|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  | | --- | |  | | The CSIAC IA Digest is a semi-weekly news summary for information assurance and software reliability professionals protecting the global information grid. It is transmitted in an HTML-formatted email and provides links to articles and news summaries across a spectrum of IA/SE/DIO/IW topics. ****The Cyber Security and Information Systems (CSIAC) Information Assurance Digest**** **The Cyber Security and Information Systems IAC:** The Defense Technology Information Center (DTIC) sponsors the Cyber Security & Information Systems IAC (CSIAC) for DoD. CSIAC will serve as a Center of Excellence for the DoD in Cyber Security, Software Engineering, Information Assurance, Modeling & Simulation, and Knowledge Management. Quanterion Solutions Incorporated, located in Utica, New York, operates CSIAC Basic Operations Center (BCO) for DTIC. Visit the [CSIAC](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2F77e7jx%3Fid%3D65276&url_id=dc67602324b14f6383d23ac3516e3cac17dc610e) website to learn more.  **CSIAC news:** Join the **CSIAC Subject Matter Expert Community of Practice**. The CSIAC SME Survey has been released! Readers may request participation by emailing [info@thecsiac.com](mailto:info@thecsiac.com). Recent Headlines:Cyber Security:[Government computers running Windows XP will be vulnerable to hackers after April 8](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fjzj513%3Fid%3D65276&url_id=49577c58c4fd4b720358c3e32528a0200da17a7a) - Washington Post Just in case you have not heard, and you are STILL on XP, MSFT support ends next month. No more security updates after April. Best upgrade to Vista while you still, nope, best upgrade to Win 7. [Website attack kits heighten threat from cyber criminals](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fdllmzw%3Fid%3D65276&url_id=90f41defea4008ea92210ef55413b23448a66dc0) - Financial Times According to Akamai, DDOS attacks up 370% in February, due to proliferation of DDOS attack kits. Web-based commerce most vulnerable to asymmetric attack, due to loss in sales. [NIST Issues Completed Cybersecurity Framework](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Favj0uk%3Fid%3D65276&url_id=2c63e10e12df8e8838dec279198d8d224943ad6b) - Info-Security In case you missed this last month - "The framework provides a consensus description of what's needed for a comprehensive cybersecurity program," according to Under-secretary of commerce for standards and technology and NIST, director Patrick Gallagher. Cyber Warfare:[NATO websites hit in cyber attack linked to Crimea tension](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fedh76q%3Fid%3D65276&url_id=9149d52b5eec46ea6851ae33515ca675d381b5c5) - Reuters "Cyber Berkut" hacktivists  ostensibly in Ukraine launch DDOS on [www.Nato.int](http://www.Nato.int) as well as NATO Cyber Center of Excellence in Estonia [Cyber-war: In deed and desire, Iran emerging as a major power](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fsay3sj%3Fid%3D65276&url_id=e5186ac79a41ca1efa4aee28f3d382528b6a4a88) - Christian Science Monitor Post-STUXNET Iran opting fo the cyber form of asymmetric warfare; at the tune of $1B annual government budget [Kremlin website hit by 'powerful' cyber attack](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fl547te%3Fid%3D65276&url_id=b7012b08fd7a7b18c9321afa960e949033300a40) - Sydney Morning Herald Kremlin, RU Foreign Ministry and Rossia Central Bank sites taken down by DDOS, possibly by Anonymous Russsia. Kremlin denies linkage to "the events in Ukraine" according to TASS. [Crimean govt: Referendum website downed by cyber-attack from US](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Ftcwr8f%3Fid%3D65276&url_id=182ea299479a5bebce1a114d6af68be3df9c5375) - Russia Today University of Illinois Urbana-Champaign accused of launching DDOS against Crimean Government site. More to come... SCADA:[Lockheed Martin Moves To Dominate Cyber Defense Of Electric Grid & Energy Complex](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Ff3oaj2%3Fid%3D65276&url_id=484884514bfb099c8361ebbb770497b4b35d808e) - Forbes "Industrial Defender" acquired to bolster Critical Infrastructure Protection Portfolio at Lock-Mart. [LightOut is Latest Cyber Threat to Target Energy Sector](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fir8fwz%3Fid%3D65276&url_id=2962c502e260ea7ee7fbc87fd09fc9443d8e0841) - Info-Security Late February "LightsOut" watering hole vector used to implant Energy Sector mal-ware through third party exploit. Target development is improving. Big Data and Cloud Computing:[How Big Data Analytics is Aiding Search for Flight 