

- [Blackberry 2011] Blackberry. *Secure Element*.
<http://www.blackberry.com/developers/docs/7.0.0api/net/rim/device/api/io/nfc/se/SecureElement.html> (2011).
- [Bloom 1956] Bloom, B. S., ed. *Taxonomy of Educational Objectives: The Classification of Educational Goals: Handbook I, Cognitive Domain*. Longmans, 1956.
- [Bloomberg 2012] Bloomberg Businessweek. *Why Congress Hacked Up a Bill to Stop Hackers*.
<http://www.businessweek.com/articles/2012-11-15/why-congress-hacked-up-a-bill-to-stop-hackers> (2012).
- [Brennan 2013] Brennan, Kristin. "Managing Risk in the Software Supply Chain Through Software Code Governance," *Crosstalk, The Journal of Defense Software Engineering*, Vol. 26, No.2, USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>
- [Briney 2001] Briney, Andy. "2001 Industry Survey." *Information Security Magazine*. October, 2001.
<http://infosecuritymag.techtarget.com/articles/october01/images/survey.pdf>
- [BSIMM 2013] Building Security In Maturity Model. BSIMM4 Download.
<http://bsimm.com/download/> (2013).
- [CA 2002a] State of California. *California Civil Code Section 1798.82*
<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84> (2002).
- [CA 2002b] State of California. *California Civil Code Section 1798.29*
<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29> (2002).
- [CERT 2007] CERT. *Survivability and Information Assurance Curriculum*. Software Engineering Institute, Carnegie Mellon University. <http://www.cert.org/sia/> (2007).
- [CERT 2012] CERT. *SQUARE for Acquisition (A-SQUARE)*. <http://www.cert.org/sse/square/a-square.html> (2012).
- [CERT 2013a] CERT. *CERT Cyber Security Engineering Team Web Page*.
<http://www.cert.org/sse/> (2013).

- [CERT 2013b] CERT. CERT Secure Coding Initiative. <http://www.cert.org/secure-coding/> (2013).
- [Chabrow 2013a] Chabrow, Eric. "NIST Unveils Security, Privacy Controls." Gov Info Security, April 30 (2013). <http://www.govinfosecurity.com/interviews/nist-unveils-security-privacy-controls-i-1907?rf=2013-05-01-eg&elq=4829c4ea50ec479eb1924559e8473116&elqCampaignId=6611>
- [Chabrow 2013b] Chabrow, Eric. "South Carolina Mulls New Ways to Secure IT." Bank Info Security, May 15 (2013). <http://www.bankinfosecurity.com/south-carolina-mulls-new-ways-to-secure-it-a-5758/op-1>
- [Charette 1990] Charette, Robert N. *Application Strategies for Risk Analysis*. New York, NY: McGraw-Hill Book Company, 1990.
- [Chrissis 2013] Chrissis, Mary Beth; Konrad, Mike; & Moss, Michele. "Ensuring Your Development Processes Meet Today's Cyber Challenges," *Crosstalk, The Journal of Defense Software Engineering, Vol. 26, No.2*, USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>
- [Christiansen 2012] Christiansen, Kent. IT and the Cloud: Buy, Build or Both? Datalink, 2012. <http://www.datalink.com/media/whitepaper/Datalink%20Cloud%20Computing%20White%20Paper.pdf>
- [Clark 2002] Clark, R. A. & Schmidt, H. A. "A National Strategy to Secure Cyberspace," The President's Critical Infrastructure Protection Board, Washington, <http://georgewbush-whitehouse.archives.gov/pcipb/> (2002).
- [Claycomb 2012] Claycomb, W.R.; Nicoll, A., "Insider Threats to Cloud Computing: Directions for New Research Challenges," *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual* (July 2012) 387-394. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6340188&isnumber=6340122>
- [CNSS 2009] Committee on National Security Systems (CNSS). *Instruction No. 4009, National Information Assurance Glossary*. Revised June 2009.
- [CNSS 2010] Committee on National Security Systems Instruction (CNSSI) No. 4009, National Information Assurance Glossary, April 2010. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.
- [Croll 2012a] Croll, Paul. "Standards and Guidance for Engineering Secure Systems." Originally presented at SSTC 2012, April 2012. Available at <https://buildsecurityin.us->

[cert.gov/swa/downloads/Croll-StandardsAndGuidanceForEngineeringSecureSystems.pdf](https://www.us-cert.gov/swa/downloads/Croll-StandardsAndGuidanceForEngineeringSecureSystems.pdf).

- [Croll 2012b] Croll, Paul. "Software Sustainability – Challenges for Acquisition, Engineering and Capability Delivery in the Face of Growing Cyber Threat." Originally presented at SSTC 2012, April 2012. Available at <https://buildsecurityin.us-cert.gov/swa/downloads/Croll-Software%20Sustainability.pdf>.
- [Davidson 2013] Davidson, Don & Shankles, Stephanie. "We Cannot Blindly Reap the Benefits of a Globalized ICT Supply Chain!," *Crosstalk, The Journal of Defense Software Engineering*, Vol. 26, No.2, USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>
- [DHS 2010a] Department of Homeland Security (DHS) Software Assurance (SwA). *Build Security In*. <https://buildsecurityin.us-cert.gov/daisy/adm-bsi/home.html> (2010).
- [DHS 2010b] Department of Homeland Security (DHS) Software Assurance (SwA) Workforce Education and Training Working Group. *Software Assurance CBK/Principles Organization*. <https://buildsecurityin.us-cert.gov/bsi/dhs/927-BSI.html> (2010).
- [DHS 2012a] Department of Homeland Security. *Build Security In: Requirements Engineering*. <https://buildsecurityin.us-cert.gov/adm-bsi/articles/best-practices/requirements.html> (2012).
- [DHS 2012b] Department of Homeland Security. *Build Security In: SDLC Process*. <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc.html> (2012).
- [DHS 2013] Department of Homeland Security. *Build Security In*. <http://www.buildsecurityin.us-cert.gov> (2013).
- [Dorofee 2007] Dorofee, Audrey J.; Killcrece, Georgia; Ruele, Robin; & Zajicek, Mark. *Incident Management Capability Metrics Version 0.1*. (CMU/SEI-2007-TR-008) Software Engineering Institute, Carnegie Mellon University, 2007. <http://www.sei.cmu.edu/library/abstracts/reports/07tr008.cfm>
- [Drew 2009] Drew, Christopher. "Wanted: 'Cyber Ninjas.'" *New York Times*, December 29, 2009. <http://www.nytimes.com/2010/01/03/education/edlife/03cybersecurity.html?mc=eta1> (Accessed January 2010).
- [DSB 2000] Defense Science Board. *Report of the Defense Science Board Task Force on Defense Software*. Defense Science Board, Office of the Under Secretary of Defense (AT&L), 2000. <http://www.acq.osd.mil/dsb/reports/ADA385923.pdf>

