|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|   |

 |

|  |
| --- |
|   |

|  |  |
| --- | --- |
| Cyber Security and Information Systems Information Analysis Center | Department of Defense Defense Technical Information Center |

|  |
| --- |
|   |

|  |  |
| --- | --- |
|

|  |
| --- |
|   |

 |
|

|  |  |
| --- | --- |
|

|  |
| --- |
|   |

 |
|

|  |
| --- |
|   |

 | ****The Cyber Security and Information Systems (CSIAC) Information Assurance Digest****If you would like to share your thoughts on the Information Assurance Digest or make suggestions as to what should be included, click the following link: [https://www.csiac.org/discussion/information-assurance-digest-suggestions](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fwww.csiac.org%2Fdiscussion%2Finformation-assurance-digest-suggestions&url_id=ee9674b4e4e58891bdea9373f63c784d42894682)Recent Headlines:Big Data & Cloud Computing:[IBM to Invest $3 Billion in Cloud Computing, Big Data Research](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fnxiwhj%3Fid%3D65276&url_id=50a4cc0a5264cca3eaba9603a7097ab2e2d82b65) - Washington PostIBM is investing $3 billion in research that could benefit its cloud computing and big data services, the company announced Thursday.Cyber-Security:[Senate Intelligence Committee Approves Cybersecurity Bill](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F66tk3x%3Fid%3D65276&url_id=76a7c1ad1260c954eba1efd7c64171047f9da83c) - Feinstein SenateSenate Intelligence Committee Chairman Dianne Feinstein (D-Calif.) and Vice Chairman Saxby Chambliss (R-Ga.) today announced committee approval of the Cybersecurity Information Sharing Act, a bill to improve the nation’s cybersecurity. The vote was 12-3.[FBI Found U.S. Military Aircraft Intel During Raid on Alleged Chinese Hacker](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fz8vgui%3Fid%3D65276&url_id=c9d687fe08923bac152a1a20cd6bc41c815237ee) - The RegisterA Chinese entrepreneur has been arrested for attempting to steal information on the United States' Lockheed F-22 and F-35 aircraft and Boeing's C-17 cargo plane.[Anatomy of the Attack: Zombie Zero](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fouwdje%3Fid%3D65276&url_id=d629db617c155a306f0e59dd596626a31c3e5aa1) - TrapxMalware hidden in Chinese inventory scanners targeted logistics, shipping firms.[U.S. Charges Chinese Businessman with Hacking Military Data](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F5u61fh%3Fid%3D65276&url_id=21a989052246a565eb61e1ccc1e22ec6749a061f) - ZdnetAs the cybersecurity row between the US and China escalates, another Chinese man has been arrested on hacking and data theft charges.[Chinese Hackers Pursue Key Data on U.S. Workers](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F5147yr%3Fid%3D65276&url_id=021a50d7f8a0f22307f21537b354e06b3f61fcf9) - NY TimesChinese hackers in March broke into the computer networks of the United States government agency that houses the personal information of all federal employees, according to senior American officials. [Unisys Survey Reveals Nearly 70% of Critical Infrastructure Providers Have Been Breached in the Past Year](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fgvb9uy%3Fid%3D65276&url_id=3762d23bbb106735ffac5c5103f688a42321b63c) - UnisysUtility, oil and gas, energy and manufacturing organizations unprepared for both internal and external threats, according to survey from Unisys and Ponemon Institute.Cyber-Warfare:[UK Boosts Spending on Cyber-Warfare](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fmhhpx9%3Fid%3D65276&url_id=c26ea239fcca2803bc35c1ac4959a9dd7e45aec7) - ZdnetWe don't need more tanks, we need the latest in cyber warfare, says UK PM David Cameron.Data Security:[The Case of Gyges, the Invisible Malware, Government-Grade Now in the Hands of Cybercriminals](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F1qp71j%3Fid%3D65276&url_id=0a8dde1ffb14bd1cd4f0644b8eded4c63f432791) - Sentinel LabsMalware originally developed for government espionage is now in use by criminals, who are bolting it onto their rootkits and ransomware.[Pushdo Trojan outbreak: 11 THOUSAND systems infected in just 24 hours](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F25ioxc%3Fid%3D65276&url_id=0b44431894b89ff136f0928f74091f0d76284d8d) - The RegisterA wave of attacks by cybercrooks pushing a new variant of the resilient Pushdo Trojan has compromised more than 11,000 systems in just 24 hours.["Gameover" Malware Returns From the Dead](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fb2s7zw%3Fid%3D65276&url_id=ca0a7a4b72d55be01f9eb0bd552afdea6ccc5c8f) - Naked SecuritySo far, SophosLabs has only seen a few samples of the new version, but it has been distributed through widespread spam campaigns, so the number of infections may already be large.