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

|  |
| --- |
|   |

 |

|  |
| --- |
|   |

|  |  |
| --- | --- |
| 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.thecsiac.com/discussion/information-assurance-digest-suggestions](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fwww.thecsiac.com%2Fdiscussion%2Finformation-assurance-digest-suggestions&url_id=ad3a6abddad70d7b94e8610ecbff98df79668749)Recent Headlines:Big Data & Cloud Computing:[Cloud-Based POS Software- "New Target For Hackers"](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F4epeqc%3Fid%3D65276&url_id=ba3f354f21d814a8566d3a3d0c30761cdf976c13) - Intel CrawlerIntelCrawler, a cyber threat intelligence firm from Los Angeles, has identified new-targeted attacks on cloud-based POS software, used by grocery stores, retailers and other small businesses using web browsers like Internet Explorer, Safari, and/or Google Chrome.[Google Embraces Docker, The Next Big Thing In Cloud Computing](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fb2me4k%3Fid%3D65276&url_id=ba2ba0a9abab9debdd9535efb451ded5a8be4234) - WiredGoogle is putting its considerable weight behind an open source technology that’s already one of the hottest new ideas in the world of cloud computing.Cyber-Security:[Net Losses: Estimating the Global Cost of Cybercrime](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fu45s09%3Fid%3D65276&url_id=87364c01d36680b6c513cedc1e7bb2241c3aac7f) - McAfeeCybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion.[Operationalizing Cyber Is New Commander's Biggest Challenge](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fgkdmp8%3Fid%3D65276&url_id=fa66caafaaf40455a1953fd43b9c811e41f6347c) - Department of Defense U.S. Cyber Command’s greatest challenge is to operationalize cyberspace to turn the electro-digital network of networks into a command-and-control environment where warriors can see the adversary and whose operations defense leaders can integrate into options for commanders and policymakers.[Cyber Chief Says Businesses Must 'Own' Cyber-Security Threats](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F57qp8o%3Fid%3D65276&url_id=a37a3180a34e52e6209942b76313e3a5a7c32146) - Department of Defense Cybersecurity threats are a vital issue for the nation, and like the Defense Department, businesses must own the problem to successfully carry out their missions.[U.S. Disrupts Major Hacking, Extortion Ring; Russian Charged](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fhv5h8k%3Fid%3D65276&url_id=b62e002e2dec6a679dcb677c3cb4b5bf2ed5bbe6) - Reuters A U.S.-led international operation disrupted a crime ring that infected hundreds of thousands of PCs around the globe with malicious software used for stealing banking credentials and extorting computer owners.Cyber-Warfare:[Putter Panda Targeting U.S. Defense](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fw8yifh%3Fid%3D65276&url_id=7569e643330e39da2bbf1425b6ba767e0dd86225) - Crowd StrikePutter Panda is a determined adversary group, conducting intelligence-gathering operations targeting the Government, Defense, Research, and Technology sectors in the United States, with specific targeting of space, aerospace, and communications.[Lockheed Martin Develops Tools to Fight Viruses](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fr0dtof%3Fid%3D65276&url_id=594fea8d1623aebca3c65515489f9be5fbef0dbb) - Orlando SentinelBuoyed by tens of millions of defense dollars, Lockheed Martin Corp. has made Orlando ground zero for a "test range" to help the military develop antivirus technology to combat hacker attacks and cyber-terrorism.Data Security:[New Banker Trojan In Town: "Dyreza"](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Ft7nxkd%3Fid%3D65276&url_id=b9540315588e823825e9743120fc1697d4137c4a) - CSISA new piece of banking malware, which is targeting some major online banking services.[Zeus Alternative "Pandemiya" Emerges In Cybercrime Underground](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F7x7a1o%3Fid%3D65276&url_id=c3971249cf0223bc40974725a336f69b6f71cef6) - Security WeekA new banking Trojan being promoted in underground forums as an alternative to the popular and widely used Zeus Trojan has the potential to become a pervasive threat.