- [DSB 2013a] Defense Science Board. *Task Force Report: Cyber Security and Reliability in a Digital Cloud*. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013.
<http://www.acq.osd.mil/dsb/reports/CyberCloud.pdf>
- [DSB 2013b] Defense Science Board. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013.
<http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>
- [DSB 2013c] Defense Science Board. *Task Force Report: Cyber Security and Reliability in a Digital Cloud*. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013.
<http://www.acq.osd.mil/dsb/reports/CyberCloud.pdf>
- [DSS 2012] Defense Security Service. *Targeting Technologies: A Trend Analysis of Reporting from Defense Industry*. Defense Security Service, Counterintelligence Directorate, 2012. <http://www.dss.mil/documents/ci/2012-unclass-trends.pdf>
- [Ellison 2008] Ellison, Robert; Goodenough, John; Weinstock, Charles; & Woody, Carol. *Survivability Assurance for System of Systems* (CMU/SEI-2008-TR-008). Software Engineering Institute, Carnegie Mellon University, 2008.
<http://www.sei.cmu.edu/library/abstracts/reports/08tr008.cfm>
- [Ellison 2010a] Ellison, Robert J.; Goodenough, John B.; Weinstock, Charles B.; & Woody, Carol. *Evaluating and Mitigating Software Supply Chain Security Risks* (CMU/SEI-2010-TN-016). Software Engineering Institute, Carnegie Mellon University, 2010.
<http://www.sei.cmu.edu/library/abstracts/reports/10tn016.cfm>
- [Ellison 2010b] Ellison, Robert; & Woody, Carol. *Survivability Analysis Framework* (CMU/SEI-2010-TN-013). Software Engineering Institute, Carnegie Mellon University, 2010. <http://www.sei.cmu.edu/library/abstracts/reports/10tn013.cfm>
- [Ellison 2010c] Ellison, Robert; Alberts, Christopher; Creel, Rita; Dorofee, Audrey; & Woody, Carol. *Software Supply Chain Risk Management: From Products to Systems of Systems* (CMU/SEI-2010-TN-026). Software Engineering Institute, Carnegie Mellon University, 2010.
<http://www.sei.cmu.edu/library/abstracts/reports/10tn026.cfm>
- [Ellison 2010d] Ellison, Robert; Goodenough, John; Weinstock, Charles; & Woody, Carol. *Evaluating and Mitigating Software Supply Chain Security Risks* (CMU/SEI-2010-TN-016). Software Engineering Institute, Carnegie Mellon University, 2010.
<http://www.sei.cmu.edu/library/abstracts/reports/10tn016.cfm>
- [ENISA 2007] European Network and Information Security Agency. *Availability and Robustness of Electronic Communications Infrastructures*.

http://www.google.com/#hl=en&output=search&client=psy-ab&q=Availability+and+Robustness+of+Electronic+Communications+Infrastructures+2007&oq=Availability+and+Robustness+of+Electronic+Communications+Infrastructures+2007&gs_l=hp.3...9381.16389.0.16786.6.6.0.0.0.0.139.675.3j3.6.0...0.0...1c.1.7.psy-ab.T684oF2VJgc&pbx=1&bav=on.2,or.r_qf.&bvm=bv.44158598,d.dmQ&fp=b01e80c1aacc47dd&biw=1244&bih=922 (2007).

- [ENISA 2009a] European Network and Information Security Agency. *Priorities for Research on Current and Emerging Network Technologies*. <http://www.ifap.ru/library/book468.pdf> (2009).
- [ENISA 2009b] European Network and Information Security Agency. *Cloud Computing: Benefits, Risks and Recommendations for Information Security*. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (2009).
- [ERAU 2010] Embry-Riddle Aeronautical University. *Master of Software Engineering Program*. <http://daytonabeach.erau.edu/degrees/graduate/software-engineering/index.html> (2010).
- [EU 1995] The European Parliament and the Council of the European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (1995).
- [EU 2009] The European Parliament and the Council of the European Union. *Directive 2002/22/EC of the European Parliament and of the Council of 22 October 2009 Concerning the the processing of personal data and the Protection of Privacy in the Electronic Communications Sector*. <http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf> (2009).
- [Fedchak 2007] Fedchak, Elaine; McGibbon, Thomas; & Vienneau, Robert. *Software Project Management for Software Assurance: DACS State of the Art Report* (DACS Report Number 347617). ITT Advanced Engineering and Sciences (prepared for Air Force Research Laboratory). September 2007.
- [Feith 2013] Feith, David. "The Weekend Interview with Timothy L. Thomas: Why China is Reading Your Email" *Wall Street Journal*, March. 30, 2013; pp. A11 (2013). <http://online.wsj.com/article/SB10001424127887323419104578376042379430724.html>

- [FIPS 2006] Federal Information Processing Standards. *Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200)*. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf> (2006).
- [Ford 1991] Ford, Gary. *SEI Report on Graduate Software Engineering Education (1991)* (CMU/SEI-91-TR-002). Software Engineering Institute, Carnegie Mellon University, 1991. <http://www.sei.cmu.edu/library/abstracts/reports/91tr002.cfm>
- [Foster 2008] I. Foster, Y. Zhau, R. Ioan, and S. Lu. "Cloud Computing and Grid Computing: 360-Degree Compared." Paper presented at the Grid Computing Environments Workshop. Austin, TX, November 16, 2008. Available at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4738445&tag=1
- [Fraser 1997] Fraser, Barbara, ed. *RFC 2196 Site Security Handbook*. Internet Engineering Task Force Network Working Group, 1997. <http://www.ietf.org/rfc/rfc2196.txt>
- [Gagliardi 2013] Gagliardi, Michael J. & Nord, Robert L. "Agile Architecting Methods for Large Scale Agile Software Development," *Software Technology Conference 2013* (April 2013). <http://sstc-online.org/Schedule/ViewPresentationInfo.cfm?abid=3053>
- [GAO 2012a] United States Government Accountability Office. *Cybersecurity: Threats Impacting the Nation (GAO-12-666T)*. <http://www.gao.gov/products/GAO-12-666T> (2012).
- [GAO 2012b] U.S. Government Accountability Office. *National Security-Related Agencies Need to Better Address Risks* (March 2012) <http://www.gao.gov/products/GAO-12-361> (2012).
- [Garfinkel 2005] Garfinkel, Simson. "History's worst software bugs." *Wired News*, Nov (2005). <http://www.wired.com/software/coolapps/news/2005/11/69355?currentPage=2>
- [Gayash 2005] Gayash, Ashwin; Viswanathan, Venkatesh; & Padmanabhan, Deepa. *SQUARE-Lite: Case Study on VADSoft Project* (CMU/SEI-2009-SR-017). Software Engineering Institute, Carnegie Mellon University, 2005. <http://www.sei.cmu.edu/library/abstracts/reports/08sr017.cfm>
- [Glorioso 2003] Glorioso, Robert. *Assured Availability of the Digital Nervous System*. <http://www.disastertolerance.com/aawhitepaper.htm> (2003).
- [Glorioso 2005] Glorioso, Robert. *Assured Availability for the Digital Nervous System: Positioning System Availability Technologies*. <http://www.disastertolerance.com/aawhitepaper.htm> (2005).