370](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2F9falxl%3Fid%3D65276&url_id=8cb7daed2468c4a9cf7016da577a14b7837bb102) - eWeek Adaptive Computing of Utah, home of "Moab HPC Suite " is teaming with DigitalGlobe of Colorado to offer crowssourcing search of commercial overhead imagery. Mobile Security:[Pre-installed malware turns up on new Android devices](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fxcbxpw%3Fid%3D65276&url_id=b2b9a32b586ee0b20363f97a58035c6d6e7d7c53) - InfoWorld Marble Security using static code analysis of Android and iOS application code discovers "preloaded" Netflix based malware phoning home to Russia. [Android RATs Branch out with Dendroid](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fp9xcwb%3Fid%3D65276&url_id=a7bf58f6ef0eeb43ff89dfcccc6aa7efce42dbf4) - Symantec Remote Access Toolkit (RAT) "Dendroid" sells for $300 on the darknet, can make and record calls, open apps, intercept texts. CSIAC Communities of Interest:[Systems and Software Producibility Collaboration Environment (SPRUCE)](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Flol28u%3Fid%3D65276&url_id=47792aead379491ea5fed88e4f51cdd763214010) - CSIAC SPRUCE is an online collaborative Forum for describing CS and SE challenging problems, assembling cannonical data sets, and  proposing models and solutions. CSIAC invites free use of this environment by  the academic, defense-industrial-base, and Government user community. Please Contact Tom McGibbon at [tmcgibbon@quanterion.com](mailto:tmcgibbon@quanterion.com) [The Cyber Shield Newsletter](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2F6pgqb4%3Fid%3D65276&url_id=855a6849fecd83d0124df3cc16b958fd6cb346e1) - New Mexico CounterIntelligence Working Group (NMCIWG) The Cyber Shield is a Cyber Newsletter for Counterintelligence, IT and Security Profressionals associated with DoD and USG agencies. There are Distribution constraints. If you would like to subscribe, please contact Dr. Paul Losiewicz at [plosiewicz@quanterion.com](mailto:plosiewicz@quanterion.com) [Cyber Security of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2F56ej4b%3Fid%3D65276&url_id=82454ad5a5181d5ee0e9634e721712c33c6ce31d) - Department of Homeland Security CSIAC serves on the EO 13636/PPD-21 Research & Development (R&D) Working Group (WG) run by DHS S&T. If you would like further information, contact Dr. Paul Losiewicz at [plosiewicz@quanterion.com](mailto:plosiewicz@quanterion.com) [Software Assurance Community of Practice (SwA COP)](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fspncnn%3Fid%3D65276&url_id=3703b8fc2f8a800061cf1c7becd0bb5b2d918193) - CSIAC CSIAC serves on the DoD  Software Assurance Community of Practice Working Group. For further information contact Taz Daughtrey at [hdaughtrey@quanterion.com](mailto:hdaughtrey@quanterion.com) [Systems Security Engineering Committee](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fbg1cds%3Fid%3D65276&url_id=fb1d476d2012f1292a637a904d1d1d702a005f47) - CSIAC CSIAC is serving as liaison to the National Defense Industrial Assocation's Systems Security Engineering Committee.  A 3-day Workshop in May is pending a follow-on to last year's Program Protection Plan (PPP) workshop. Point of contact is Taz Daughtrey. For more information contact [info@thecsiac.com](mailto:info@thecsiac.com) Policy Resources:[Committee on National Security Systems (CNSS)](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fpv4d5z%3Fid%3D65276&url_id=9deea5984093cd9719684621e9ee9a465dd8b91b) - Committee on National Security Systems[DHS Cyber Security Strategy ("Blueprint for a Secure Cyber Future", 2011)](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fzgsl0c%3Fid%3D65276&url_id=d6423b653fd78dee51f679f96826d8c56c8de70f) - Department of Homeland Defense[DoD COI Governance and Guidance](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2F91z59c%3Fid%3D65276&url_id=1b5938eeddd2b2872f0a2b89f0371337bd6d1ed4) - DoD Chief Information Officer[DoD IA Portal (Defense Knowledge Online)](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fqs6tw8%3Fid%3D65276&url_id=db2fdde67eb64cb8292bc2f983d32c4ea73e165d) - Department of Defense Requires CAC to access [Trustworthy CyberSpace: Strategic Plan For The Federal Cybersecurity Research and Development Program](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fj1pqa4%3Fid%3D65276&url_id=e5c716ff77e0b83a2227c315eba250bdb787e05f) - NITRD[SANS SCADA and Process Control Security Survey](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fqpgkgf%3Fid%3D65276&url_id=14a92d46b17246472f8b7bbc69c4f0e473da9171) - SANS[GAO-13-187 Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2F48fy0s%3Fid%3D65276&url_id=9033703e09d7320648ccb06547bbda4d2a3147b0) - GAO[DoD Cyber Domain