[Security Firms Team Up and Take Down Shylock Malware](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F5q8f02%3Fid%3D65276&url_id=9692b6301cf80d0a006410b9a7d1f8f7bbf911c0) - SymantecTrojan.Shylock is designed to intercept online banking transactions and steal victims’ credentials.[Zeus PIF - The Evolving Strain Looking to Defeat Your Security Software](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fl9o6lk%3Fid%3D65276&url_id=4ecfa1df8bba51c03b61a4b58b117adb7a0d2032) - WebsenseWebsense Security Lab have identified a Zeus strain that implements information stealing procedures that appear to be an evolution of the 'DNA' of previous emerging Zeus variants.Mobile Security:[U.S. Targeted by Coercive Mobile Ransomware Impersonating the FBI](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fwd172c%3Fid%3D65276&url_id=e9e29cb6c039363be52fc80058a96e154a6da217) - LookoutLookout has discovered a highly concerning piece of malware that targets the U.S. [Google's iOS Gmail App Potential Target for Threat Actors](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Ff6syo1%3Fid%3D65276&url_id=b33eab832635d97ce08957b62b1d8a29be9d0fff) - LacoonDuring a routine analysis of the Gmail iOS app we unexpectedly came across a vulnerability which enables a threat actor that is performing a Man-in-the-Middle attack to view, and even modify, encrypted communications.Network Security:[Netgear Switches Exposed to Attacks From Hardcoded Credentials](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fkp1f77%3Fid%3D65276&url_id=4009a4ba674d38615a99d774f574b1b9961d6596) - CertA remote attacker could log into certain NETGEAR switches and execute arbitrary code because of hardcoded credentials installed within the firmware used on the devices.CSIAC Communities of Interest:[Software Assurance Community of Practice (SwA COP)](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fqla91o%3Fid%3D65276&url_id=fd69fe89536e11721fe71ed9dccd94a828a69908) - CSIACCSIAC serves on the DoD  Software Assurance Community of Practice Working Group. For further information contact Taz Daughtrey at hdaughtrey@csiac.org[The Cyber Shield Newsletter](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F0hokb5%3Fid%3D65276&url_id=43460d132bf3758d962e33c39719a8e49ef08a76) - 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[Systems and Software Producibility Collaboration Environment (SPRUCE)](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F0jkscs%3Fid%3D65276&url_id=ed2f41792376e61c5f746e9fe2c9d940301552a6) - CSIACSPRUCE 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[Cyber Security of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fwcwioq%3Fid%3D65276&url_id=419800001cc5037cbe27d8cdb8e2354c9167b38d) - Department of Homeland SecurityCSIAC 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.orgTechnical Resources:[US-CERT Bulletins](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fj2s50q%3Fid%3D65276&url_id=8c8c436582b1095b6f38f9e6ebccfb41641101c7) - Department of Homeland SecurityBulletins 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=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fegm4tq%3Fid%3D65276&url_id=35cdcf74b71d7ecd45b4acfc950b2b9a22d355b9) - Department of Homeland SecurityAlerts provide timely information about current security issues, vulnerabilities, and exploits.[National Vulnerability Database](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F63eibi%3Fid%3D65276&url_id=4723fddd7977cfff7b6dff31ce1354b9900d7206) - NISTNVD 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:[NEW CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Flsao0n%3Fid%3D65276&url_id=e777e47cfb372bb238573806aa8416e913a88c89) - CSIACUpdated 16 July 2014[DoD Cyber Domain Resources](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F8ksd72%3Fid%3D65276&url_id=df1bf929f686c2c8e40f75b3f299dc57ca4ee54e) - DoD[Trustworthy CyberSpace: Strategic Plan For The Federal Cybersecurity Research and Development Program](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Ftgmx5g%3Fid%3D65276&url_id=a4387a99172a6bc377106e4e0fcc5a58aa2a28c9) - NITRD[DoD COI Governance and Guidance](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F3qujkj%3Fid%3D65276&url_id=0e73c51b8d5dc3afc70cf7fe9350da1e804316e7) - DoD Chief Information Officer[DHS Cyber Security Strategy ("Blueprint for a Secure Cyber Future", 2011)](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fhv9he3%3Fid%3D65276&url_id=8bb2054627e4d66a6ce1fec2236d33abd1445149) - Department of Homeland Defense[Committee on National Security Systems (CNSS)](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fzwt9q5%3Fid%3D65276&url_id=23dce8503330792fe019e8582822ff541d6851dc) - Committee