- [GMU 2012] George Mason University School of Law. *The CIP Report* (August 2012)
http://energy.gov/sites/prod/files/August2012_SmartGrid_FINAL.pdf (2012).
- [Google 2013] Google. *Secure Element Evaluation Kit for the Android Platform*.
<http://code.google.com/p/seek-for-android/> (2013).
- [GovtInfoSec 2012] “Stolen Password Led to South Carolina Tax Breach”
<http://www.govinfosecurity.com/stolen-password-led-to-south-carolina-tax-breach-a-5309/op-1>
- [Guel 2007] Guel, Michele D. *A Short Primer for Developing Security Policies*. The SANS Institute. http://www.sans.org/security-resources/policies/Policy_Primer.pdf (2007).
- [Hagen 2013a] Hagen, Christian & Sorenson, Jeff. “Delivering Military Software Affordably.”
Defense AT&L (March/April 2013).
http://www.dau.mil/pubscats/ATL%20Docs/Mar_Apr_2013/Hagen_Sorenson.pdf
- [Hagen 2013b] Hagen, Christian; Hurt, Steven; Sorenson, Jeff; Heckler, Alan; & Wall, Dan.
“Software: The Brains Behind U.S. Defense Systems.” AT Kearney, Inc (2012).
http://www.atkearney.com/documents/10192/247932/Software-The_Brains_Behind_US_Defense_Systems.pdf/69129873-eecc-4ddc-b798-c198a8ff1026
- [Hayden 2013] Hayden, Ernie. *Assumption of Breach: How a New Mindset Can Help Protect Critical Data*. TechTarget (March 2013).
<http://searchsecurity.techtarget.com/tip/Assumption-of-breach-How-a-new-mindset-can-help-protect-critical-data>
- [Hernan 2006] Hernan, Shawn; Lambert, Scott; Ostwald, Tomasz; & Shostack, Adam. “Uncover Security Design Flaws Using the STRIDE Approach” *MSDN Magazine* (November 2006). <http://msdn.microsoft.com/en-us/magazine/cc163519.aspx>
- [Hodges 2011] Hodges, J.; Jackson, C; & Barth, A. *HTTP Strict Transport Security (HSTS) draft-ietf-websec-strict-transport-sec-02*. Internet Engineering Task Force (IETF).
<http://tools.ietf.org/html/draft-ietf-websec-strict-transport-sec-02> (2011).
- [Howard 2003] Howard, M. *Fending Off Future Attacks by Reducing Attack Surface*.
<http://msdn.microsoft.com/en-us/library/ms972812.aspx> (2003).
- [Howard 2006] Howard, M. & Lipner, S. *The Security Development Lifecycle*.
<http://www.microsoft.com/learning/en/us/book.aspx?ID=8753&locale=en-us> (2006).

- [Hough 2006] Hough, Eric; Ojoko-Adams, Don; Chung, Lydia; Hung, Frank; & Mead, Nancy. *Security Quality Requirements Engineering (SQUARE): Case Study Phase III* (CMU/SEI-2006-SR-003). Software Engineering Institute, Carnegie Mellon University, 2006.
<http://www.sei.cmu.edu/library/abstracts/reports/06sr003.cfm>
- [HRG 2003] Harvard Research Group. *Availability Environment Classifications (AEC)*.
<http://www.hrgresearch.com/pdf/AEC%20Defintions.pdf> (2003).
- [Huitt 2006] Huitt, W. "The Cognitive System." *Educational Psychology Interactive*. Valdosta State University, 2006.
<http://www.edpsycinteractive.org/topics/cognition/cogsys.html> (Accessed May 22, 2008).
- [IEEE 2011] IEEE Computer Society. "Malware Infects US Military Drone System." *Computer* 44, 11 (November 2011): 15-16.
<http://www.computer.org/csdl/mags/co/2011/11/mco2011110015.pdf>
- [IEEE-CS 1998] Software & Systems Engineering Standards Committee, IEEE Computer Society. *IEEE Std. 1062, IEEE Recommended Practice for Software Acquisition*. IEEE Computer Society, 1998.
- [IEEE-CS 2008] Institute of Electrical and Electronics Engineers. *1062-1998 – IEEE Recommended Practice for Software Acquisition (ISO/IEC 1062:1998)*.
<http://standards.ieee.org/findstds/standard/1062-1998.html> (1998).
- [IEEE-CS 2004a] IEEE Computer Society (IEEE-CS) & the Association for Computing Machinery (ACM). "Computer Engineering 2004: Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering." *Computing Curriculum Series*.
http://www.acm.org/education/education/curric_vols/CE-Final-Report.pdf (2004).
- [IEEE-CS 2004b] IEEE Computer Society (IEEE-CS) & the Association for Computing Machinery (ACM). "Software Engineering 2004: Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering." *Computing Curriculum Series*.
<http://sites.computer.org/ccse/SE2004Volume.pdf> (2004).
- [IEEE-CS 2004c] IEEE Computer Society (IEEE-CS). *Software Engineering Body of Knowledge (SWEBOK)*. <http://www.computer.org/portal/web/swebok> (2004).
- [IEEE-CS 2008] Institute of Electrical and Electronics Engineers. *12207-2008 – IEEE Systems and Software Engineering—Software Life Cycle Processes (ISO/IEC 12207:2008)*.
<https://standards.ieee.org/findstds/standard/12207-2008.html> (2008). [Ingalsbe 2008] Ingalsbe, J.A.; Kunimatsu, L.; Baeten, T.; Mead, N.R. "Threat Modeling: Diving into the Deep End." *IEEE Software* (January/February 2008).

