|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | |  | | |  | | --- | |  |  |  |  | | --- | --- | | [Cyber Security and Information Systems Information Analysis Center](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=http%3A%2F%2FtheCSIAC.com&url_id=3df6fa9231b5b4fddc7adbfaa302377532f2b0ea) | Department of Defense Defense Technical Information Center |  |  | | --- | |  |  |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  | | --- | |  | | 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=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F19m4af%3Fid%3D65276&url_id=a479ddb0df9bfbbec3011750c48e2f920dc312dc) 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 Crime:[81 People Arrested in International Operation Against BlackShades RAT Users](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fghs8dw%3Fid%3D65276&url_id=05adf4c501bb95409388b1bffb8aa2d3d21b6fe7) - SoftPedia Interpol and European Cybercrime Centre (EC3) strike back at BlackShades Remote Access Trojan propagators in 10 countries in coordinated action. Cyber Security:[National Initiative for Cybersecurity Education (NICE) releases draft of the National Cybersecurity Workforce Framework 2.0](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F9vgtbz%3Fid%3D65276&url_id=feefcd19018b96a1fb16616dae43f18c0188e585) - NICE (22 May) The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework (the Workforce Framework) to define the cybersecurity workforce and provide a common taxonomy and lexicon by which to classify and categorize workers.  The draft of Version 2.0 is available in spreadsheet format at the NICCS portal here:  [http://niccs.us-cert.gov/research/national-cybersecurity-workforce-framework](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=http%3A%2F%2Fniccs.us-cert.gov%2Fresearch%2Fnational-cybersecurity-workforce-framework&url_id=5424ec38739dbb64adcdd3d49b8e8a087b7e3c7c) Version 1.0 is still available in interactive form here:  [http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=http%3A%2F%2Fniccs.us-cert.gov%2Ftraining%2Fnational-cybersecurity-workforce-framework&url_id=39fa65179474283864464dbf5ac38dc1ff83a637) [Heartbleed Saga Continues: Highlights of Vulnerability's First 30 Days](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Ft5cio3%3Fid%3D65276&url_id=4bce64c03384f407f0fe6c36937ca9ebf9e1fe14) - eWEEK Nice Heartbleed impact-at-a-glance review. [How the Elderwood Platform is Fueling 2014’s Zero-Day Attacks](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fwubggn%3Fid%3D65276&url_id=4c8dc9f44ce7dd441e3b7635befaade2e6bf67f8) - Symantec Elderwood resurfaces in 2014 in zero-day attacks using waterhole and spearfishing vectors. [Windows Gadget Malware](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F0wmui4%3Fid%3D65276&url_id=fd62b43638739a884fe7f6d33ea5c452a4fdc5c2) - AppRiver Trojan downloader found in Windows .gadget file - only Malwarebytes detects it. [Five Year Old Security Vulnerability Patched in LINUX Kernel](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F7g13gm%3Fid%3D65276&url_id=ae2bdfdafe5b3f24587a77fe1680ebdf2928574b) - Threatpost Another Open Source vulnerability - need more info on Android and Chrome applicability. [Vulnerability in Internet Explorer Could Allow Remote Code Execution](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fdfz7qa%3Fid%3D65276&url_id=9cd8957f4398a3ba0a73167c2eb2aaab6bcc5b37) - Microsoft In case any of you have not updated Internet Explore yet, you need to... [After Heartbleed, OpenSSL Is Forked Into LibreSSL](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fqecbuj%3Fid%3D65276&url_id=0f3b425daf3fa8a3ded3ca909841d458dba0dcb4) - eWEEK Open Source strikes back - decentralization a boost for responsiveness? Cyber Warfare:[Attorney General Eric Holder Speaks at the Press Conference Announcing U.S. Charges Against Five Chinese Military Hackers for Cyber Espionage](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F8mjpup%3Fid%3D65276&url_id=0b19e85c42a0f1c8236eff416c98f8d1300341b1) - U.S. Justice Department In unprecedented move, five Chinese Military members indicted for Industrial Cyber Espionage by DOJ. [China accuses US of hacking hypocrisy and bans Windows 8](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fm8a6yj%3Fid%3D65276&url_id=b821275cb0484cc21f0503981f0972f67c9ecff8) - ZDNet Tit-for-Tat response by China bans Windows 