|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | |  | | |  | | --- | |  |  |  |  | | --- | --- | | [Cyber Security and Information Systems Information Analysis Center](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=http%3A%2F%2FtheCSIAC.com&url_id=3df6fa9231b5b4fddc7adbfaa302377532f2b0ea) | Department of Defense Defense Technical Information Center |  |  | | --- | |  |  |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  | | --- | |  | | ****The Cyber Security and Information Systems (CSIAC) Information Assurance Digest**** 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. Recent Headlines:Big Data & Cloud Computing:[Microsoft Makes Azure ExpressRoute Hybrid-Cloud Networking Technology Avialiable](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fe2r1ak%3Fid%3D65276&url_id=630edbee00117cfdd9d3939cc87b5d4413aced90) - Zdnet Microsoft has made its Azure ExpressRoute private-networking service available to enterprise users who want a more secure way to connect their datacenters to Microsoft's cloud. [IBM Breaks Tape Storage Record With Big Data In Mind](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fu3fyzw%3Fid%3D65276&url_id=06235a25ff5ed5877bf748d269a506aeb7dfe400) - Eweek To help handle the onslaught of big data, IBM has set a new record for storing large amounts of data on tape. Cyber-Security:[Testing Distributed Computing to Protect Against Cyberattacks On Power Grids](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F3gggvy%3Fid%3D65276&url_id=59ac19c9b34998313c156a8e58ca2f64742aa3ff) - Homeland Security News Wire The Smart America Challenge, which kicked off in late 2013 to highlight U.S. research in the field of cyberphysical systems, aims to address power grid security concerns. [Debating Disclosures of Cyber Vulnerabilities](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fl8clvh%3Fid%3D65276&url_id=4cfdd91a378495daed7d91f8f7e753d827466691) - Homeland Security News Wire Cybersecurity experts are debating whether the NSA and U.S. Cyber Command should keep cyber vulnerabilities secret, or disclose and fix them. [Homeland Security: Hackers Break into Utility's Control System](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fjrti37%3Fid%3D65276&url_id=ab400024866cb3b18a205263c5cd6d1524f2e379) - Money News A sophisticated hacking group recently attacked a U.S. public utility and compromised its control system network, but there was no evidence that the utility's operations were affected, according to the Department of Homeland Security. [Defense Authorization Bill Boosts Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F6vsngy%3Fid%3D65276&url_id=f96f00c656bc7b9bf6f4ab1bb3da753c88212266) - Docs.House.Gov Fiscal 2015 defense authorization bill that would meet the Pentagon’s $5.1 billion request for cybersecurity operations. [The Hacker Who Worked on a Navy Nuclear Aircraft Carrier](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F5taxoy%3Fid%3D65276&url_id=78442a725d9c151c3f6538731a410036d3b54e36) - The Atlantic They posted the information—with social security numbers redacted—and crowed about it on Twitter. [A Wake-up Call for SATCOM Security](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Ffa8tc7%3Fid%3D65276&url_id=5a1a597e13243d14e194fa673ad26eeff1a79120) - IO active U.S. military communication satellites vulnerable to cyberattacks. Cyber-Warfare:[DARPA's Cyber-Warfare Program Critical to Future of Kinetic Warfare](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fxg5y89%3Fid%3D65276&url_id=61dad55f45afee8e0bd73f83c9ada1fa638c6ddf) - Defense.gov Despite a year of workforce furloughs and dwindling budgets, the Defense Department’s science and technology enterprise reports advances ranging from a full hypersonic weapon system and high-energy lasers to light-based brain treatments and new core capabilities in cyber warfare, senior DOD officials told a Senate panel today. [Military Acknowledges It Will Use Cyber-Warfare](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fzgylak%3Fid%3D65276&url_id=b2c6fd1a4f40031354686958e425906bef1661f3) - The Sydney Morning Herald The Australian Defence Force has embraced cyber warfare, deception and disinformation through the internet as key elements of future military operations. [Cyber-Warfare Goes Wireless](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fc044p7%3Fid%3D65276&url_id=5f3c229fe3141ae183b5ea5f4209485d855babe3) - US News Russian forces intercepted a U.S. surveilance drone. Cyber-warfare is changing rapidly and the U.S. military has to change with it. Data Security:[Researchers Crack Supposedly Impregnable Encryption Algorithm in Two Hours](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fkqr7ih%3Fid%3D65276&url_id=f98f24b55e59d03abe631fd58fad69252068b9fb) - Homeland