Cyber-Threat Newsletter – 16 Sep 16

Patches & Updates of the Week:

(U) Patch Tuesday: Adobe issues fixes for 29 Flash Player vulnerabilities
(U) September's Patch Tuesday kicked off with a notification from Adobe that it has made available security updates for Adobe Digital Editions, AIR SDK & Compiler and Flash Player, which alone had 29 critical vulnerabilities. The Flash Player patches were for Linux, Microsoft Internet Explorer 11 and Edge and Google Chrome along with extended support release and desktop runtime. The vast majority of the fixes patch memory corruption vulnerabilities and use-after-free vulnerabilities, both of which can lead to remote code execution. Other updates cover a memory corruption and integer overflow vulnerabilities that can also lead to code execution. The update to Digital Editions covers eight memory corruption and use-after-free problems impacting version 4.51 and earlier for Windows, Macintosh, iOS and Android. All can lead to remote code execution. Adobe AIR SDK & Compiler received just one update this month. The non-critical path is for version 22.0.0.153 and earlier for Windows and Macintosh and adds support for secure transmission of runtime analytics for AIR applications on Android. (scmagazine.com 13Sep16)

(U) Patch Tuesday: Microsoft rolls out 14 bulletins, prepares new updating system for October
(U) Microsoft's September Patch Tuesday offering, which included 14 bulletins covering 60 vulnerabilities or almost twice as many as were issued in August, is the last to be delivered under this update system with the company moving to a "monthly rollup" delivery mechanism starting in October. Microsoft announced in August that it would institute the "monthly rollup" for its October update that will include security issues and reliability issues in a single update instead of putting out a series of updates from which system administrators can pick and choose. Microsoft believes this will make life easier for admins and make Windows more reliable by eliminating update fragmentation. However, not everyone agrees with Microsoft's line of thought. Craig Young, security researcher at Tripwire, told SCMagazine.com that while a cumulative patch does make things easier for consumers and IT staffers there are some pitfalls. The first being the inability to roll back a specific patch that was not compatible, while retaining the good updates. "Under a completely cumulative patching model however this is not possible and a serious application interaction could force users to stay on outdated code until the interaction is resolved. When this happens as it did earlier this year when updates from Microsoft proved incompatible with certain software from Citrix, it is a serious problem for enterprises looking to balance risk and business continuity," Young said. Amol Sarwate, director of Vulnerability Labs at Qualys, told SCMagazine.com in an email, agreed with Young's points, but brought up another issue. "Another point to note is that previously shipped patches will not be included in the October roll-up and will instead be eventually rolled up in the upcoming year or so. This may create more work in the short run for administrators to keep track of which past KB is rolled up in each month's update," he said. Seven of the bulletins are rated "critical" with the remainder considered "important" with 10 of the vulnerabilities containing potential remote code execution issues with various Microsoft products. A zero-day vulnerability is also included CVE-2016-3352, under MS16-110, said Sarwate. A couple of the non-critical updates caught the eye of another Core Security researcher as being out of the ordinary. "There's a windows lock screen escalation of privilege fix MS16-112 as well as an update to Microsoft SMB server MS16-114 that could allow remote access to an attacker sending malicious messages to the SMBv1 server. Definitely consider how these surfaces are exposed in your organization," he told SCMagazine.com in an email. (scmagazine.com 13Sep16)

Threats & Vulnerabilities of the Week:

(U) Space invasion: Solar storms pose critical threat to internet, US infrastructure
(U) Ask anyone to make a list of the worst natural disasters, and you're likely to get a dissertation on the relative risks of hurricanes, floods, tornadoes, and similar terrestrial events. A solar storm, in contrast, is unlikely to make anyone's Top 5. According to Joseph N. Pelton, the former dean of the International Space University, that's a critical error in thinking that we need to address. Pelton, who also serves as a board member of the International Association of Space Safety (IAASS), argues that humanity should create an artificial Van Allen belt to supplement the natural Van Allen belts that already exist around Earth. These belts extend from an altitude of 600 to 36,000 miles above the Earth's surface and form a natural shield that prevents high-energy particles from hitting the Earth's atmosphere. Ordinarily, the Earth's magnetosphere shapes the Van Allen Belts and deflects the charged particles emitted by the sun (called the solar wind), while the VABs act to block high-energy electrons. Periodically, however, the sun releases solar flares. These flares are high-energy events that release a concentrated burst of energy in a particular direction. If that direction happens to be towards us, it can temporarily compress the magnetic field and allow high-energy particles through the Van Allen Belts. The largest flares are sometimes accompanied by a coronal mass ejection -- and as Pelton notes, these have the potential to wreak serious damage on both satellites and Earth infrastructure. There's certainly reason for concern. On 1 September 1859, the most powerful geomagnetic storm of modern times hit the Earth. Aurorae, normally visible only at high latitudes, reached the Caribbean. The glow over the Rocky Mountains was so bright, gold miners reportedly exited their tents and began preparing breakfast. Telegraphs failed across the world -- though in some areas, they continued to send and receive messages, even after being disconnected from their electrical supplies. The event became known as the Carrington Event, after British astronomer Richard Carrington -- but what caused small problems and unusual events in the 1800s would be absolutely devastating today. The handful of moderate geomagnetic storms in the last 40 years have caused significant damage to the grid; a full hammer blow would destroy the US electrical grid for several years. The economic impact of a similar disaster today is estimated at $2.6 trillion. Since we started monitoring the Sun's solar cycle, we've gotten lucky on a number of occasions -- CMEs that would have hit us even harder than 1859 have merely glanced us due to a non-ideal trajectory. Meanwhile, the United States' grid is more vulnerable to such events than ever before -- our transformer grid is, on average, nearly 40 years old, high-voltage power lines are carrying far more energy than they used to on a day-to-day basis, and there's virtually no way to quickly repair the damage such a storm would cause. (extremetech.com 13Sep16)

(U) MySQL zero-day exploit puts some servers at risk of hacking

(U) A publicly disclosed vulnerability in the MySQL database could allow attackers to completely compromise some servers. The vulnerability affects "all MySQL servers in default configuration in all version branches (5.7, 5.6, and 5.5) including the latest versions," as well as the MySQL-derived databases MariaDB and Percona DB, according to Dawid Golunski, the researcher who found it. The flaw, tracked as CVE-2016-6662, can be exploited to modify the MySQL configuration file (my.cnf) and cause an attacker-controlled library to be executed with root privileges if the MySQL process is started with the mysqld_safe wrapper script. The exploit can be executed if the attacker has an authenticated connection to the MySQL service, which is common in shared hosting environments, or through an SQL injection flaw, a common type of vulnerability in websites. Golunski reported the vulnerability to the developers of all three affected database servers, but only MariaDB and Percona DB received patches so far. Oracle, which develops MySQL, was informed on 29 July, according to the researcher, but has yet to fix the flaw. Oracle releases security updates based on a quarterly schedule and the next one is expected in October. However, since the MariaDB and Percona patches are public since the end of August, the researcher decided to release details about the vulnerability Monday so that MySQL admins can take actions to protect their servers. Golunski's advisory contains a limited proof-of-concept exploit, but some parts have been intentionally left out to prevent widespread abuse. The researcher also reported a second vulnerability to Oracle, CVE-2016-6663, that could further simplify the attack, but he hasn't published details about it yet. Oracle didn't immediately respond to a request for comments on the vulnerability. (IDG News Service 12Sep16)

(U) Macro-based malware evolves to bypass traditional defenses

(U) Macro-based malware is growing into full-featured malware capable of detecting and bypassing traditional security tools, Barkly researchers have discovered. Macro-based malware: The past Malware peddlers have been misusing Word macros to deliver malware for nearly fifteen years. The approach, which takes advantage of the macros' capability to automatically execute a series of instructions as a single command, has initially been used in the early 2000s. As users became accustomed to it, this malware delivery tactic was abandoned, only to resurface again in late 2014, allowing criminals to prey on newer generations of computer users. In the last two years, they have cycled through many different approaches for tricking users into enabling Word macros, but the malicious Word documents usually contained just scripts that would be triggered to download a dropper, which would then download the final malicious payload from a C&C server. Macro-based malware: The future? Barkly researchers have recently spotted a new wave of phishing emails that deliver booby-trapped Word documents posing as invoices, and asking users to enable macros in order to view the content: But this run was unlike many others before it, because the criminals have decided to leverage a second-stage executable payload embedded directly into the Word document. "One thing that makes this latest version of [well-known downloader] Hancitor stand out is that its payload is already bundled as a binary object directly in the Word doc. It's this payload that pings the C2 server. What it receives are pointers back to two additional binary objects (one executable and one DLL), which it downloads and executes," the researchers explained. The executed dynamic linked library (DLL) calls is what allows the attackers access to operating system resources and to grab additional payloads. The change in approach is an attempt to throw traditional security tools off the malware's scent. In this particular spam campaign, Hancitor attempts to drop the Pony and Vawtrak information-stealing Trojans, but it could just as easily be any other type of malware. Protecting users against macro-based malware in enterprise setups, employees can be protected through a combination of AV and behavioral-based protection, email filtering, and event monitoring, the researchers advised. Educating users on how to spot malicious emails and phishing attempts, and making sure that they can report incidents easily and without fear of negative repercussions, is also a must. In Office 2016, Microsoft has added a new feature that allows enterprise administrators to block all macros from running in Office documents that come from the Internet. Non-enterprise users must still rely on their own capabilities to spot these attempts, but endpoint security solutions and spam filters used by popular email providers can be of great help. (helpnetsecurity.com 12Sep16)