- <http://www.computer.org/csdl/mags/so/2008/01/mso2008010028-abs.html>
(2008).
- [ISO/IEC 2005] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *Information Technology—Security Techniques—Code of Practice for Information Security Management (ISO/IEC 27002:2005)*.
http://www.iso.org/iso/catalogue_detail?csnumber=50297 (2005).
- [ISO/IEC 2008] Software & Systems Engineering Standards Committee, IEEE Computer Society. *ISO/IEC 12207, IEEE Std. 12207-2008, Systems and Software Engineering - Software Life Cycle Processes, Second Edition*. IEEE Computer Society, 2008.
- [ISO/IEC/IEEE 2010] International Organization for Standardization. *Systems and Software Engineering—Vocabulary (ISO/IEC/IEEE 24765)*.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=50518 (2010).
- [iSSEc 2009] Integrated Software & Systems Engineering Curriculum (iSSEc) Project. *Graduate Software Engineering 2009 (GSWE2009) Curriculum Guidelines for Graduate Degree Programs in Software Engineering, Version 1.0*. Stevens Institute of Technology, 2009.
- [Jackson 2013] Jackson, Wayne. “Open Source and the Software Supply Chain: A Look at Risks vs. Rewards,” *Crosstalk, The Journal of Defense Software Engineering, Vol. 26, No.2*, USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>
- [Jacquith 2002] Jacquith, Andrew. “The Security of Applications: Not All Are Created Equal.” *@stake*, February 2002.
http://www.atstake.com/research/reports/acrobat/atstake_app_unequal.pdf
- [Jones 2007] Jones, Capers. “Geriatric Issues of Aging Software,” *Crosstalk, The Journal of Defense Software Engineering, Vol. 20, No. 12*, USAF Software Technology Support Center, Hill AFB, UT, December 2007. Available at <http://www.crosstalkonline.org/storage/issue-archives/2007/200712/200712-Jones.pdf>
- [Khan 2009] Khan, M. & Zulkernine, M. “On Selecting Appropriate Development Processes and Requirements Engineering Methods for Secure Software.” *Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference*. IEEE Computer Society, 2009.
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5254051>
- [Klos 2013] Klos, Steve & Richardson, John. “Software ID Tags Support Better Cyber Security,” *Crosstalk, The Journal of Defense Software Engineering, Vol. 26, No.2*,

USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>

- [Könings 2011] Könings, Bastian; Nickels, Jens; & Schaub, Florian. "Catching AuthTokens in the Wild-The Insecurity of Google's ClientLogin Protocol." <http://www.uni-ulm.de/in/mi/mi-mitarbeiter/koenings/catching-authtokens.html> (2011).
- [Krutz 2002] Krutz, Ronald; Vines, Russell. *The CISSP Prep Guide*. Wiley, 2001. <http://www.wiley.com/WileyCDA/WileyTitle/productCd-047126802X.html>
- [Kushner 2013] Kushner, David. "The Real Story of Stuxnet" IEEE Spectrum v50, n 3, pp. 48-53 (March 2013) <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- [Lapham 2006] Lapham, Mary Ann & Woody, Carol. *Sustaining Software-Intensive Systems*. (CMU/SEI-2006-TN-007) Software Engineering Institute, Carnegie Mellon University, 2006. Available at <http://www.sei.cmu.edu/library/abstracts/reports/06tn007.cfm>.
- [Lapham 2010] Lapham, Mary Ann; Williams, Ray; Hammons, Charles (Bud); Burton, Daniel; & Schenker, Alfred. *Considerations for Using Agile in DoD Acquisition* (CMU/SEI-2010-TN-002). Software Engineering Institute, Carnegie Mellon University, 2010. <http://www.sei.cmu.edu/library/abstracts/reports/10tn002.cfm>
- [Lapham 2011] Lapham, Mary Ann; Miller, Suzanne; Adams, Lorraine; Brown, Nanette; Hackemack, Bart; Hammons, Charles; Levine, Linda; & Schenker, Alfred. *Agile Methods: Selected DoD Management and Acquisition Concerns* (CMU/SEI-2011-TN-002). Software Engineering Institute, Carnegie Mellon University, 2011. <http://www.sei.cmu.edu/library/abstracts/reports/11tn002.cfm>
- [Lapham 2012a] Lapham, Mary Ann. *Using Agile Effectively in DoD Environments*. Software Engineering Institute Blog, Carnegie Mellon University. <http://blog.sei.cmu.edu/archives.cfm/author/mary-ann-lapham> (2012).
- [Lapham 2012b] Lapham, Mary Ann. "DoD Agile Adoption: Necessary Considerations, Concerns, and Changes," *CrossTalk, The Journal of Defense Software Engineering* 25, 1 (January/February 2012): 31-35. Available at <http://www.crosstalkonline.org/storage/issue-archives/2012/201201/201201-Lapham.pdf>
- [Lapham 2012c] Lapham, Mary Ann. *SEI Agile Research Forum: Agile Methods: Tools, Techniques, and Practices for the DoD Community*. Software Engineering Institute, Carnegie Mellon University. <http://www.sei.cmu.edu/library/abstracts/webinars/Tools-Techniques-and-Practices-for-the-DoD-Community.cfm> (2012).