[U.S. Army Loses 16,000 Personnel Records In South Korea](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fcha80f%3Fid%3D65276&url_id=1c225ca7f7002371e362225f13abffd366093597) - United States Forces KoreaUnited States Forces Korea (USFK) was made aware of a potential theft of personal information from the Korean National Recruitment System (KNRS) maintained by the U.S. Department of the Army.Mobile Security:[AT&T Confirms Serious Mobile Security Breach](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F169s0y%3Fid%3D65276&url_id=66a90b27c7727e9f2ee5250830d88d168c50a121) - SoftpediaSome AT&T customers received a letter from the company informing them that some of their details have been accessed without authorization by employees of one of their service providers.[First Seen Trojan App That Encrypts Files on Android Devices and Asks For Ransom](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fk0oaeu%3Fid%3D65276&url_id=51474c2a312ffb140d38df532c21c4dd5ebb9aec) - Virus RadarAndroid/Simplocker.A is a trojan that encrypts files on local drives. The trojan collects various sensitive information. The trojan attempts to send gathered information to a remote machine.Network Security:[Advanced Exploit Techniques Attacking the IE Script Engine](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fa1w7k2%3Fid%3D65276&url_id=6c993b2ff1b935faf70159327c614e8f031fc5c7) - FortinetExploit mitigation techniques available in Internet Explorer keep the browser strong in face of memory exploits, but attacks could be carried out through the script interpreter engine.[Six More Bugs Found In OpenSSL Security Tool and Patched](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F3xrev4%3Fid%3D65276&url_id=c8d120b56fa415dee45d38fd7a2db6b4a2a5f14a) - OpenSSLThe OpenSSL team has pushed out fixes for six security vulnerabilities in the widely used crypto library. These holes include a flaw that enables man-in-the-middle (MITM) eavesdropping on encrypted connections, and another that allows miscreants to drop malware on at-risk systems.Internet-Of-Things:[IoT Revenue to Hit $7.1 Trillion In 2020](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fiexix3%3Fid%3D65276&url_id=f965ecc6272be2523d8f9966befaf49eea38d0cb) - International Data CorporationA transformation is underway that will see the worldwide market for IoT solutions grow from $1.9 trillion in 2013 to $7.1 trillion in 2020.CSIAC Communities of Interest:[Systems and Software Producibility Collaboration Environment (SPRUCE)](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fvpvni4%3Fid%3D65276&url_id=102248672c0b86c30a4fc86f1cef3bae8d0a5e29) - 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[The Cyber Shield Newsletter](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F9eyk4t%3Fid%3D65276&url_id=765bd39b033c6b510ad92d968517e00f08b0b567) - 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[Cyber Security of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fgamjh5%3Fid%3D65276&url_id=4a9705c44b449aba46ad2bfe8b3739d8a30088fd) - 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.org](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fwww.thecsiac.com%2Fresources%2Fjournals%2Fia_digest%2Fissue%2Fplosiewicz%40csiac.org&url_id=79734f2314d68b93d7bf4ba843dcdbda6e42ff4a)[Software Assurance Community of Practice (SwA COP)](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fota5lt%3Fid%3D65276&url_id=4a76cd22b58295c9b26abeb772d1966c35f099f5) - CSIACCSIAC serves on the DoD  Software Assurance Community of Practice Working Group. For further information contact Taz Daughtrey at hdaughtrey@csiac.orgTechnical Resources:[National Vulnerability Database](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fxvu1t3%3Fid%3D65276&url_id=9f4d08bee66baf50f2536e5c0142830f54508ec4) - 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.[US-CERT Alerts](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fu6we5i%3Fid%3D65276&url_id=6b6f8a88b0c1de736b1c531b4cf11aaa33a3d8cc) - Department of Homeland SecurityAlerts provide timely information about current security issues, vulnerabilities, and exploits.