Security News Wire A protocol based on “discrete logarithms,” deemed as one of the candidates for the Internet’s future security systems, was decrypted by École polytechnique fédérale de Lausann (EPFL) researchers. Allegedly tamper-proof, it could only stand up to the school machines’ decryption attempts for two hours. [Major Step Toward Stronger Encryption Technology](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Ff3gage%3Fid%3D65276&url_id=c9c7bd8a1a681164f5636428e2171c3ff7795fc3) - Homeland Security News Wire Researchers the other day announced the first successful trial of Quantum Key Distribution (QKD) technology over a live “lit” fiber network. The trial paves the way for more advanced research into QKD, the next frontier of data encryption technology, which will deliver even greater levels of network security. [NIST Removes Cryptography Algorithm From Random Number Generator Recommendations](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fznnb97%3Fid%3D65276&url_id=585ea1837171b58c934a61e08d0b2ff975f05363) - CSRC.NIST NIST has removed a cryptographic algorithm from its draft guidance on random number generators. It omits an algorithm known as Dual\_EC\_DRBG, or Dual Elliptic Curve Deterministic Random Bit Generator. Network Security:[Australian Apple Devices Hacked and Held to Ransom](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F68lj6v%3Fid%3D65276&url_id=f77b7918d223d12dd3f74b9256fd460d8ffa9514) - Cnet A number of Apple users across Australia have reported having their iPhones, iPads and Macs targeted by hackers threatening to erase their data and demanding US$100 to regain access to devices. [Is the Computer 'Superbug' Killing the Anti-Virus?](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fivukz2%3Fid%3D65276&url_id=4ef5ed780b9c25b9154461f10c8dc11aeb0688a5) - Ottawa Citzen Brian Dye, senior vice-president for information security at Symantec Corp., which makes the Norton Antivirus software, said this week that today’s antivirus software is barely stopping 45 per cent of all computer system attacks, and that record is getting worse. [Ex Subway Franchise Owner Pleads Guilty to Gift Card POS Hacking Scam](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fhbfw15%3Fid%3D65276&url_id=64f837b66b1b97d3c9180756e6f0ec2e153d4d1a) - Finextra A former Subway franchise owner has admitted to remotely hacking point-of-sale terminals at the sandwich chain and topping up gift cards to the tune of $40,000. [Feds Seek to Broaden Hack Warrant Authority](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fnglp05%3Fid%3D65276&url_id=30702019203c8db28ed27ad90a7b92b0a9b5f775) - Zdnet A proposed modification to the Federal Rules of Criminal Procedure would allow a judge to issue a warrant to search computers where their physical location is unclear, or where criminal activity takes place in five or more areas. Software Reliability:['Big Code' Initiative Aims to Build Better Software](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fr1g5qq%3Fid%3D65276&url_id=a89b5717a571155809197dd09c96a9003abb35b4) - Defense Systems Darpa is attempting to take big data analytics to the next level through a "big code" project designed to improve overall software reliability through a large-scale repository of software that drives big data. [Pentagon Report Faults F-35 On Software, Reliability](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fvdzjb5%3Fid%3D65276&url_id=27bffdd8cfddef0eb7c16d3dacff960c8b54a0e0) - Reuters Ongoing software, maintenance and reliability problems with Lockheed Martin Corp's F-35 stealth fighter could delay the Marine Corps' plans to start using its F-35 jets by mid-2015. Mobile Security:[New iOS App Secures IM With 'Post Quantum' Encryption](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fv8g0xw%3Fid%3D65276&url_id=41228a234d5e162594c4900a27bc2f061dbc918c) - PQ-Chat PQChat is the world's first commercially available post-quantum messenger based on our "Never The Same" technology. Every message you send has a different encrypted output. [Defense Personnel Can Now Use Samsung Galaxy Devices On Pentagon Networks](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fy1jilz%3Fid%3D65276&url_id=d6a8e9795b6d59463afac25125e3bfa194793078) - Defense Information Systems Agency The Defense Information Systems Agency (DISA), as the lead agency for the DOD Mobility Capability, implemented its 2.0 release for Android/Samsung Knox capability under the DOD Mobility Unclassified Capability (DMUC) to mission partners May 9. [Phishing Scams Increasingly Using Mobile Apps to Bait Victims](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F81mrle%3Fid%3D65276&url_id=b9be2562053e56832e4941604c8bc75bc900bb0e) - Secure List Phishers