- [Lapham 2012d] Lapham, Mary Ann & Miller, Suzanne. *Agile Acquisition*. Software Engineering Institute, Carnegie Mellon University.
<http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=7D03CB1F-9D60-C314-66526F8E8B2864B8&wtPodcast=AgileAcquisitio> (2012).
- [Larman 2013] Larman, Craig & Vodde, Bas. "Scaling Agile Development," *Crosstalk, The Journal of Defense Software Engineering*, Vol. 26, No.3, USAF Software Technology Support Center, Hill AFB, UT, May/June 2013. Available at
<http://www.crosstalkonline.org/storage/issue-archives/2013/201305/201305-Larman.pdf>
- [Lee 1960] Lee, Leonard. *The Day the Phone Stopped - How People Get Hurt When Computers Go Wrong*. New York City: Donald I Fine, Inc., 1960.
- [Lee 2013] Lee, Wenke & Rotoloni, Bo. *Emerging Cyber Threats Report 2013*. Georgia Tech Cyber Security Summit 2012, November 2012. Georgia Institute of Technology.
<http://www.gtcybersecuritysummit.com/report.html>
- [Leibs 2003] Leibs, Scott. "A Sense of Insecurity." *CFO Magazine*, March 04, 2003.
<http://www.cfo.com/article/1,5309,8841,00.html>
- [Lewis 2010] Lewis, Grace. *Basics About Cloud Computing*. Available at
<http://www.sei.cmu.edu/library/assets/whitepapers/Cloudcomputingbasics.pdf>
- [Lewis 2011] Lewis, Grace. "Architectural Implications of Cloud Computing," *SEI Technologies Forum*. Available at
www.sei.cmu.edu/library/assets/presentations/SEITECHFORUM_GL.pdf.
- [Lipner 2005] Lipner, Steve & Howard, Michael. "The Trustworthy Computing Security Development Lifecycle." <http://msdn.microsoft.com/en-us/library/ms995349.aspx> (2005).
- [Lipson 1999] Lipson, Howard, Fisher, David. "Survivability - A New Technical and Business Perspective on Security." *Proceedings of the 1999 New Security Paradigms Workshop*. Association for Computing Machinery, 1999.
<http://www.cert.org/archive/pdf/busperspec.pdf>
- [Lloyd 1999] Lloyd, Robin. "Metric mishap caused loss of NASA orbiter." CNN Interactive (1999). http://articles.cnn.com/1999-09-30/tech/9909_30_mars.metric.02_1_climate-orbiter-spacecraft-team-metric-system?_s=PM:TECH

- [LSEC 2009] Leaders in Security. "Building In ... Information Security, Privacy And Assurance." Paper presented at the Knowledge Transfer Network Paris Information Security Workshop. Paris, France, March 30, 2009.
- [Marlinspike 2011] Marlinspike, Moxie. *Blog>>sslsniff: Anniversary Edition*. Moxie Marlinspike Blog. <http://www.thoughtcrime.org/blog/sslsniff-anniversary-edition/> (2011).
- [Martin 2013] Martin, Bob. "RPI All-Stars Secure Coding Review Part 1: Organizing Your Secure Coding Efforts for Automation, Compliance, and Successful Risk Management," *Software Technology Conference 2013* (April 2013). <http://sstc-online.org/schedule/ViewPresentationInfo.cfm?abid=3164>
- [McBride 2002] McBride, Patrick, et al. *Secure Internet Practices: Best Practices for Securing System in the Internet and e-Business Age*. Boca Raton, FL: Auerbach Publications, 2002. <http://www.crcpress.com/product/isbn/9780849312397>
- [McGraw 2009a] McGraw, Gary. "Software [In]security: You Really Need a Software Security Group." *InformIT*. <http://www.informit.com/articles/article.aspx?p=1434903> (2009).
- [McGraw 2009b] McGraw, Gary; Chess, Brian; & Miguez, Sammy. "Software [In]security: The Building Security In Maturity Model (BSIMM)." *InformIT*. <http://www.informit.com/articles/article.aspx?p=1332285> (2009).
- [McGraw 2011a] McGraw, Gary. "Software [In]security: Software Security Zombies." *InformIT*. <http://www.informit.com/articles/article.aspx?p=1739924> (2011).
- [McGraw 2011b] McGraw, Gary; Chess, Brian; & Miguez, Sammy. "Software [In]security: Third-Party Software and Security." *InformIT*. <http://www.informit.com/articles/article.aspx?p=1809143> (2011).
- [McGraw 2011c] McGraw, Gary; Chess, Brian; & Miguez, Sammy. "Software [In]security: BSIMM3." *InformIT*. <http://www.informit.com/articles/article.aspx?p=1755416> (2011).
- [McGraw 2012] McGraw, Gary & Miguez, Sammy. "Software [In]security: vBSIMM Take Two (BSIMM for Vendors Revised)." *InformIT*. <http://www.informit.com/articles/article.aspx?p=1832574> (2012).
- [Mead 2005] Mead, Nancy R.; Hough, Eric; & Stehney, Ed. *Security Quality Requirements Engineering* (CMU/SEI-2005-TR-009). Software Engineering Institute, Carnegie Mellon University, 2005. <http://www.sei.cmu.edu/library/abstracts/reports/05tr009.cfm>

- [Mead 2008] Mead, Nancy R. *Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) Method*. <http://www.igi-global.com/chapter/identifying-security-requirements-using-security/23136> (2008).
- [Mead 2009a] Mead, N.R.; Shoemaker, D.; Ingalsbe, J. "Ensuring Cost Efficient and Secure Software Through Student Case Studies in Risk and Requirements Prioritization," *Hawaii International Conference on System Sciences*. Maui, Hawaii, January 2009. IEEE Computer Society, 2009.
- [Mead 2009b] Mead, N.R.; Shoemaker, D.; Ingalsbe, J., "Software Assurance Practice at Ford: A Case Study" *Crosstalk, The Journal of Defense Software Engineering, Vol. 22, No. 3*, USAF Software Technology Support Center, Hill AFB, UT, March 2009. Available at <http://www.crosstalkonline.org/storage/issue-archives/2009/200903/200903-Mead.pdf>
- [Mead 2010a] Mead, N. R. et al. *Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum*. (CMU/SEI-2010-TR-005) Software Engineering Institute, Carnegie Mellon University, 2010. Available at <http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm>.
- [Mead 2010b] Mead, Nancy R.; Hilburn, Thomas B.; & Linger, Rick. *Software Assurance Curriculum Project Volume II: Undergraduate Course Outlines* (CMU/SEI-2010-TR-019, ESC-TR-2010-019). Software Engineering Institute, Carnegie Mellon University, 2010. <http://www.sei.cmu.edu/library/abstracts/reports/10tr019.cfm>
- [Mead 2012] Mead, Nancy R.; Woody, Carol; & Shoemaker, Dan. *Foundations for Software Assurance*. Available at <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/1408-BSI.html>
- [Mell 2009] Mell, Peter & Grance, Tim. *The NIST Definition of Cloud Computing*. <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf> (2009).
- [Microsoft 2010a] Microsoft Corporation. *Microsoft Security Development Lifecycle (SDL) - Version 4.1a*. (online) <http://www.microsoft.com/downloads/details.aspx?FamilyID=d045a05a-c1fc-48c3-b4d5-b20353f97122&displaylang=en>
- [Microsoft 2010b] Microsoft Corporation. *SDL Threat Modeling Tool*. *TechNet discussion* <http://technet.microsoft.com/en-us/video/sdl-threatmodeling-tool.aspx> (2010).
- [Microsoft 2012a] Microsoft Corporation. *Microsoft Security Development Lifecycle (SDL) — version 5.2*. <http://www.microsoft.com/en-us/download/details.aspx?id=29884> (2012).