8 in China and freezes bilateral cyber working  group activity with U.S. Internet of Things:[The Internet of Things Will Thrive by 2025](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F4087uu%3Fid%3D65276&url_id=ae7c333c851fd5d7573dd67d6cdc8c27b25f987e) - Pew Research Cisco's projected 50 billion of connected things by 2020 will include "devices of which we have not yet conceived." [Business Adapts to a New Style of Computer](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fal4cmp%3Fid%3D65276&url_id=574fdc7f81f7cd9d46c849d9e4705852e36b09cd) - Technology Review The convergence of embedded computing, pervasive computing, and high bandwidth is leading to the Internet of Everything. Standby. Mobile Security:[F-Secure Mobile Threat Report for 2014](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fshippd%3Fid%3D65276&url_id=4a0279fb960d4ab05c1f0d916d08418b6348893e) - F-Secure Mobile security status report in a compact graphic by the Finnish security company - a good read. Network Security:[Cisco CEO: U.S. Should Reform Surveillance Rules](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fta6z5h%3Fid%3D65276&url_id=5276d4e0d3a2b4b9080135995d4dd43780574bd5) - InformationWeek Cisco CEO John Chambers denies allegations of complicity with NSA, demands Government support in security of future Internet of Things. SCADA:[SP 800-82 Rev.2 - DRAFT Guide to Industrial Control Systems (ICS) Security](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fbmbv0e%3Fid%3D65276&url_id=62061844d183c39591302bd135edb2d28321f2aa) - NIST Draft Industrial Control Systems (ICS) Guide released for review. Open Public comment period: 14 May through 18 July 2014. CSIAC Communities of Interest:[Systems and Software Producibility Collaboration Environment (SPRUCE)](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fqbpczg%3Fid%3D65276&url_id=6a80f54f7ce49c4b3574a273d3efd6f21c386448) - 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. For more information contact Tom McGibbon at [tmcgibbon@csiac.org](mailto:tmcgibbon@csiac.org) [The Cyber Shield Newsletter](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F75f00x%3Fid%3D65276&url_id=e49596e5d035ca4133e88f194bd3cb46b818bb44) - 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@csiac.org](mailto:plosiewicz@csiac.org) [Cyber Security of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fnmvjt2%3Fid%3D65276&url_id=19ed7c93d863929f5180d79ef4f3f91989b01f16) - 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@csiac.org> [Software Assurance Community of Practice (SwA COP)](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F6o8qvc%3Fid%3D65276&url_id=5739e6b7312562ed439d62aa9eca88575d018642) - CSIAC CSIAC serves on the DoD  Software Assurance Community of Practice Working Group. For further information contact Taz Daughtrey at [hdaughtrey@csiac.org](mailto:hdaughtrey@csiac.org) Technical Resources:[Common Vulnerabilities and Exposures](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fzygbwb%3Fid%3D65276&url_id=522146a4fceccd576f4ca8a6544b00a39ed00e3d) - MITRE International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE’s common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services. Policy Resources:[CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F8jttyu%3Fid%3D65276&url_id=99468d4773de7e4943d7bbc89044264dbd0f86ca) - CSIAC Updated 15 April 2014 [DoD COI Governance and Guidance](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fbv9pfb%3Fid%3D65276&url_id=7ea8ac2f3edf2d74a6ad56fbff1089d414e97dc3) - DoD Chief Information Officer[Trustworthy CyberSpace: Strategic Plan For The Federal Cybersecurity Research and Development Program](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fxok5dp%3Fid%3D65276&url_id=4b010ee4bcacba2e3132600fd2438478f6a60d75) - NITRD[DHS Cyber Security Strategy ("Blueprint for a Secure Cyber Future", 2011)](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fy6vyuc%3Fid%3D65276&url_id=4e7eeb7efeb88ed2ce517fd33e22a89c7f37b38b) - Department of Homeland Defense[Committee on National Security Systems (CNSS)](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fs4ix8i%3Fid%3D65276&url_id=b0482e1e07046c4c3fd00680106e4bf611550879) - Committee on National Security Systems[SANS SCADA and Process Control Security Survey](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Ftdhfkm%3Fid%3D65276&url_id=f3d364af3246888059d5c3fa650073f839ea1141) - SANS[DoD