(U) New version of RAA ransomware only goes after business users

(U) A new version of the RAA ransomware was found recently by security researchers at Kaspersky Lab. This one, written completely in Jscript, seems to be targeting business users exclusively, the researchers claim. It comes as they all do: through an email with the malicious attachment. This one, however, comes in a password-protected zip file. This method does two things, it makes it harder for anti-virus software to recognize the malware and ii makes it seem more legitimate to the victims. The email usually says something about "overdue payment order from a supplier", to trick the victim into opening the attachment. The second biggest change in this new version is that the victim's machine no longer needs to be online to be encrypted -- all files can be locked while offline, as the malware does not need to communicate with its server. Once the malicious file is run, it starts encrypting files, while simultaneously showing a text document with random characters to confuse the victim. Before realizing what's going on, the files get encrypted. The malicious attachment also installs the Pony Trojan, which steals all email passwords. Hackers can then use the victim's accounts to further spread the malware. (BetaNews 12Sep16)

(U) Hackers selling GovRAT 2.0 malware used for targeting US government

(U) Hackers have infected several US military and other government agencies with a stealthy piece of malware called GovRAT, created specifically for spying on high-value targets. First discovered in November 2015 by InfoArmor, the GovRAT malware is a remote access trojan (RAT) sold on the Hell forum and TheRealDeal Dark Web marketplace. The malware coder's nickname is bestbuy, but after InfoArmor released its first report, he started using and selling the malware under the Popopret nickname as well. The malware, which was recently updated to v2.0, is very advanced, based on its capabilities. The crook selling it has intentionally named it this way, to target a specific niche of hackers who go after government agencies primarily. According to a recent listing on TheRealDeal, GovRAT's price is 2.5740 Bitcoin (~$1,600), but users can also buy access to the malware's source code for $6,000. Once a target is infected with GovRAT, InfoArmor says the attackers can use it to sniff on the local network, or use the malware to dump passwords from the infected computer's apps. This data can then be used to spread to nearby servers, from where they can infect more victims. GovRAT allows its buyers to use it and access an infected host, search for crucial files and then exfiltrate stolen data to a remote server. GovRAT 2.0 can also deploy USB worms to USB flash drives, which will infect any other PCs the flash drive is plugged into. This functionality is used for jumping from target to target on air-gapped networks. (Softpedia 11Sep16)

(U) Crafty malware is found targeting US government employees

(U) A tough-to-detect malware that attacks government and corporate computers has been upgraded, making it more aggressive in its mission to steal sensitive files, according to security firm InfoArmor. Last November, InfoArmor published details on GovRAT, a sophisticated piece of malware that's designed to bypass antivirus tools. It does this by using stolen digital certificates to avoid detection. Through GovRAT, hackers can potentially steal files from a victim's computer, remotely execute commands, or upload other malware to the system. Earlier this year, however, the makers of GovRAT came out with a second version, according to a new report from InfoArmor. The malware features an additional function to secretly monitor network traffic over the victim's computer -- something with scary consequences. "If you're downloading something from a particular resource, the hackers can intercept the download and replace it with malware," said InfoArmor CIO Andrew Komarov on Friday. Last year, InfoArmor said that earlier versions of GovRAT had attacked more than 15 governments around the world, in addition to seven financial institutions and over 100 corporations. The number of GovRAT victims, however, is growing, according to InfoArmor. That's partly because the maker behind the malware has been selling it to other hackers on Hell Forum, a black market website, Komarov said. Buyers of GovRAT have also been supplied with a stolen database of 33,000 Internet accounts, some of which belong to US government employees, InfoArmor said. It includes email addresses, hashed passwords, full names, and addresses. Hackers can use the contact information to carry out GovRAT attacks on US government targets, Komarov said. That can be done through phishing emails or drive-by downloads. The security firm has already alerted government offices that may be affected. It's been identifying victims by pulling data from the GovRAT malware's command and control servers. Komarov declined to name how many US government agencies have been attacked with GovRAT, but InfoArmor's report said they include defense and military departments. It's unclear who developed GovRAT, but the malware was designed for long-term cyberespionage operations, Komarov added. (IDG News Service 09Sep16)