- [Microsoft 2012b] Microsoft Corporation. *Attack Surface Analyzer 1.0*. (online) August 2012. <http://blogs.msdn.com/b/sdl/archive/2012/08/02/attack-surface-analyzer-1-0-released.aspx>
- [Microsoft 2013a] Microsoft Corporation. *Security Development Lifecycle Blog*. (online) <http://blogs.msdn.com/sdl>
- [Microsoft 2013b] Microsoft Corporation. *Security Development Lifecycle Portal*. (online) <http://www.microsoft.com/sdl>
- [Microsoft 2013c] Microsoft Corporation. *Microsoft Security Development Lifecycle (SDL) – version 5.2*. (online) <http://msdn.microsoft.com/en-us/library/cc307406.aspx>
- [Microsoft 2013d] Microsoft Corporation. *Microsoft Security Development Lifecycle Tools*. (online) <http://www.microsoft.com/security/sdl/adopt/tools.aspx>
- [Microsoft 2013e] Microsoft Corporation. *Security Webcasts and Screencasts*. (online) <http://msdn.microsoft.com/en-us/security/aa570424.aspx>
- [Miller 2006] Miller, Craig. *Security Considerations in Managing COTS Software*, Cigital, Inc. 2006, Department of Homeland Security, <https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/legacy/623-BSI.html>
- [Miller 2013a] Miller, Suzanne. *Mitigating Agile Adoption Risks: Organization Climate*. Software Engineering Institute Blog, Carnegie Mellon University. <http://blog.sei.cmu.edu/archives.cfm/author/suzanne-miller> (2013).
- [Miller 2013b] Miller, Suzanne M. & Lapham, Mary Ann. "Ready & Fit: Understanding Agile Adoption Risks in DoD and Other Regulated Settings," *Software Technology Conference 2013* (April 2013). <http://sstc-online.org/Schedule/ViewPresentationInfo.cfm?abid=3115>
- [Mitre 2013a] Mitre Corporation. *CWE: Common Weakness Enumeration, a Community-Developed Dictionary of Software Weakness Types*. (online) <http://cwe.mitre.org/>
- [Mitre 2013b] Mitre Corporation. *CVE: Common Vulnerabilities & Exposures Database*. (online) <http://cve.mitre.org>
- [Montalbano 2011] Montalbano, Elizabeth. "Air Force Says Drone Virus Is No Threat." *InformationWeek*. <http://www.informationweek.com/government/security/air-force-says-drone-virus-is-no-threat/231900741>. (2011).
- [Morse 2011] Morse, Edward A.; Raval, Vasant;& Wingender, John R. Jr. "Market Price Effects of Data Security Breaches." *Information Security Journal: A Global Perspective* 20,6 (2011) 263-273.

<http://www.tandfonline.com/doi/ref/10.1080/19393555.2011.611860#tabModule>

- [Mouratidis 2007] Mouratidis, H. & Giorgini, P. *Integrating Security and Software Engineering: An Introduction (ITB13354)*. <http://www.irma-international.org/viewtitle/24048/> (2007).
- [Mouratidis 2013] Mouratidis, Haralambos. Biography. <http://www.uel.ac.uk/ace//staff/haralambosmouratidis/> (2013).
- [MSDN 2013] Microsoft Corporation. *Threat Modeling Blog*. <http://blogs.msdn.com/b/threatmodeling/> (2013).
- [NCSL 2013] National Conference of State Legislatures. *State Security Breach Notification Laws*. <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx> (2013).
- [NDIA 2008] National Defense Industrial Association. *Engineering for System Assurance* (October 2008) <http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf> (2008).
- [NIST 2003] National Institute of Standards and Technology. *Building an Information Technology Security Awareness and Training Program (NIST Special Publication 800-50)*. <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf> (2003).
- [NIST 2005] National Institute of Standards and Technology. *Creating a Patch and Vulnerability Management Program (NIST Special Publication 800-40, v2.0)*. <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf> (2005).
- [NIST 2008] National Institute of Standards and Technology. *Guidelines on Cell Phone and PDA Security*. (NIST Special Publication 800-124). <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf> (2008).
- [NIST 2009a] National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Revision 3)*. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf (2009).
- [NIST 2009b] National Institute of Standards and Technology. *Information Security Training Requirements: A Role- and Performance-Based Model DRAFT (NIST Special Publication 800-16 Revision 1 DRAFT)*. <http://csrc.nist.gov/publications/drafts/800-16-rev1/Draft-SP800-16-Rev1.pdf> (2009).

- [NIST 2009c] National Institute of Standards and Technology. *Guidelines on Firewalls and Firewall Policy (NIST Special Publication 800-41 Revision 1)*. <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf> (2009).
- [NIST 2009d] National Institute of Standards and Technology. *Recommendation for Key Management—Part 3: Application-Specific Key Management Guidance (NIST Special Publication 800-57)*. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf (2009).
- [NIST 2010a] National Institute of Standards and Technology. *Guide for Assessing the Security Controls in Federal Information Systems and Organizations (NIST Special Publication 800-53A)*. <http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf> (2010).
- [NIST 2010b] National Institute of Standards and Technology. *Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34 Revision 1)*. http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf (2010).
- [NIST 2011a] National Institute of Standards and Technology. *The NIST Definition of Cloud Computing (NIST Special Publication 800-145)*. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (2011).
- [NIST 2011b] National Institute of Standards and Technology. *Guidelines on Security and Privacy in Public Cloud Computing (NIST Special Publication 800-144)*. <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf> (2011).
- [NIST 2011c] National Institute of Standards and Technology. *DRAFT Cloud Computing Synopsis and Recommendations (NIST Special Publication 800-146)*. <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf> (2011).
- [NIST 2011d] National Institute of Standards and Technology. *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers (NIST Special Publication 800-70 Revision 2)*. <http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf> (2011).
- [NIST 2011e] National Institute of Standards and Technology. *Electronic Authentication Guideline (NIST Special Publication 800-63-1)*. <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf> (2011).
- [NIST 2012a] National Institute of Standards and Technology. *Computer Security Incident Handling Guide DRAFT (NIST Special Publication 800-61 Revision 2 DRAFT)*.

