|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  | | --- | |  | | 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fv9zt4x%3Fid%3D65276&url_id=fa47eeef5dae558fd2332e0ae5cb8fb0ebcc5bdd) 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:Big Data and Cloud Computing:[How Big Data Could Help the U.S. Predict the Next Snowden](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fwbejp6%3Fid%3D65276&url_id=ad6b84f84c07fce1f14e3ac8b521362a513959db) - Defense One NDI James Clapper; Insider Threat;  Joint Information Environment; Data Mining; Cloud and Big Data, and World of Warcraft?  A good read... Cyber Security:[Kaspersky Lab Uncovers "The Mask"](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F7woccg%3Fid%3D65276&url_id=9d9a47adc36c0e64c0fb18542dda9d80c5d37f67) - Kaspersky Labs Kaspersky claims "Mask"  or "Careto" is more sophisticated than "Duqu", uses spear-fishing to infect machines and exfiltrate data and keys [MtGox fallout bogs down Bitcoin traders as malleability issue goes mainstream](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F9qt75x%3Fid%3D65276&url_id=01330157aaa49e544917c17579dadd5f9f5d81e2) - The Register Transaction malleability flaw undercuts Bitcoin… more to follow [Email Attack on Vendor Set Up Breach at Target](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Flo3f1q%3Fid%3D65276&url_id=45a4c3c1af64f02a89aca4b9a718045ec4ad1e0a) - Krebson Security Email was conduit for Fazio Mechanical infection.  Possible Spear-fishing attack suspected Cyber Warfare:[Attack on US veterans website may have been aimed at military members](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fmt3lkb%3Fid%3D65276&url_id=0e4eb63feaf7816d41566ef944cf62cbc31053d1) - PCWorld More interesting, is that the VFW attack  employed a new zero-day vulnerability in I.E. 10, according to FireEye [Biggest DDoS ever aimed at Cloudflare’s content delivery network - Network Time Protocol attack reached 400Gbps](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fqrwjrz%3Fid%3D65276&url_id=e87905cebe68df805ed5c68618447afdc8b5f241) - Ars Technica Network Time Protocol reflection based  DDoS can be mitigated against, but the size of the attack set a new record Mobile Security:[Federal Workers Lax On Mobile Security](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F87midz%3Fid%3D65276&url_id=012fd504ee4b0153725777f4bcbf75c3e0314219) - Information Week "We have met the enemy, and he is us" - half of mobile device users in Government admit poor security practices SCADA:[Siemens SIMATIC WinCC OA Multiple Vulnerabilities](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Ffvvaro%3Fid%3D65276&url_id=39a797b14040403200e6d6b1c6d94a9830c9fc12) - ICS CERT SIMATIC WinCC OA  client-server human-machine interface (HMI) susceptible to "crafted" packet attacks w/o authentication [Air Force Researchers Plant Rootkit In A PLC](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F2cqhlc%3Fid%3D65276&url_id=482816f2e7f0324c423c90980fa8d9afd382a59d) - DarkReading Air Force Institute of Technology Center for Cyberspace Research roots Rockwell Automation Programmable Logic Controller, weak supply chain could provide vector CSIAC Communities of Interest:[Systems and Software Producibility Collaboration Environment (SPRUCE)](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fcs5wzv%3Fid%3D65276&url_id=a457f6f140819551326fa1084723f3c7d50f0fca) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fs9ikxc%3Fid%3D65276&url_id=8da25da629df4df66b546ebc72c2d6e1bd86a5be) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F0h5wa1%3Fid%3D65276&url_id=0f200492add9b23f7ef298471d59fd5f59c05141) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fuo4qta%3Fid%3D65276&url_id=9da798cfc0bc16d01512173275613bcab07446dc) - 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) Policy Resources:[Committee on