(U) New Linux trojan coded in Mozilla's Rust language

(U) A new trojan coded in Rust is targeting Linux-based platforms and adding them to a botnet controlled through an IRC channel, according to a recent discovery by Dr.Web, a Russian antivirus maker. Initial analysis of this trojan, detected as Linux.BackDoor.Irc.16, reveals this may be only a proof-of-concept or a testing version in advance to a fully weaponized version. Currently, the trojan only infects victims, gathers information about the local system and sends it to its C&C server. The trojan, which is coded in Rust, a programming language sponsored by the Mozilla Foundation, also integrates the "irc" Rust library by Aaron Weiss, in order to communicate via the IRC protocol to a remote IRC public channel. At the time of writing, the channel hardcoded in the trojan's configuration is offline. All trojans that infect a target will automatically connect to this IRC channel and wait for commands. The hacker in control of this IRC channel can submit a message to the channel's public chat, and all connected bots will parse this message and execute it. Support is currently included only for a limited set of commands, hence the reason why Dr.Web researchers consider this to be work-in-progress malware. Researchers say the botnet's operator can currently only query a bot for its technical specifications, retrieve a list of running processes (apps), and kill the malware, if they want to remove a bot. There's also support for a feature that updates the trojan's source code, but it has not yet been fully implemented. (Softpedia 09Sep16)

(U) Latest Dridex includes new cryptocurrency targeting and new features to evade detection

(U) Despite its reduction in volume, Dridex malware is still actively being developed and Forcepoint researchers have spotted a number of changes and improvements including a feature that targets crypto wallets and others which make it harder to detect and protect against. Researchers said the malware's operators have built up profiles of commercial sandboxes and researcher VMs to essentially blacklist the machines to prevent researchers from obtaining the core module and list of peers and to make it more difficult for automated analysis systems to find and block the appropriate IP addresses, according to a 5 Sept blog post. The trojan also contains additional coding which allows its operators to quickly and effectively profile a victim's system for software which could be targeted for financial gain. To make outside analysis more difficult, Dridex developers have also changed parts of the malware's XML structure to more complicated binary structures. Despite the new features, researchers said it is still very much possible to reconstruct the Dridex settings configuration file received by the core module, the post said. Dridex is indeed a popular banking trojan and its main infection method is and still consists of phishing emails with malicious attachments, VASCO Data Security Senior Manager of Market and Security Strategy Frederik Mennes told SCMagazine.com via email comments. "Even though Dridex is designed to evade detection, security companies are continuously updating their software to counter viruses such as Dridex," Mennes said. To avoid infection, Mennes recommended the use of anti-virus software, two-factor authentication, anti-malware tools and up to date software. (scmagazine.com 09Sep16)

(U) How to crack Windows and OS X passwords

(U) A security researcher has revealed a way to determine the password needed to access a protected Windows or OS X account. Using Rob Fuller's technique, it doesn't matter if the computer in question is locked, and it uses a USB SoC-based device to crack user credentials. By modifying the firmware of a USB dongle, Fuller was able to make the device appear as an Ethernet adaptor. By spoofing a network connection, it is then possible to trick a target computer into giving up an account password. Fuller provides a detailed breakdown of how the attack works in a blog post. The hack can be achieved using very cheap hardware, and Fuller says that "this is dead simple and shouldn't work, but it does". While an attacker would need physical access to a computer in order to take advantage of the exploit, tests show that 13 seconds is all that's needed to gather passwords. Fuller managed to perform successful attacks using USB Armory and the Hak5 Turtle on all versions of Windows up to Windows 10 (but not Windows 8 for some reason), as well as OS X El Capitan. (BetaNews 07Sep16)