typically use spam email to try and lure victims, but Kaspersky report says the new trend is exploiting users' love of gadgets. Info Systems & Finance:[Bitcoin Exchanges Investigated Over Possible Silk Road Links](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fj901ch%3Fid%3D65276&url_id=dcdcc37e29b9d103976ce883ab72682177d54016) - Zdnet  Reports suggest that Bitcoin exchanges including Mt. Gox are under investigation over potential ties to the online marketplace Silk Road. [Poland Gets Europe's First Biometric ATM Shared Network](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F3sklug%3Fid%3D65276&url_id=0a5f54acb44f7ce2bf584db5e3e63327a8557bea) - Finextra Polish ATM shared network Planet Cash is installing nearly 2000 machines equipped with finger vein technology, enabling users to withdraw cash without a card. [Bitcoin 101: A Primer](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fzj1y6c%3Fid%3D65276&url_id=991891c364ee2673184d1a6241f9774e1ff642f1) - Finextra The report provides an introduction to Bitcoin — what it is and how it works — the potential, the problems and the price swings. [U.S. Election Panel Approves Bitcoin Donations to Political Committees](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F4cg5ja%3Fid%3D65276&url_id=6b0d2aaa986303310a79265166cce9e5594662a4) - Federal Election Commission The U.S. Federal Election Committee said on Thursday that the virtual currency, bitcoin, could be used for donations to political action committees under certain conditions. Quantum Computing:[Forging a Qubit to Rule Them All](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fxrh7cc%3Fid%3D65276&url_id=f96619c1cf0381932edc776481a5a58f766ee707) - Simons Foundation Construction is now under way on a new information-storing device that could become the building block of a robust, scalable quantum computer. [Flipping the Switch](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Faftl7x%3Fid%3D65276&url_id=1398faa1309858b323d33d9901f4b0bd01217b9b) - Harvard Harvard researchers have succeeded in creating quantum switches that can be turned on and off using a single photon, a technological achievement that could pave the way for creating highly secure quantum networks. High Performance Computing:[How Climate Researchers Use High-Performance Computing + Big Data](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fljbfza%3Fid%3D65276&url_id=971661f2b5bd563f73dd6c3638c7dde51f479084) - Silicon AngleInternet-Of-Things:[Cisco Plugs Away At Internet-Of-Things](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F46n5g9%3Fid%3D65276&url_id=f517878d69c62d72a3fce57972f50453121b5f89) - Zdnet Cisco executives finally provide a much-needed clarification between the Internet-of-Things and the Internet-of-Everything. CSIAC Communities of Interest:[Software Assurance Community of Practice (SwA COP)](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fa3c0o1%3Fid%3D65276&url_id=4d05d6770ccc60f3d4400cb84eab689e198d0d67) - 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) [Cyber Security of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fmgg6ie%3Fid%3D65276&url_id=88e649c30e6c834f70b4609f085146f0c34834d2) - 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](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fwww.thecsiac.com%2Fresources%2Fjournals%2Fia_digest%2Fissue%2Fplosiewicz%40csiac.org&url_id=79734f2314d68b93d7bf4ba843dcdbda6e42ff4a) [The Cyber Shield Newsletter](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fu5m6wx%3Fid%3D65276&url_id=41d6c7732bdc6caab6c2c62525f1d994d374d129) - 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) [Systems and Software Producibility Collaboration Environment (SPRUCE)](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F5j3db1%3Fid%3D65276&url_id=957ef4ac2b921c14dc42ef820ea7e8227de64d63) - 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) Technical Resources:[US-CERT Bulletins](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fqrlg81%3Fid%3D65276&url_id=e699fc7be0269cefc26d9c31dc7b5d503701515f) - Department of Homeland Security Bulletins provide weekly summaries of new vulnerabilities. Patch information is provided when available. [US-CERT Alerts](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F5b5yjy%3Fid%3D65276&url_id=f78f343660ea85e4d347f57616b44609e80a48de) - Department of Homeland Security Alerts provide timely information about current security issues, vulnerabilities, and exploits. [National Vulnerability Database](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F7waqb2%3Fid%3D65276&url_id=0b90617344a76bedf7a895310ae748d349cbf572) - NIST NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. Policy Resources:[DoD Cyber Domain