[US-CERT Bulletins](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fj2ghbg%3Fid%3D65276&url_id=a508f8738adb6b90a030fba8a999a2454f57c439) - Department of Homeland SecurityBulletins provide weekly summaries of new vulnerabilities. Patch information is provided when available.Policy Resources:[CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fm6vh8k%3Fid%3D65276&url_id=704d1d5b0ad61593b73df0388570f920b4b0d75b) - CSIACUpdated 15 April 2014[DoD COI Governance and Guidance](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Ffg922e%3Fid%3D65276&url_id=abd8090dc20cad16bfb0ac3a31503eec54fed82b) - 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=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fg7phi4%3Fid%3D65276&url_id=886dbd803bc46b67f5ebc5d2877b3191bfd11201) - NITRD[DHS Cyber Security Strategy ("Blueprint for a Secure Cyber Future", 2011)](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fahrls8%3Fid%3D65276&url_id=efe38a9d797402f98ca805689d6e2235efa12ae7) - Department of Homeland Defense[Committee on National Security Systems (CNSS)](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fuohk8z%3Fid%3D65276&url_id=005c11625eccd37a1ce7cc695b52525f6a0dae2f) - Committee on National Security Systems[DoD Cyber Domain Resources](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fv1phs4%3Fid%3D65276&url_id=c72c5302b7e8aaee4be16301b718239df810d873) - DoDGuidance:[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=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fhe9ono%3Fid%3D65276&url_id=20b778836ffa0ba4765bca2b6cb965953bd7664d) - 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 8500.01](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F5fkmg1%3Fid%3D65276&url_id=215cc4fbe0633ddd0dc4a0d95fc9651706fe4197) - 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.[DoDI 8510.01](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fyolv0a%3Fid%3D65276&url_id=28391251418be539819c46a9e1b6b5dad982c430) - 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.[GAO February 2013 High Risk Update](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fxh6kzr%3Fid%3D65276&url_id=a8c8be2415d3d23af9041fa340dfec0b22da741e) - 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)[GAO-13-187 Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Feejkao%3Fid%3D65276&url_id=475fd06c7d59cf4f7cd98d47349c285a5f20a579) - Government Accountability OfficeNational 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=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fdw9jf8%3Fid%3D65276&url_id=09a493002c60bc927e4a1169964d41fe2deba3b3) - 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=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2F3fhein%3Fid%3D65276&url_id=c673abfc97cd75844d6b6cbafd7fcb6cefec45ac) - CNSSNSA-Approved Commercial Solution Guidance.[DoD Commercial Mobile Implementation Plan](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fpqm2o7%3Fid%3D65276&url_id=1b71fe05309bf7d587f3d7e2680825d04e7eeb3d) - 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=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fg88sqp%3Fid%3D65276&url_id=493f339828d114dba01145e17394033ebb4fb0ad) - The White HouseWhite House Economic Cyberwarfare Strategy.[ISO Standards on Vulnerability Handling and Disclosure](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Flf3n5i%3Fid%3D65276&url_id=a293ce9485de891c2deab52fa0cdd0f0e1ee369d) - 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=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fy9uyyg%3Fid%3D65276&url_id=25576352ca0168b4975b42406d0726a2c80e7e51) - National Institute of Standards and TechnologyNIST Framework published 12 February 2014.Feedback from the last ia digest:Most Popular:[Cyber-Warfare Goes Wireless](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fdrrk7v%3Fid%3D65276&url_id=c0ec4147ab46c249905d664cde888ed7146cdfe3) - US NewsRussian forces intercepted a U.S. surveilance drone. Cyber-warfare is changing rapidly and the U.S. military has to change with it.[A Wake-up Call for SATCOM Security](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fd09rz3%3Fid%3D65276&url_id=1c072bc26636522a9b1833783fcc3cb9de422b41) - IO activeU.S. military communication satellites vulnerable to cyberattacks.[The Hacker Who Worked on a Navy Nuclear Aircraft Carrier](http://click.thecsiac.com/track/click.php?u=30024433&id=17fe0a5a918d4a5ba8ec2da6af8651ba&url=https%3A%2F%2Fr.thecsiac.com%2Fu6kaz4%3Fid%3D65276&url_id=692c2d5f40c9e6d6382eb423ad08d02d9a724161) - The AtlanticThey posted the information—with social security numbers redacted—and crowed about it on Twitter.

|  |
| --- |
|   |

 |

|  |
| --- |
|   |

 |

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=17fe0a5a918d4a5ba8ec2da6af8651ba&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=17fe0a5a918d4a5ba8ec2da6af8651ba&url=http%3A%2F%2Fquanterion.com%2F&url_id=3b4777036bfee2cb4a30a9e959d099db43d7151b) Copyright © 2013811 Court Street. Utica, NY. 13502 |

 |

