[redacted]

[redacted] Cyber-Threat Newsletter – 16 May 16

(b)(3) 10 USC ⊥ 424

Patches & Updates of the Week:

(U) 0day alert: Be ready to update Adobe Flash Player tomorrow

(U) On Tuesday, Adobe has pushed out security updates for Cold Fusion and Adobe Acrobat and Reader, but has also announced an update for Flash Player that should be released on Thursday and will fix a zero-day flaw (CVE-2016-4117) that's being actively exploited in attacks in the wild. What kind of attacks? Adobe didn't say. But the vulnerability is considered to be critical, as successful exploitation could cause a crash and potentially allow an attacker to take control of the affected system. It affects Adobe Flash Player 21.0.0.226 and earlier versions for Windows, Macintosh, Linux, and Chrome OS, and has been discovered by Genwei Jiang of FireEye. Genwei Jiang is also one of the researchers who has been credited with the discovery of a Flash Player zero-day vulnerability (CVE-2016-1019) that has been patched in April. The flaw, an exploit for which was integrated into the Magnitude Exploit Kit, was exploited to deliver Locky ransomware. So, if you used Flash Player, be ready to patch your installation as soon as possible once the fix is released. Alternatively, given all these problems, you might want to reconsider its use, and uninstall the media player altogether. (helpnetsecurity.com, 11May16)

(U) Patch Tuesday: Microsoft rolls out 16 bulletins, eight rated critical

(U) Microsoft's May Patch Tuesday roll out which contains 16 bulletins covering 37 vulnerabilities, with half of them being rated critical and possibly leading to remote code execution, is a slightly larger batch compared to the 13 issued in April. The critical rated bulletins are MS16-051, MS16-052, MS16-053, MS16-054, MS16-055, MS16-056, MS16-057 and MS16-064 with several industry watchers tagging MS16-051 for Internet Explorer as one of the more important issues because, as Microsoft has already noted, it is under attack in the wild. "On the top of our list is the update for Internet Explorer (MS16-051) that addresses a critical RCE-type vulnerability CVE-2016-0189 that is currently under attack. The vulnerability is in the JavaScript engine and in Vista and WIndows 2008 the engine is packaged separately from the browser, so if you run these variants of Windows (only 2 percent still run on Vista) you need to install MS16-053," Wolfgang Kandek, Qualys CTO told SCMagazine in an email Tuesday. David Picotte, Rapid7's engineering manager said in an email to SCMagazine.com that if for whatever reason administrators can't patch their systems right away, Microsoft has provided a workaround in MS16-051 that disables the VBScript.dll and JScript.dll functionality. A method Picotte described as "a crude but effective means of reducing your risk." The remaining critical bulletins are for Microsoft Edge, JScript and VBScript, Office, Graphics Component, Windows Journal and Windows Shell. Bulletin MS16-064 contains a link for users to see Adobe's advisory APSB16-14 for updates to several products, including Flash Player. Chris Goettl, a product manager with Shavlik, said, in comments emailed to SCMagazine.com, "Adobe Flash Player only released an advisory today, but it included high-level details of a vulnerability that has been detected in exploits in the wild. If information gleaned from MS16-064 is accurate, this Zero Day will be accompanied by 23 additional CVEs, with the release expected on 12 May. With this in mind, the recommendation is to roll this update out immediately." Although not rated critical MS2016-061 also caused some raised eyebrows. This Windows vulnerability could allow elevation of privilege if an unauthenticated attacker makes malformed Remote Procedure Call requests to an affected host. "Although Microsoft rates CVE-2016-0178 as less likely to be exploited, the potential for abuse on this one is enormous," Tripwire security researcher Craig Young said in comments emailed to SCMagazine.com. "The underlying flaw affects all supported servers and desktops from Windows Vista to Windows 10 and can allow an unauthenticated attacker to gain control of unpatched systems". (scmagazine.com, 10May16)