Resources](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F67ot5x%3Fid%3D65276&url_id=ebb6d1f9a8fe17a8f7669df9b1165821acfeebd2) - DoD[Committee on National Security Systems (CNSS)](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fj6rv79%3Fid%3D65276&url_id=3310417107835042259ecb380dcd7bb03250e049) - 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=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F4qjtyi%3Fid%3D65276&url_id=c6e49b67e99ae7d40a62eab05fc851ed05d68648) - Department of Homeland Defense[Trustworthy CyberSpace: Strategic Plan For The Federal Cybersecurity Research and Development Program](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fjwbtvq%3Fid%3D65276&url_id=a49060fe9e76629738848b9b3d1ac616338dd148) - NITRD[DoD COI Governance and Guidance](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fquzj96%3Fid%3D65276&url_id=cf61d935c5f5b5affd42c6150d4a88e351fab7ca) - DoD Chief Information Officer[CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fz9of3q%3Fid%3D65276&url_id=cf6e71dc30f01be0f4e44f61f0c0f9a313a7dda9) - CSIAC Updated 15 April 2014 Guidance:[Framework for Improving Critical Infrastructure Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F6hrj3j%3Fid%3D65276&url_id=90cecf77c7b061b419f553a7a76020f90761d45b) - National Institute of Standards and Technology NIST Framework published 12 February 2014. [ISO Standards on Vulnerability Handling and Disclosure](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2F63974g%3Fid%3D65276&url_id=418d0e0b9e6382c3689f213d74b7f5b7cfb3d09c) - Internet Storm Center Two new ISO standards for vulnerability verification and reporting. [Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fp10tzs%3Fid%3D65276&url_id=7126668f057afe51c8d27590f7ddbf8e8c16056a) - The White House White House Economic Cyberwarfare Strategy. [DoD Commercial Mobile Implementation Plan](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fsr4u2v%3Fid%3D65276&url_id=9e5a893ba641181993946ed874939a821689df46) - 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=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fckdgq7%3Fid%3D65276&url_id=4d350e0111a024e6f81cece231917fe92e8f8572) - CNSS NSA-Approved Commercial Solution Guidance. [Bring Your Own Device](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Ffgj71d%3Fid%3D65276&url_id=50db1c34b11d228c88bd2caa8ddfb05c3718e5d1) - 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. [GAO-13-187 Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fw17c2s%3Fid%3D65276&url_id=23207616ddb9d1c1404621bcc11700efa0870fea) - Government Accountability Office National strategy, roles, and responsibilities need to be better defined and more effectively implemented. [GAO February 2013 High Risk Update](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fcxv1hh%3Fid%3D65276&url_id=7f1395597c4bfc0736677df5274881ff06f7ad93) - 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) [DoDI 8510.01](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fcwbspx%3Fid%3D65276&url_id=40ba688b300807dd1fa7f3c51822978620ee07a0) - 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. [DoDI 8500.01](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fa6z23x%3Fid%3D65276&url_id=d581f46e08f50fdeee610ce0e3a91c67c7ac9586) - 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. Feedback from the last ia digest:most popular:[The Internet of Things Will Thrive by 2025](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fq6f34b%3Fid%3D65276&url_id=a64d2b965f43c0f5cf41305b58e1ae7547c30fe8) - Pew Research Cisco's projected 50 billion of connected things by 2020 will include "devices of which we have not yet conceived." [Heartbleed Saga Continues: Highlights of Vulnerability's First 30 Days](http://click.thecsiac.com/track/click.php?u=30024433&id=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fz28ynt%3Fid%3D65276&url_id=1fa234346b9e0c65b559fa06b8e0337d8ee091d4) - eWEEK Nice Heartbleed impact-at-a-glance review. [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=be2265618bab4b82be0b03d17a7ec272&url=https%3A%2F%2Fr.thecsiac.com%2Fxr06gj%3Fid%3D65276&url_id=de351fa5803296e8aab8deafca41e4f84af22fa1) - NICE 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=be2265618bab4b82be0b03d17a7ec272&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=be2265618bab4b82be0b03d17a7ec272&url=http%3A%2F%2Fniccs.us-cert.gov%2Ftraining%2Fnational-cybersecurity-workforce-framework&url_id=39fa65179474283864464dbf5ac38dc1ff83a637)   |  | | --- | |  | | |  | | --- | |  | | | |  | | --- | |  | |  | | --- 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=be2265618bab4b82be0b03d17a7ec272&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=be2265618bab4b82be0b03d17a7ec272&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=be2265618bab4b82be0b03d17a7ec272