- <http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf>
(2012).
- [NIST 2012b] National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Revision 4)*. <http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf> (2012).
- [NIST 2013a] National Institute of Standards and Technology. *NIST Publications*. <http://csrc.nist.gov/publications/> (2013).
- [NIST 2013b] National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Revision 4)*. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (2013).
- [NIST 2013c] National Institute of Standards and Technology. National Vulnerability Database. <http://nvd.nist.gov/> (2013).
- [NRC 2010] Committee for Advancing Software-Intensive Systems Producibility; National Research Council. *Critical Code*. The National Academies Press, 2010.
- [NSTISS 1994] National Security Telecommunications and Information Systems Security. *National Training Standard for Information Systems Security (INFOSEC) Professionals (NSTISSI No. 4011)*. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf (1994).
- [Oltsik 2012] Oltsik, Jon. "Understanding and Addressing APTs." *BankInfoSecurity.com*. <http://www.bankinfosecurity.com/whitepapers/understanding-addressing-aptsw-658> (2012).
- [OPM 2010] U.S. Office of Personnel Management. *Federal Cyber Service: Scholarship for Service*. <http://www.nsf.gov/pubs/2012/nsf12531/nsf12531.htm> (2010).
- [OWASP 2012a] The Open Web Application Security Project. *OWASP Cloud-10 Project: Cloud Top 10 Security Risks*. https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project (2012).
- [OWASP 2012b] The Open Web Application Security Project. *OWASP Mobile Security Project – Top Ten Mobile Controls*. https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Controls (2012).

- [OWASP 2012c] The Open Web Application Security Project. *OWASP Web Services*. https://www.owasp.org/index.php/Web_Services (2012).
- [OWASP 2013] The Open Web Application Security Project. *Top 10 2013*. https://www.owasp.org/index.php/Top_10_2013 (2013).
- [Ozkaya 2013] Ozkaya, Ipek; Gagliardi, Michael; & Nord, Robert L. "Architecting for Large Scale Agile Software Development: A Risk-Driven Approach," *Crosstalk, The Journal of Defense Software Engineering, Vol. 26, No.3*, USAF Software Technology Support Center, Hill AFB, UT, May/June 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201305/201305-Ozkaya.pdf>
- [Palmer 2001] Palmer, Malcolm, et al. "Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age." *Information Systems Security*. Auerbach, May/June 2001. <http://academic.research.microsoft.com/Paper/4441193.aspx>
- [Panusuwan 2009] Panusuwan, Varokas; Batlagundu, Prashanth; & Mead, Nancy. *Privacy Risk Assessment Case Studies in Support of SQUARE (CMU/SEI-2009-SR-017)*. Software Engineering Institute, Carnegie Mellon University, 2009. <http://www.sei.cmu.edu/library/abstracts/reports/09sr017.cfm>
- [Patterson 1988] Patterson, David A; Gibson, Garth; & Katz, Randy H. "A Case for Redundant Arrays of Inexpensive Disks (RAID)," 109-116. *Proceedings of the 1988 ACM SIGMOD International Conference on Management of Data (SIGMOD 88)*. Vol. 17, Issue 3. ACM, June 1988.
- [PPS 2009] Partnership for Public Service & Booz Allen Hamilton. *Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce*. Partnership for Public Service. <http://ourpublicservice.org/OPS/publications/viewcontentdetails.php?id=135> (July 2009).
- [Redwine 2006] Redwine, S. T. ed., "Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software, Version 1.1," U.S. Department of Homeland Security, Washington, 2006.
- [Reifer 2008] Reifer, Don ; & Bryant, E. "Software Assurance in COTS and Open Source Packages," *Proceedings of the DHS Software Assurance Forum*, October 14-16, 2008.
- [Roman 2005] Roman, Jeffrey. "Encryption; A Unified Approach." *Bank Info Security*, March 26 (2013). <http://www.bankinfosecurity.com/encryption-unified-approach-a-5628/op-1>

- [Roman 2013] Roman, Jeffrey. "Using Cyber-Attacks for C-Suite Buy-In." *BankInfoSecurity.com*. <http://www.bankinfosecurity.com/using-cyber-attacks-for-c-suite-buy-in-a-5646/op-1> (2013).
- [SAFECode 2009] Software Assurance Forum for Excellence in Code. *The Software Supply Chain Integrity Framework: Defining Risk and Responsibilities for Securing Software in the Global Supply Chain*. http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf (2009).
- [SAFECode 2010] Software Assurance Forum for Excellence in Code. *Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*. http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf (2010).
- [Saltzer 1974] Saltzer, Jerome H.; & Schroeder, Michael D. "The Protection of Information in Computer Systems" *Communications of the ACM*, 17, 7, July 1974. <http://web.mit.edu/Saltzer/www/publications/protection/>
- [SANS 2013] Selected readings from the SANS Security Policy Project Website, including Guel, Michele. "A Short Primer for Developing Security Policies" *The SANS Institute*, 2013. <http://www.sans.org/resources/policies/>
- [Schmidt 2011a] Schmidt, Doug. The Growing Importance of Sustaining Software for the DoD, Part 2 SEI R&D Activities Related to Sustaining Software for the DoD, *SEI Blog*, Software Engineering Institute, Carnegie Mellon University, August 15, 2011. Available at <http://blog.sei.cmu.edu/post.cfm/the-growing-importance-of-sustaining-software-for-the-dod-1>
- [Schmidt 2011b] Schmidt, Doug. The Growing Importance of Sustaining Software for the DoD, Part 1 Software Sustainment Trends and Challenges, *SEI Blog*, Software Engineering Institute, Carnegie Mellon University, August 1, 2011. Available at <http://blog.sei.cmu.edu/post.cfm/the-growing-importance-of-sustaining-software-for-the-dod>
- [Schmidt 2012] Schmidt, Douglas C. *Agile Methods: Tools, Techniques, and Practices for the DoD Community*. Software Engineering Institute Blog, Carnegie Mellon University. <http://blog.sei.cmu.edu/post.cfm/agile-methods-tools-techniques-and-practices-for-the-dod-community> (2012).