Cyber Domain Resources](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fo0zn73%3Fid%3D65276&url_id=d4fb45e5d69feb01a0c2583112b7a7ad0dbf38b7) - DoDGuidance:[DoDI 8500.01](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fv4ohyb%3Fid%3D65276&url_id=79b54f5672a313206a6c090baec148f3cf296f34) - 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. [DoDI 8510.01](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fg7a61m%3Fid%3D65276&url_id=89e445ffd9feea3b009cf1bea44a2a1ae4d6dd02) - 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. [GAO February 2013 High Risk Update](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fagel87%3Fid%3D65276&url_id=2395d83292edb1fc009c6b65e3b089f9500ce50e) - Government Accountability Office GAO recommends assessment of government-wide material weakness in information security be upgraded to a significant deficiency for 2 consecutive years. (p.189) [GAO-13-187 Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Flh7bro%3Fid%3D65276&url_id=a9c56000cc4a7f070792e2f2ccb7d2eef2e00759) - Government Accountability Office National strategy, roles, and responsibilities need to be better defined and more effectively implemented. [Bring Your Own Device](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fi7cmd7%3Fid%3D65276&url_id=78b7f7c1cc1cf956b2971bbe8f094cf93da370b4) - 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=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2F8a0xz8%3Fid%3D65276&url_id=2d9526f97bbb2450bac362d6cef87ed832c60a85) - Defense.gov July 2011: DoD's five strategic initiatives. [CNSS Advisory Memorandum Information Assurance 01-12 6 June 2012](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Ff5q3qw%3Fid%3D65276&url_id=0cb31f4e67b9a17bfb85806689cc86c8bc812087) - CNSS NSA-Approved Commercial Solution Guidance. [DoD Commercial Mobile Implementation Plan](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fony6s9%3Fid%3D65276&url_id=015928c20aa838930cce8793c9541b91a9a26825) - DoD Update to DoD Mobile Device Strategy. [Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fjldglw%3Fid%3D65276&url_id=eb4f5ac9b969eb99b1e24f9b44d09640593de518) - The White House White House Economic Cyberwarfare Strategy. [ISO Standards on Vulnerability Handling and Disclosure](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fefzc7f%3Fid%3D65276&url_id=deca5a6b5757ececcbb66356cdb34cead6bb1cb3) - Internet Storm Center Two new ISO standards for vulnerability verification and reporting. [Framework for Improving Critical Infrastructure Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Frsgjsv%3Fid%3D65276&url_id=ad1281191ac3e5089d31167eb60b7512574a7901) - National Institute of Standards and Technology NIST Framework published 12 February 2014. Feedback from the Last IA Digest:Most Popular:[Government computers running Windows XP will be vulnerable to hackers after April 8](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fy5lt4h%3Fid%3D65276&url_id=bb7d78c7268e5f7ffc58b4667ba51103cc9a2732) - 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. [Lockheed Martin Moves To Dominate Cyber Defense Of Electric Grid & Energy Complex](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fogbnmc%3Fid%3D65276&url_id=1a40455a892a55770f0a9cead1727943835aadcd) - Forbes "Industrial Defender" acquired to bolster Critical Infrastructure Protection Portfolio at Lock-Mart. [NIST Issues Completed Cybersecurity Framework](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fr.thecsiac.com%2Fy69r4o%3Fid%3D65276&url_id=b2f19a18a0ed9193c9b5a6578f46894cf454b244) - 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.   |  | | --- | |  | | |  | | --- | |  | | | |  | | --- | |  | |  | | --- 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=a52a52e9157645f4b89ec503dd701680&url=https%3A%2F%2Fwww.csiac.org%2Fsubscription_manager%2F%3Fid%3D65276%26e%3Dnjones%40coastline.edu&url_id=1ef4ddd5cee0ac60106b630945987a64c54642bb).   |  | | --- | |  | | |  | | |  | | --- | |  | |
| |  | | --- | | [Quanterion Solutions Incorporated.](http://click.thecsiac.com/track/click.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680&url=http%3A%2F%2Fquanterion.com%2F&url_id=3b4777036bfee2cb4a30a9e959d099db43d7151b) Copyright © 2013 811 Court Street. Utica, NY. 13502 | | | |

http://click.thecsiac.com/track/open.php?u=30024433&id=a52a52e9157645f4b89ec503dd701680