Resources](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Frkrv54%3Fid%3D65276&url_id=7e3eaa3686ea6aa659373b6ca9789bf28bf40216) - DoD[CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fe35nvz%3Fid%3D65276&url_id=4e14e467bb8c6eb11f4e2c179f05a9ef94d1150a) - CSIAC Updated March 14, 2014 Guidance:[Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fkyvupy%3Fid%3D65276&url_id=a1ef20be874cd014f332caf1c26d86f8fe846ce5) - The White House White House Economic Cyberwarfare Strategy [DoD Commercial Mobile Implementation Plan](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fxb97wz%3Fid%3D65276&url_id=e8b868d5777b2edbb6f5848486249c952d1210c3) - DoD Update to DoD Mobile Device Strategy [CNSS Advisory Memorandum Information Assurance 01-12 6 June 2012](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2F74baro%3Fid%3D65276&url_id=f1494e3a4738af9af17ba0774d12dc0349289377) - CNSS NSA-Approved Commercial Solution Guidance [Bring Your Own Device](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Ffe52t9%3Fid%3D65276&url_id=661988bf551a3793382e39ae74fe7abdcc363cae) - The White House A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs - August 23, 2012. Product of the Digital Services Advisory Group and Federal Chief Information Officers Council [Department of Defense Strategy for Operating in Cyberspace](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fab1fip%3Fid%3D65276&url_id=39b58e2820932a4c74d52299342f4e4d9cb98361) - Defense.gov July 2011: DoD's five strategic initiatives [GAO February 2013 High Risk Update](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fkvqwpp%3Fid%3D65276&url_id=b135f48cf6b14ce540812559287c91f299d8f628) - GAO GAO recommends assessment of government-wide material weakness in information security be upgraded to a significant deficiency for 2 consecutive  years (p.189) [NEW! Framework for Improving Critical Infrastructure Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fpsgzhh%3Fid%3D65276&url_id=f03f011ffbabd67cb6ed358a93d84909c8d00489) - NIST National Institute of Standards and Technology (NIST) Framework published February 12th 2014 [NEW! ISO Standards on Vulnerability Handling and Disclosure](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fcm5e2t%3Fid%3D65276&url_id=61d6f77b83b11235b104f5f7f32616535e9868e9) - Internet Storm Center Two new ISO standards for vulnerability verification and reporting [NEW! DoDI 8500.01](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fykgzh7%3Fid%3D65276&url_id=d9e13d786850a7faeffd601083ef7c8df325412f) - DTIC DoDD 8500.01E (which it replaced),  DoDI 8500.02, DoDD C-5200.19, DoDI8552.01 and DTM 08-060 were all cancelled because the new DoDI 8500.01 incorporates them all. Effective 14 March 2014 [NEW! DoDI 8510.01](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fu77fxr%3Fid%3D65276&url_id=f085b2130c301f629d7170295a3a46bcd7dad2c2) - DTIC Provides procedural guidance for the reciprocal acceptance of authorization decisions and  artifacts within DoD, and between DoD and other federal agencies, for the authorization and  connection of information systems (ISs). Effective 12 March 2014 Feedback from the Last IA Digest:Most Popular:[How Big Data Could Help the U.S. Predict the Next Snowden](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fttdae2%3Fid%3D65276&url_id=e7711cf2825cc60430ee6c0c44427ee872fc06f3) - Defense One NDI James Clapper; Insider Threat;  Joint Information Environment; Data Mining; Cloud and Big Data, and World of Warcraft?  A good read... [Kaspersky Lab Uncovers "The Mask"](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fblmxq9%3Fid%3D65276&url_id=330864033665d46998fbfd26069ab5263b41dfec) - Kaspersky Labs Kaspersky claims "Mask"  or "Careto" is more sophisticated than "Duqu", uses spear-fishing to infect machines and exfiltrate data and keys [Air Force Researchers Plant Rootkit In A PLC](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fr.thecsiac.com%2Fa7prdm%3Fid%3D65276&url_id=bb756b8bfcf79da93d01f0af8d877276a6c01b60) - DarkReading Air Force Institute of Technology Center for Cyberspace Research roots Rockwell Automation Programmable Logic Controller, weak supply chain could provide vector   |  | | --- | |  | | |  | | --- | |  | | | |  | | --- | |  | |
| --- This is an automatic message from the Cyber Security and Information Systems Information Analysis Center. To unsubscribe from this email list or other CSIAC email lists, [update your subscriptions settings](http://click.thecsiac.com/track/click.php?u=30024433&id=d7d2c32215044dfdb4cdc0069b11b1ee&url=https%3A%2F%2Fwww.thecsiac.com%2Fsubscription_manager%2F%3Fid%3D65276%26e%3Dnjones%40coastline.edu&url_id=e2d71aaf8e85abedb4ce5a427d68f13387b8b641).   |  | | --- | |  | | |