- [Schweitzer 2009] Schweitzer, Dino; Boleng, Jeff; Hughes, Colin; & Murphy, Louis. "Visualizing Keyboard Pattern Passwords." Paper presented at the 6th International Workshop on Visualization for Cyber Security. Atlantic City, New Jersey, October 11, 2009. Available at <http://cs.wheatoncollege.edu/~mgousie/comp401/amos.pdf>
- [Seacord 2013] Seacord, Robert C. "RPI All-Stars Secure Coding Review Part 2: Secure Coding Standards and Conformance Testing," *Software Technology Conference 2013* (April 2013). <http://sstc-online.org/Schedule/ViewPresentationInfo.cfm?abid=3165>
- [SEI 2012] Software Engineering Institute. *SQUARE*. <http://www.cert.org/sse/square.html> (2012).
- [SEI 2013a] Software Engineering Institute. *The CERT Insider Threat Center*. http://www.cert.org/insider_threat/ (2013).
- [SEI 2013b] Software Engineering Institute. *SEI Mission Success in Complex Environments (CSE) Special Project*. <http://www.sei.cmu.edu/risk/> (2013).
- [Shankles 2013] Shankles, Stephanie; Moss, Michele; Pickel, Jed; & Bartol, Nadya. "How International Standard Efforts Help Address Challenges in Today's Global ICT Marketplace," *Crosstalk, The Journal of Defense Software Engineering, Vol. 26, No.2*, USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>
- [Shaw 2013] Shaw, Mary. Personal Web Page: Research. <http://spoke.compose.cs.cmu.edu/shaweb/r/research.htm> (2013).
- [Shoemaker 2013] Shoemaker, Dan & Mead, Nancy. "Building a Body of Knowledge for ICT Supply Chain Risk Management," *Crosstalk, The Journal of Defense Software Engineering, Vol. 26, No.2*, USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>
- [Shostack 2008a] Shostack, Adam. "Experiences Threat Modeling at Microsoft." Microsoft Corporation, 2008. <http://download.microsoft.com/download/9/D/3/9D389274-F770-4737-9F1A-8EA2720EE92A/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf>
- [Shostack 2008b] Shostack, Adam. "Reinvigorate Your Threat Modeling Process" *MSDN Magazine* (July 2008). <http://msdn.microsoft.com/en-us/magazine/cc700352.aspx>

- [Silowash 2012] [Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012.
<http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm>
- [Spafford 2011] Spafford, Eugene H. "Testimony before the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade." *US House of Representatives*, May 5, (2011).
- [Spectorsoft 2013] Spectorsoft Corporation. "Six Obvious Threats to Data Security You Haven't Really Addressed." *BankInfoSecurity.com*.
<http://www.bankinfosecurity.com/whitepapers/six-obvious-threats-to-data-security-you-havent-really-addressed-w-671> (2013).
- [Stephenson 1999] Stephenson, Arthur G., Daniel R. Mulville, Frank H. Bauer, Greg A. Dukeman, Peter Norvig, L. S. LaPiana, P. J. Rutledge, D. Folta, and R. Sackheim. Mars Climate Orbiter Mishap Investigation Board Phase I Report. NASA, 1999.
- [Steven 2006] Steven, John. "Adopting an Enterprise Software Security Framework." *IEEE Security & Privacy* 4, 2 (March-April 2006): 84-87. <https://buildsecurityin.us-cert.gov/daisy/bsi/resources/published/series/bsi-ieee/568.html>
- [Stewart 2013] Stewart, Roger. "Advancing SCRM with Standardized Inspection Technology," *Crosstalk, The Journal of Defense Software Engineering, Vol. 26, No.2*, USAF Software Technology Support Center, Hill AFB, UT, April 2013. Available at <http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf>
- [Swiderski 2004] Swiderski, Frank & Snyder, Window. *Threat Modeling*. Microsoft Professional, 2004.
http://www.microsoft.com/learning/en/us/book.aspx?ID=6892&locale=en-us#fbid=lu_qHhIlth
- [Symantec 2013] Symantec Connect. BugTraq Mailing List: How to Exploit & Fix Vulnerabilities. <http://www.securityfocus.com/archive/1> (2013).
- [TechTarget 2007] TechTarget Storage Media. Definition of RAID (redundant array of independent disks). <http://searchstorage.techtarget.com/definition/RAID> (2007).
- [Thompson 2013] Thompson, H. "The Human Element of Information Security." *Security & Privacy, IEEE*, 11, 1, (January/February 2013) 32-35.
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6376054&isnumber=6427803>

- [UMD 2011] University of Maryland Robert H. Smith School of Business. *The ICT SCRM Community Framework Development Project*.
http://csrc.nist.gov/scrm/documents/umd_ict_scrm_initiatives-report2-1.pdf (2011).
- [USA ASO 2011] U.S. Army, Army Software Operations, Maintenance and Sustainment Study Overview, *Software Sustainment Collaborators Workshop*, September 14, 2011.
- [USAF STSC 2003] U.S. Air Force, Software Technology Support Center, *Guidelines for Successful Acquisition and Management of Software-Intensive Systems: Weapon Systems Command and Control Systems Management Information Systems, Condensed Version*, "Chapter 16, Sustainment and Product Improvement," February 2003.
- [Verizon 2013a] Verizon. *2013 Data Breach Investigations Report*
<http://www.verizonenterprise.com/DBIR/2013/> (2013).
- [Verizon 2013b] Verizon. *2013 Data Breach Investigations Report Executive Summary*
http://www.verizonenterprise.com/resources/reports/es_data-breach-investigations-report-2013_en_xg.pdf (2013).
- [Warfield 2012] Warfield, Douglas. "Critical Infrastructures: IT Security and Threats from Private Sector Ownership." *Information Security Journal: A Global Perspective* 21,3 (2012) 127-136.
<http://www.tandfonline.com/doi/abs/10.1080/19393555.2011.652289>
- [WASC 2013] Web Application Security Consortium. WASC Web page.
<http://www.webappsec.org/> (2013).
- [Wikipedia 2013] Wikipedia. RAID. <http://en.wikipedia.org/wiki/RAID> (2013).
- [Williams 2013] Williams, Jeff. "OWASP Top Ten for 2013." Gov Info Security, May 7 (2013).
<http://www.govinfosecurity.com/blogs/top-10-app-security-risks-update-p-1465/op-1>
- [Wood 2005] Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy, Version 2*. Houston, TX: Information Shield, 2005.
http://www.informationshield.com/israr_main.htm
- [Woody 2005] Woody, Carol. "GUIDELINE 8: Information Assurance for COTS Sustainment," in Novak, W (Ed.), *Software Acquisition Planning Guidelines* (CMU/SEI-2005-HB-006) Software Engineering Institute, Carnegie Mellon University, December 2005.
- [Woody 2012] Woody, C.; Mead, N.; & Shoemaker, D. "Foundations for Software Assurance," *Hawaii International Conference on System Sciences*. Maui, Hawaii, January

2012. IEEE Computer Society, 2012. <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/1408-BSI.html>