(U) Lenovo patches serious flaw in pre-installed support tool

(U) Lenovo has fixed a vulnerability in its Lenovo Solution Center support tool that could allow attackers to execute code with system privileges and take over computers. The Lenovo Solution Center (LSC) is an application that comes pre-installed on many Lenovo laptops and desktops. It allows users to check their system's virus and firewall status, update their software, perform backups, check battery health, get registration and warranty information and run hardware tests. The tool has two components: a graphical user interface and a service called LSCTaskService that runs in the background at all times even if the user interface is not started. The Lenovo Solution Center version 3.3.002, released on 25 April, contains a fix for a local privilege escalation vulnerability reported by a security researcher from Trustwave. The flaw could allow a local Windows user, or an attacker who compromises a local user, to execute malicious code with system privileges and take control of the whole OS. This is not the first time such a vulnerability was found and fixed in LSC. In fact, Lenovo updated an old advisory for flaws reported in December with information about the new vulnerability, making it somewhat hard to spot. Users should automatically be prompted to update LSC when they open the application, but in case they don't, they should download the latest version manually from Lenovo's website. (IDG News Service, 06May16)

(U) Microsoft will cease support for TLS certs signed by SHA1.

(U) Microsoft announced it will soon cease support for TLS certificates signed by the SHA1 hashing algorithm, according to ArsTechnica. After hinting in November that it might, the tech giant made it official last week. The end was expected following new research that revealed the popular cryptographic algorithm was susceptible to collision attacks--in which miscreants attempt to find two inputs producing the same hash value. Should they succeed, they would be able to forge digital signatures. As well-financed cybercriminals increase their sophistication and the costs of developing attacks decreases, experts have long been warning of vulnerabilities in SHA1, used by nearly a third of existing digital certificates. For example, the Carberp banking trojan employed malware signed by dual certificates, SHA1 and SHA2. Most browsers announced plans to cease accepting SHA1-based signatures beginning in January 2017. SHA1-based certificates will be blocked starting in February, Microsoft announced. (scmagazine.com, 05May16)

Threats & Vulnerabilities of the Week:

(U) CryptXXX 2.0 foils decryption tool, locks PCs
(U) CryptXXX ransomware, first spotted in mid-April, has reached version 2.0, and a new level of nastiness. It's also on its way to become one of the top ransomware families in the wild. The malware's first version would encrypt files but leave the rest of the infected computer alone, and victims would be able to use it to buy Bitcoin and pay the required ransom. This also allowed them to deploy a decryption tool, developed by Kaspersky Lab researchers only a week after the first instance of the ransomware was spotted. The AV maker added the decryption capability to its decryptor tool meant initially for decrypting files taken hostage by the Rannoh ransomware. But that option is not available any more, as CryptXXX 2.0 not only bypasses the decryption tool, but also locks the computer's screen after popping-up the ransom request: In addition to all this, the page where the crooks explain how the victims can effect the ransom payment mentions a Google Decrypter tool they will be able to use to decrypt their files. Proofpoint researchers believe that's just a misdirection, to prevent victims to identify with which ransomware they have been hit. "While new decryption tools may emerge, CryptXXX's active development and rapid evolution suggest that this new ransomware will continue to compete strongly in malware ecosystems," the researchers noted. "As always, best practices for avoiding infection include patching systems and software, updating endpoint antimalware, deploying robust network protections, and regularly backing up all critical systems". (helpnetsecurity.com, 11May16)

(U) SAP vulnerability exploited to compromise enterprises worldwide
(U) A SAP vulnerability, patched over five years ago, is being leveraged to exploit SAP systems of many large-scale global enterprises, US-CERT warns. At least 36 organizations in the US, the UK, Germany, China, India, Japan, and South Korea, spanning a number of industries, have had their SAP business applications compromised via this flaw, says SAP security company Onapsis. The company's researchers have discovered that the exploitation of this flaw and the compromises of those organizations were publicly disclosed on a digital forum registered in China during the last three years. "In early 2016, we became aware of this issue after we noticed common similarities within the results of initial Onapsis Security Platform scans at SAP customers, together with indicators of compromise found at SAP forensics & incident response engagements. The Onapsis Research Labs decided to dig deeper into this topic and realized that information about these exploitations had been sitting in the public domain for several years," they shared. The researchers notified the affected companies, who then remediated the problem. US-CERT was also contacted, and public disclosure of the problem was coordinated. "The core vulnerability being exploited has been identified as the Invoker Servlet vulnerability, which was patched by SAP in 2010. This is being leveraged in tandem with a sensitive SAP Java application to remotely gain full administrative access to the SAP systems," the researchers explained. "Exploits can take advantage of this vulnerability over HTTP (S) and without the need to have a valid SAP user in the target system. In order to exploit this vulnerability, an attacker only needs a Web browser and the domain/hostname/IP address of the target SAP system." This type of foothold can also be used to access other systems. An extensive and likely still not complete list of potentially affected SAP business solutions and technical components has been provided, and companies that deployed them are urged to check whether they have been working on outdated and misconfigured SAP systems. If they did, they should check whether they have been compromised. US-CERT recommends users and administrators implement SAP Security Note 1445998 and disable the Invoker Servlet. Onapsis researchers do not believe that the attacks mounted via this flaw are the work of nation-state-backed hackers or another group. But, they do believe that these documented attacks are just the tip of the iceberg. "Software will always have security vulnerabilities and the most a vendor can do once an issue is discovered is to release a security patch quickly. In this specific case, SAP made a patch available more than 5 years ago," the researchers concluded. "Therefore, what this news illustrates is not an SAP problem but the reigning lack of visibility, governance and control over cyber security risks affecting SAP platforms once they are installed and running, a responsibility that falls on SAP customers' information security teams, service providers and external audit firms". (helpnetsecurity.com, 11May16)