on National Security SystemsGuidance:[NIST announces that the Second Public Draft of Special Publication (SP) 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, has been released for public comment. (June 3, 2014)](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Faoa2gf%3Fid%3D65276&url_id=e4e13ff39ad92bf170f79d5137ec762c8f62ba25) - NISTThis document provides guidance to federal departments and agencies on identifying, assessing, and mitigating Information and Communications Technology (ICT) supply chain risks at all levels in their organizations. It integrates ICT supply chain risk management (SCRM) into federal agency enterprise risk management activities by applying a multitiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance. [DoDI 8510.01](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fe7e0g9%3Fid%3D65276&url_id=03079a9d31c75cca0db95c05a3c881d12cfc2d83) - DTICProvides 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=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fyhmrzq%3Fid%3D65276&url_id=2a0bdfd4fa6885c10aaa1e804721f6ae70bf2a44) - DTICDoDD 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.[ISO Standards on Vulnerability Handling and Disclosure](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fh9t3nd%3Fid%3D65276&url_id=d0904be6414dde09d3dedda7d2d50beeb7524387) - 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=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fdxa1zt%3Fid%3D65276&url_id=5c30cce34381905ffdead0b3fe2c1b9311ff1686) - National Institute of Standards and TechnologyNIST Framework published 12 February 2014.[GAO-13-187 Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fmjoel1%3Fid%3D65276&url_id=d496cab0efb34a91e307d46598393fad770839cf) - Government Accountability OfficeNational 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=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fyqnf2i%3Fid%3D65276&url_id=07e2f2815702f6c5d627b1a61002f596401b3dad) - Government Accountability OfficeGAO recommends assessment of government-wide material weakness in information security be upgraded to a significant deficiency for 2 consecutive years. (p.189)[Bring Your Own Device](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fcy9car%3Fid%3D65276&url_id=bcac4ef9e2e1a328ad5ce6d8e612b9a9fe84bf39) - The White HouseA 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.[CNSS Advisory Memorandum Information Assurance 01-12 6 June 2012](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fw0yms8%3Fid%3D65276&url_id=247f04448c90a6305b6e4d9f395a713ca6185d3b) - CNSSNSA-Approved Commercial Solution Guidance.[DoD Commercial Mobile Implementation Plan](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2F91fpdi%3Fid%3D65276&url_id=01dafd2a048740a94f5ea2529323cf114c038e4f) - DoDUpdate 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=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fwh3kl6%3Fid%3D65276&url_id=8315024b0bc490b083c09c371f2a0cf41b1becfe) - The White HouseWhite House Economic Cyberwarfare Strategy.Feedback from the last ia digest:most popular:[The 2014 Quadrennial Homeland Security Review](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fksdk84%3Fid%3D65276&url_id=af68c81cc9db0450d4150fa050631acfeda9d5ec) - Department of Homeland SecurityThis report provides a strong analytic and strategic foundation for one of my highest priorities, which is ensuring that the Department invests and operates in a cohesive, unified fashion and makes decisions that strengthen Departmental unity of effort. [Marked Ghost Imaging](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fkz2izx%3Fid%3D65276&url_id=3a00514ddd1dc4b8f357243c33169b4a5213cce0) - ScritationIn recent years, ghost imaging has been widely applied in various areas, such as optical security. Here, we report how an object and multiple hidden marks can be simultaneously recovered by using only one rebuilt reference intensity sequence in ghost imaging.[New Oil and Gas ISAC Opens It's Doors, Targets Cybersecurity of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=466d6dbb3d4c40cd95415494defc3c43&url=https%3A%2F%2Fr.csiac.org%2Fjyv93t%3Fid%3D65276&url_id=ca0a5153e6f506d1a5d9f64db0baf736026ed123) - ONG-ISACA secure and trusted environment for sharing cybersecurity information across the oil and natural gas industry.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.

|  |
| --- |
|   |

 |

|  |
| --- |
|   |

 |

 |

|  |
| --- |
|   |

 |  |
| ---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=466d6dbb3d4c40cd95415494defc3c43&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=466d6dbb3d4c40cd95415494defc3c43&url=http%3A%2F%2Fquanterion.com%2F&url_id=3b4777036bfee2cb4a30a9e959d099db43d7151b) Copyright © 2013811 Court Street. Utica, NY. 13502 |

 |