Incidents of Interest:

(U) WADA confirms Fancy Bear behind attack on anti-doping database

(U) The Russian cyberespionage group called Tsar Team, also known as Fancy Bear, was indeed the culprit behind the attack on the WADA Anti-Doping Administration and Management System (ADAMS) database through an account created by the International Olympic Committee for the 2016 Rio Games, the World Anti-Doping Agency (WADA) confirmed Tuesday. "While it is an evolving situation, at present, we believe that access to ADAMS was obtained through spear phishing of email accounts; whereby, ADAMS passwords were obtained enabling access to ADAMS account information confined to the Rio 2016 Games," a WADA release said of the attack on the database that housed athlete data, including private medical information. "At present, we have no reason to believe that other ADAMS data has been compromised." Adam Levin, chairman and founder of IDT911, and author of "Swiped," said "targeted US Olympians, including Serena and Venus Williams and Simone Biles, could be in serious jeopardy, as medical identity theft is perhaps the deadliest form of this pandemic." Once a cybercriminal nicks medical information "they, as well as those who purchase it from them on the dark web, can exploit your health insurance or obtain multiple prescriptions and medical treatments in your name and stick you with the bill," Levin said in emailed comments to SCMagazine.com. "Health records can easily be contaminated when test results and medical histories are co-mingled, blood types change and allergies disappear, putting victims' lives at risk." (scmagazine.com 13Sep16)

OGA

(U) FBI arrests hackers who allegedly leaked info on government agents

(U) US authorities have arrested two suspects allegedly involved in dumping details on 29,000 officials with the FBI and the Department of Homeland Security. Andrew Otto Boggs and Justin Gray Liverman have been charged with hacking into the internet accounts of senior US government officials and breaking into government computer systems. Both suspects were arrested on Thursday, according to the US Department of Justice. Boggs, age 22, and Liverman, 24, are from North Carolina and are allegedly part of a hacking group called Crackas With Attitude. From October 2015 until February, they used hacking techniques, including "victim impersonation" to trick internet service providers and a government help desk into giving up access to the accounts, the DOJ alleged. After gaining access, they stole personal information and uploaded it to Twitter. In addition, they defaced their victim's social media accounts and harassed the government officials and their families through phone calls. The suspects' Twitter handles. The FBI's affidavit of the case doesn't name the government officials involved, but they're believed to include CIA Director John Brennan. The document mentions five victims. Three other hackers located in the UK are also suspects in the case, and local authorities there are investigating. All three are male teenagers, two of which are 17, another 15. The suspects also broke into government sites, including the DOJ management system. To gain access, one of the suspects tricked the department's help desk into giving him the login credentials simply by making a phone call. In February, the group then used Twitter to post details on 29,000 FBI and Department of Homeland Security officials, including their phone numbers and email addresses. Both Boggs and Liverman will appear in a federal court in Virginia next week. (IDG News Service 08Sep16)

OGA

Items of Interest

(U) NSA using bomb-defusing software to grow the next generation of cyber analysts

(U) Cybersecurity students are scouring networks for a secret computer program designed to trigger a (prop) roadside bomb, in a twist on the National Security Agency's annual codebreaking contest, according to NSA officials. A few days ago, the agency provided college undergraduates and graduate students with file downloads for solving the Codebreaker Challenge, which, in this case, is to locate, replicate or "reverse engineer," and neutralize an improvised explosive device. According to a countdown clock on the competition website, you have 109 days left to deactivate the bomb. NSA officials say they will confront young computer scientists with the kinds of threats the agency faces daily, partly as an intelligence analyst recruitment effort. "The challenge is designed to simulate aspects of NSA's mission," agency spokeswoman Clarese Wilson told Nextgov in an email. New for 2016, the spy agency has added "network traffic analysis" to the specialties players will have to apply during the competition. "Software reverse engineering and network analysis are two disciplines that are critical foundations of both NSA's defensive mission and its support to offensive missions carried out by the military," Wilson said. The tasks range from identifying IED network ports to decrypting an IED key file to permanently disabling any IED, according to a competition FAQ. A scoreboard on the contest site ranks participating students by tasks solved. So far, Georgia Tech is leading in three of the six tasks, with Carnegie Mellon University first in two activities. The most active players hail from Carnegie Mellon University Georgia Institute of Technology Dakota State University, University of Maryland, Baltimore County, North Carolina State and Johns Hopkins University. (defenseone.com 14Sep16)