(U) Researchers create self-propagating worm that targets SCADA equipment
(U) German researchers from OpenSource Security (OSS) have created a proof-of-concept worm that targets programmable logic controllers (PLCs), crucial ICS/SCADA equipment. Their research builds on previous work by fellow German researchers, who presented at last year's Black Hat USA conference a port scanner that can identify Internet-accessible PLCs. The OSS team led by Ralf Spenneberg has created a worm, a self-propagating computer virus, that can live in the small memories of PLC devices, scan the local network, and spread to other similar devices. In their proof-of-concept code, the researchers created a worm that can infect Siemens SIMATIC S7-1200 PLCs. Nicknamed PLC-Blaster, the worm will scan the local network via port 102, shared by Siemens devices and the Inter-Control Center Communications Protocol (ICCP), to find new targets to copy itself. After identifying a new target, the worm shuts down the device, copies its code, and reboots it. Researchers say the actual infection process works because the worm mimics the Siemens TIA-Portal and also leverages a vulnerability already patched by Siemens. Researchers say that this kind of attacks will need the malicious actor to have access to the vulnerable network, or to compromise the PLCs before getting shipped to their customers. Once installed on an industrial network, PLC-Blaster executes, spreads to other devices, and then executes other types of malicious code that can damage SCADA equipment or create a DoS (Denial of Service) state for critical equipment. Researchers also said their worm can be easily modified to target other types of PLCs, but that it is also easy to detect, thanks to the mandatory ten seconds interruption needed for the worm to copy itself. More details about the PLS-Blocker mode of operation can be found in the research paper and this Black Hat Asia 2016 presentation. (Softpedia, 10May16)

(U) Aruba fixes networking device flaws that could open doors for hackers
(U) Wireless networking device manufacturer Aruba Networks has fixed multiple vulnerabilities in its software that could, under certain circumstances, allow attackers to compromise devices. The vulnerabilities were discovered by Sven Blumenstein from the Google Security Team and affect ArubaOS, Aruba's AirWave Management Platform (AMP) and Aruba Instant (IAP). There are 26 different issues, ranging from privileged remote code execution to information disclosure, insecure updating mechanism and insecure storage of credentials and private keys. However, Aruba combined them all under two CVE tracking IDs: CVE-2016-2031 and CVE-2016-2032. The impact of these issues vary depending on the network configuration, but the company plans to fix them in Aruba Instant and AirWave Management Platform later this year. The planned update will change PAPI so that it operates within a secure channel such as DTLS or IPsec, the company said. Until then, customers can apply the recommendations included in the "Control Plane Security Best Practices" document that was published on the company's support portal. There are two issues in IAP that Aruba does not consider security vulnerabilities, but because they're not in line with industry best practices the company will fix them in a future update. One of them stems from the use of a static password for an engineering support mode that provides additional configuration and diagnostic capabilities, the misuse of which could result in physical damage to the AP hardware. This mode can only be accessed from an authenticated administrative session so potential attackers would already need to have access to administrative credentials. The other issue stems from the use of a static key to encrypt all passwords stored in the IAP configuration file. If such a file is stolen, an attacker could reverse engineer the platform's code to extract the key and decrypt the passwords. (IDG News Service, 09May16)

Incidents of Interest:

[redacted] OGA

(U) Tax payer info exposed in five breaches, FDIC
(U) Five major breaches since 30 October have put the personally identifiable information (PII) of taxpayers at risk, the Federal Deposit Insurance Corp. [FDIC] told Congress on Monday, according to the Washington Post. Each instance was blamed on insiders who, when leaving the agency, took corporate files with them. In affidavits, those involved testified they did not share the information. The cases were reported only because of requirements that mandate that the FDIC -- which provides banks with deposit insurance -- disclose any breach exceeding 10,000 records. The FDIC reported that it has stepped up security measures, including prohibitions on the use of removable media devices by the majority of its employees and the implementation of software "to force encryption of portable devices." The agency also will hire a contractor to conduct an IT security assessment and offer best practices. (scmagazine.com, 10May16)

(U) Fraudsters loot W-2 data stored by Equifax
(U) Equifax, one of the big-three US credit bureaus, has been targeted by fraudsters that search for W-2 data and use it for claiming fraudulent tax returns. But the company hasn't been breached. Instead, in an approach similar to the one recently used to steal W-2 data from the ADP customer portal, the crooks misused the fact that not many users change default login credentials they have been assigned, and managed to access random accounts and harvest the data in them. The real victims are the employees, current and former, of US grocery giant Kroger, Stanford University, Northwestern University, and probably other businesses and institutions, whose data has been stolen and misused. Users can access their accounts via Equifax's W2Express tax form management website, and to do that they are provided with login credentials that are based on their Social Security numbers (SSN) and dates of birth. Unfortunately, after years of massive data breaches left and right, this kind of information on US citizens has become easy to obtain on dark web markets. The users who have made the effort to change those login credentials once they entered their account aren't affected by these attacks. At Stanford University, 600 current and former employees had their data stolen in this way. At Northwestern University the number is 150. Kroger is still trying to determine how many of their employees have been hit. "The information in question was accessed by unauthorized individuals who were able to gain access by using users' personally identifiable information. We have no reason to believe the personally identifiable information was attained through Equifax systems," Equifax spokeswoman Dianne Bernez told Brian Krebs. "Unfortunately, as individuals' personally identifiable information has become more publicly available, these types of online fraud incidents have escalated. As a result, it is critical for consumers and businesses to take steps to protect consumers' personally identifiable information including the use of strong passwords and PIN codes. We are working closely with Kroger to assess and monitor the situation." I can't help but think that with Equifax not making it mandatory for users to change the default credentials for the portal they have contributed considerably to this unfortunate situation. (helpnetsecurity.com, 09May16)

[redacted] OGA

[redacted]

OGA

(U) Troy investment company hacked, stealing $495K

(U) An email hacker is apparently responsible for a $495,000 rip-off from a Troy investment company, investigators said Tuesday. Police received a report on 18 April from the Pomeroy Investment Corp. that an employee had received an email from another company worker requesting the transfer of $495,000 to a Hong Kong bank. Eight days later, the company determined the email was a fake designed to steal the funds. "Previously, it was typical for company employees to communicate by email and to make transfers of funds--even overseas," Troy Police Sgt. Meghan Lehman said. "But in this case, someone hacked the account of the sender requesting the funds. And then was days later before anyone questioned the transaction and learned they had been hacked." Lehman said the company has since reported the theft to its insurer and has changed internal policies, including doing business by email. "We warn residents all the time not to trust emails from strangers asking for any sums of money," Lehman said. "Here, it was believed to be a trusted email from a trusted source. "Considering the size of the transaction, a phone call might have been in order to verify the request. I would advised anyone, even if they believe they know the sender, to check by phone before ever making a financial transaction". (Detroit News, 03May16)

Items of Interest

(U) DHS is under the gun to collect data about threats to infrastructure, networks