National Security Systems (CNSS)](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fobp4d2%3Fid%3D65276&url_id=b1be2792d8e6087b2743402079e45aaa9efc5b69) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F7vsx6i%3Fid%3D65276&url_id=fc064e4a2e6961086ad0c1fe3902818472d57a8b) - Department of Homeland Defense[DoD COI Governance and Guidance](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F7b94kk%3Fid%3D65276&url_id=7ee43a0f972248ef351028b32eee3bc3f4f41a91) - DoD Chief Information Officer[DoD IA Portal (Defense Knowledge Online)](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fp9n7x5%3Fid%3D65276&url_id=4b1beaa74e9ac84a6c46d8999c25e2387189e8c7) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fvfjgkg%3Fid%3D65276&url_id=bcabdf19156662a621f348ce3d87d110d84dc521) - NITRD[SANS SCADA and Process Control Security Survey](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fw7fvcs%3Fid%3D65276&url_id=391e6e3090163a69f6d6f760670d56bd9e7677c9) - SANS[GAO-13-187 Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fnd34yy%3Fid%3D65276&url_id=8d9f8f21cb90ae5a7609ba8bfc89d4e4aa75d414) - GAO[DoD Cyber Domain Resources](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fs3mytw%3Fid%3D65276&url_id=4a992b7715244c4ae8e76445710cd9310d617843) - DoD[CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fffriso%3Fid%3D65276&url_id=8dbe5a9fbd70e56bd761745dacba800425304c6b) - CSIAC Updated February 4, 2014 Guidance:[Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fkc2jgb%3Fid%3D65276&url_id=38713881b0d709ced29c47eb454e2f34c48f1091) - The White House White House Economic Cyberwarfare Strategy [DoD Commercial Mobile Implementation Plan](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F4vala6%3Fid%3D65276&url_id=c69517071eb5c2ba04db43734ac66a1b5c7523f5) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fvddmfa%3Fid%3D65276&url_id=e0ed218fa3649444b04163e1717799bd67b43019) - CNSS NSA-Approved Commercial Solution Guidance [Bring Your Own Device](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F2faxts%3Fid%3D65276&url_id=281ce0ae7eee9c62552f9e49d1b184cd17a29669) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fvmavzv%3Fid%3D65276&url_id=eac3b566c6aafb076d81d6b90a980d814e3df55e) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F4xf95s%3Fid%3D65276&url_id=8fc8eae2aa1de7e8e77c2c9d853692b3e055fb8b) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Foltjx3%3Fid%3D65276&url_id=3eade10eddb42692c067c7ba68934c5684981915) - 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F3qnbjg%3Fid%3D65276&url_id=1662990fc15f22deb713d3d5e9e6eb8121c233c5) - Internet Storm Center Two new ISO standards for vulnerability verification and reporting Feedback from the Last IA Digest:Most Popular:[Target's point-of-sale terminals were infected with malware](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2Fotevu3%3Fid%3D65276&url_id=2ab0989c1483f44ee37dca317da825517541ecab) - ComputerWorld Point of Sale terminal malware blamed, may have been an inside job, credit card Track 1 and 2 data taken, PINs supposedly still encrypted. [Critical Backdoor in Linksys and Netgear routers found](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F2yddb7%3Fid%3D65276&url_id=b27b0b3990de41f0292ccdbe6659583783a88b27) - NetSecurity Factory reset vulnerability allows access via default admin account and password [CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fr.thecsiac.com%2F37o9gu%3Fid%3D65276&url_id=6610779382d154035e9e0ebe3a4eb832111265fd) - CSIAC Updated February 4, 2014   |  | | --- | |  | | |  | | --- | |  | | | |  | | --- | |  | |
| --- 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=0d509e3666f448ed9f7abcc1086e58e8&url=https%3A%2F%2Fwww.thecsiac.com%2Fsubscription_manager%2F%3Fid%3D65276%26e%3Dnjones%40coastline.edu&url_id=e2d71aaf8e85abedb4ce5a427d68f13387b8b641).   |  | | --- | |  | | |