(U) The Homeland Security Department is under the gun to collect massive amounts of data about threats to the nation's physical and network infrastructure, according to contracting documents. To meet a 1 June deadline to come up with an aggregation strategy, DHS has awarded a contract to Sunesis Consulting LLC without holding a competition, a sole-source justification states. The strategy is the first step in a larger effort to unite operations across the department's "cybersecurity, critical infrastructure protection and law enforcement situational awareness," as well as counterterrorism programs, among other domestic protection duties. Sunesis is the only firm "up to speed" on the mission, having recently helped select the "situational awareness data" that must be gathered, a contracting officer wrote in 28 April justification. The Alexandria, Virginia-based small business crafted interview questions for a Situational Awareness Data and Information Assessment report that identified the desired data sets, the officer said. The report was finished in February. A DHS spokeswoman told Nextgov the report is for internal use only. Also, Sunesis "provided a review of the need for additional capabilities/capacity for big data analytics to authenticate situational awareness" and for "identifying outage/disruption patterns," the officer said. If there is not a plan in place by 1 June, the department's Office of Information Protection will restrict funding to execute the project by $2 million. The scope of the immediate work "will include the development of detailed objectives and the definition of near-time situational awareness, a prioritization framework to support selection among the data sources, coordination opportunities" across the federal government "to leverage available sources at low or no-cost, and expected enhancements from the available data," an award notice states. By September, Homeland Security needs another plan detailing how to use the data at the department's 24/7 physical infrastructure watch center, the officer said. The facility -- called the National Infrastructure Coordinating Center -- serves as an information-sharing hub, when there is an incident affecting key US sectors that requires coordination between DHS and industry. The new information collection strategy "represents the first step toward developing a plan to implement the authoritative data sources study to assist NICC watch operations to effectively monitor critical infrastructure and provide situational awareness," the notice stated. The center communicates with a round-the-clock US IT network protection operation, the National Cybersecurity Communications and Integrations Center, to support the entire spectrum of critical infrastructure. The "learning curve" for any other vendor would essentially double the cost of the contract, the officer said. The dollar amount of the award is redacted in the documents. On Wednesday, presidential advisers are scheduled to discuss recommendations for DHS and other agencies on using big data analytics to protect US infrastructure. The National Security Telecommunications Advisory Committee's draft report describes how extensive, disparate data sets can produce intelligence in a crisis -- using the hypothetical scenarios of a hurricane, terrorist strikes on cities, and a cyberattack. (NextGov, 11May16)

(U) DISA unveils new cybersecurity review

(U) The Defense Information Systems Agency unveiled a cybersecurity review process on 9 May that takes an agile, "outside-in" assessment of the resources and technologies the Department of Defense Information Network (DODIN) needs to defend itself against attack. DISA calls the effort NSCSAR, short for NIPRNet/SIPRNet Cyber Security Architecture Review. Pete Dinsmore, DISA's risk technology executive, said the framework looks at all aspects of cybersecurity, from endpoints to the internet. DISA is working with the National Security Agency, DOD's CIO office, Cyber Command, combatant commands and other agencies to evolve DODIN's cybersecurity architecture. Officials plan to compare existing cybersecurity capabilities against a threat framework that details adversaries' tactics and techniques. Those capabilities are evaluated for their effectiveness in mitigating an attack. DISA has already begun implementing NSCSAR as an agile process with "spin cycles" that take a new look at the network every 90 days. Officials completed the first spin in April and has a second spin scheduled for completion on 30 June. (fcw.com, 10May16)

(U) Intelligence bill to require report on cybersecurity at US ports

(U) The bill that authorizes funding for the country's intelligence-related activities includes language that would require Homeland Security officials to give updates on the cybersecurity threats connected to the country's maritime industry. H.R. 5077 passed unanimously in the House Intelligence Committee late last month. It awaits a vote in the full House. The Undersecretary of Homeland Security for Intelligence and Analysis would be required to consult with the Director of National Intelligence and give House and Senate Intelligence Committee members a report on the cyber threats and vulnerabilities within six months after the bill becomes law. That report would include a description of recent attacks and attempts as well as any identified attacks being planned. The undersecretary also would need to address how the country's ports and shipping concerns are mitigating their risks. In addition to port cybersecurity, the authorization bill includes funding for fighting terrorism and containing the growth of weapons of mass destruction. Other measures include updating whistleblowing procedures; strengthening oversight of the privacy and civil liberties board; and improving how the intelligence community provides reports to Congressional leaders, said House Intelligence Committee Chairman Rep. Devin Nunes. The Intelligence bill is just the latest effort for lawmakers to strengthen cybersecurity at America's ports. Last December, the House passed a similar standalone measure that would have required DHS to establish voluntary guidelines for reporting cybersecurity risks. (Government Security News, 10May16)

(U) NIST unveils 'flexible' second draft for agency cybersecurity

(U) No two agencies are exactly alike, nor are cyber threats all the same -- that's why the National Institute of Standards and Technology's latest version of system security guidance can be adjusted for fit. Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems -- NIST Special Publication 800-160 -- is a guide for helping agencies and organizations assign value to their assets and choose the right set of tools that work best to secure their systems. "This publication is designed to be extremely flexible in its application to meet the diverse needs of organizations," the document states. "It is not intended to provide a specific recipe for execution -- rather, it is a catalog or handbook for achieving the identified security outcomes of each systems engineering process, leaving it to the experience and expertise of the engineering organization to determine what is correct for their purpose. Organizations choosing to use this guidance for their systems security engineering efforts can select and employ some or all of the thirty ISO/IEC/IEEE 15288 processes and some or all of the security?related activities and tasks defined for each process." The way security controls are applied today is through a categorization under the Federal Information Processing Standard, said NIST Fellow Dr. Ron Ross in an interview with Federal News Radio. Data and the security system are determined to be low, moderate or high impact, and then a set of controls out of NIST's SP 800-53 are selected and implemented. "This 800-160 comes at it from a different perspective," Ross said. "This says what are the stakeholder protection needs that are tied to critical mission space or business models, and that ends up spawning a set of security requirements. Then the question is what security controls can we select to satisfy those requirements." The agency released the draft version in May 2014. It's based on an IEEE and ISO joint standard. Ross said the second version took so long because NIST answered all of the public comments, and had to factor in a major update to the standard that took place in 2015. The 30 processes are sorted into four categories: Agreement, organization project-enabling, technical management and technical. Each process is broken down into purpose, outcome, activities and tasks. For example, the purpose of human resource management sets the criteria for the qualification, assessment and ongoing training for skilled cyber personnel. The outcome states the goal is to have a skilled cyber workforce that can be assigned to projects. Activities and tasks more specifically suggest actions to take to achieve that outcome. The 30 processes don't need to be applied all at once, Ross said, but the hope is to have agencies integrate all of them over time. "The aim of 800-160 is to "normalize" security activities both institutionally and through operations. Institutionalizing means integrating cybersecurity into every aspect of an organization and every decision-making process. You don't want to have security be a stovepipe, you want it to be fully integrated across the entire enterprise," Ross said. "Operationalizing cybersecurity ensures the workforce understands the responsibilities and protections, and what each person is supposed to do. Our goal is to get us on the right path and give people information," Ross said. NIST is collecting comments on the second draft. Send comments to sec-cert@nist.gov no later than 1 July 2016. -- federalnewsradio.com. (IDC News Service, 09May16)

(U) DARPA wants god-mode attribution platform to pin and predict crime

(U) The US Military skunkworks Defense Advanced Research Projects Agency (DARPA) is hoping to build a platform to help bolster the treacherous world of attack attribution that would generate, anonymise, and share threat data. The agency is seeking proposals for an "Enhanced Attribution" program which would bring high quality "transparency" to the "opaque" world of actor attribution, hopefully revealing the activities of online actors without compromising sources and methods. Project lead Angelos Keromytis says there is presently little chance that a criminal will be caught. "Malicious actors in cyberspace currently operate with little fear of being caught due to the fact that it is extremely difficult, in some cases perhaps even impossible, to reliably and confidently attribute actions in cyberspace to individual," Keromytis says. "The reason cyber attribution is difficult stems at least in part from a lack of end-to-end accountability in the current internet infrastructure. "Cyber campaigns spanning jurisdictions, networks, and devices are only partially observable from the point of view of a defender that operates entirely in friendly cyber territory." DARPA wants ideas about how to identify actors using physical and behavioural biometrics, break down tools into knowledge "representations", draw on open source data, and to build webs of information to reveal past and present malicious activity. It should also sport algorithms to predict criminal campaign behaviour. Internet-of-things, mobile phones, and desktop and laptops are all interesting "vantage points", according to the program document. Keromytis says actors can foil many attribution efforts by changing their tactics, techniques, and procedures, a fact which also inhibits response options and policy-making. He says Enhanced Attribution will develop techniques and tools to produce "operationally and tactically relevant information about multiple concurrent independent malicious cyber campaigns" that each have multiple actors. Threat intelligence has enjoyed a boom in the security industry with large firms and independent consultants spinning up firms dedicated to sieving through attack data and offering possible actor identities. Proposals for the DARPA project should "investigate innovative approaches that enable revolutionary advances in science, devices, or systems", the agency says. It comes as DARPA appealed for hackers to weaponise everyday objects under its Improv project to find flaws in all things. -- theregister.co.uk. (IDC News Service, 09May16)

(U) Internet of Fail: How modern devices expose our lives
(U) Should you sync your family's calendar to your refrigerator or have it display photos? Samsung believes you should. They also think you need cameras that display the food inside, to help during shopping. These features can make life easier, but how would you feel about someone accessing this information? What could a stranger do if he knew you're out of the house tomorrow night? I'm not saying this particular refrigerator is insecure, but do you have any assurances it's secure? How do you know the data it uses is safe from prying eyes? During the past few years we've seen examples of all sorts of IoT devices exhibiting glitches, getting hacked, manipulated, and exfiltrated of information: At Black Hat USA 2015, security researchers Runa Sandvik and Michael Auger demonstrated how they hacked a Linux-powered rifle made by Texas-based company TrackingPoint. They found vulnerabilities that can be exploited to make users hit targets they didn't intend to. Earlier this year, SF Globe reported on a deeply disturbing hack: someone accessed a Washington's family Foscam baby monitor and talked to their child at night. In January, Alphabet-owned smart homeware company Nest has asked users to reset their connected thermostats after a software bug drained its battery and sent homes into a chill in the middle of the night. A vulnerability in the mobile app used to interact with the Nissan LEAF electric can be exploited by remote, unauthenticated attackers to switch the car's AC and heating system on and off, but also to extract details about the owner's journeys, security researcher Troy Hunt has demonstrated. Last week, researchers exploited design flaws in the Samsung SmartThings smart home programming platform and successfully mounted a series of attacks that could result in smart homes being entered, burglarized, and generally made insecure via malicious apps. I believe we still haven't seen all the real dangers that the Internet of Things will bring. The Snowden revelations propelled privacy concerns into the mainstream. People are blocking their computer webcams by putting things over the lens, but at the same time they're wearing smart watches that track movements, using Smart TVs that monitor viewing habits, and buying all sorts of appliances that connect to the Internet insecurely. "When faced with a looming deadline like the holiday shopping season, given a choice between shipping a product or securing it, manufacturers will choose to ship every time," Bob Baxley, Chief Engineer at Bastille, told Help Net Security. "The big risk is not that a criminal will be able to break into your house through your smart lock, but that the smart lock will provide the attacker access to your network and online credentials. Why would a sophisticated criminal steal a $500 TV, when he could instead raid your bank account through your Internet connection?" Without a doubt, IoT is now mainstream. In fact, IoT use is growing rapidly across almost every industry. One of the things that makes IoT so disruptive is that its impact isn't restricted to a single sector or function. Enterprise IoT is having a huge impact, according to the "State of the Market: Internet of Things 2016" report by Verizon Enterprise. According to Baxley, this is scary for two reasons: 1. Enterprises don't even know what IoT devices are in their environment because these devices tend to communicate using off-network wireless protocols. 2. Enterprises keep more sensitive information than an individual does. All these attacks are predicated on the idea that you can't see the wireless IoT networks. There is some potential good news. According to Gartner, worldwide IoT security spending will reach $348 million in 2016, a 23.7 percent increase from 2015. Furthermore, spending on IoT security is expected to reach $547 million in 2018. (helpnetsecurity.com, 09May16)

(U) Opera VPN offers secure, private browsing for iPhone and iPad
(U) Norwegian browser developer Opera Software has launched Opera VPN 1.0, a free VPN service for iPhone and iPad users. The app provides users with the ability to encrypt their connection to the web for additional security, plus spoof one of five countries to bypass regional or network-specific restrictions. Other features include the blocking of both ads and tracking cookies. Opera VPN unashamedly targets this market with its free iOS app, coming hot on the heels on the recent introduction of VPN services to its desktop browser. Users can spoof one of five countries in this initial release -- US, Canada, Netherlands, Singapore and Germany -- with more likely to follow in due course. The app merely provides a gateway to the internet -- once the encrypted connection is configured, users simply switch to their other apps and continue as normal. There's a noticeable lag, but this is the price paid for re-routing the connection, and is found with all VPN services. Opera VPN tries to sweeten the deal by offering to block all ads and cookies -- this will speed up browsing, but there's no whitelisting facility for permitting ads from trusted websites. Both features can be switched on and off as required. It's worth noting that an increasing number of network providers are starting to block VPN access, so there may be times when the service doesn't work. (BetaNews, 09May16)

[redacted]

(b)(3) 10 USC ⊥ 424

Note: This is not original product but is consolidated from various sources.

[redacted]

(b)(3) 10 USC ⊥ 424