(U) CREST takes over cyber-assurance program from NSA in America

(U) The National Security Agency has handed over responsibility for operating and promoting its CIRA accreditation program to CREST, best known in the UK for its accreditation schemes with GCHQ, CESG and the Bank of England. CREST has signed a deal with the National Security Agency in America to run its Cyber Incident Response Assistance (CIRA) accreditation program. CREST is a not-for-profit accreditation and certification body which began in the UK in 2006 and represents and supports the technical information security market. It works closely with GCHQ, CESG and the Bank of England on a number of cyber-accreditation schemes. Under the memorandum of understanding between the NSA's Information and Assurance Directorate (IAD) and CREST, the two organizations will aim to grow CIRA while maintaining a strict accreditation process. The IAD provided advanced CIRA and Vulnerability Assessment (VA) services to address security incidents against national security systems. The National Security Cyber Assistance Program (NSCAP) was created to leverage the cyber-expertise of the industry to perform select cyber-security services for owners and operators of critical computer systems. Accreditation of qualified commercial industry partners capable of providing cyber-security assistance services is based on stringent NSA criteria and industry and government best practices. To support the work, CREST has established a new US chapter, welcoming Gotham Digital Services (a Stroz Friedberg company), MWR InfoSecurity, Nettitude, Stroz Friedberg and Trustwave as its first members. In addition to the UK, CREST has chapters in Australia, Malaysia, Hong Kong and Singapore. The deal is being hailed as another example of the benefits of collaboration between industry and government to develop and support cyber-security capabilities. It is also seen as a triumph in the quest to export more British cyber-security expertise, and CREST has welcomed the active support of the FCO in establishing the new chapter in New York City. Rowland Johnson, director of CREST International, is delighted with CREST's latest international chapter. "The US market is likely the largest cyber market in the world, and the opportunity to work with key stakeholders in the market is the dawn of a new era for CREST," he told SCMagazineUK.com. (scmagazine.com 14Sep16)

(U) Army wants cyber capability everywhere

(U) The Army's new cyber director said the service is still struggling to make cyber, electronic warfare and information operations tangible to warfighters. Speaking at West Point's annual Mad Scientist Conference, Brig. Gen. Patricia Frost said the Army's "cyber mission force is on track," but the service lacks a coherent electronic warfare strategy. "For the last decade-plus, EW's been very focused on [countering improvised explosive devices], which I'd say is a soda-straw view of where electronic warfare needs to be," she added. "If we say we are going to fight in a contested and congested electromagnetic spectrum, what does that mean for the Army, and are we organized and equipped to fight well in that environment?" She added that the Army cannot continue to rely on old technology for new fights and instead needs to ask how technology can help in the near term and the future. "We have a force strategy today that I believe is just not efficient because it is not organized correctly," she said. Frost, who has an intelligence background, previously served as deputy commanding general for operations at Army Cyber Command, so she is passionate about signals intelligence, cyber and electronic warfare. Her goal is to adopt a more comingled and integrated approach in which the Army treats cyber and electronic warfare as intrinsic to the warfighting mission rather than as separate entities. "I don't believe you can separate it anymore...because of where we've gone in this environment," she said. "To sit there and say it's separated -- I'm having trouble with that." In the past, commanders knew the electronic signals and spectrum they were going to encounter in the battlespace, and the US military dominated that space. "Now the complexity of understanding what could be attacking or collecting on us is a little bit more difficult, and then how do you protect the outer soldier in the vehicle?" she said. Frost said warfighters need to understand "that when they roll out, there are ones and zeros, there is information flowing that we didn't experience...in the past." The Army must address that new environment in its training, she told FCW. She acknowledged that it's difficult to conduct cost-effective training exercises that highlight what it's like to fight in a contested and congested electronic environment. But the training needs to demonstrate "that they can actually be denied being able to operate a certain system because then they will go, 'Ah, I get it! You just made it impossible for me to execute my warfighter function.'" Frost added that there is substantial buy-in from leaders who understand the importance of cyber and electronic warfare, but she reiterated that the constant challenge for her directorate is to make highly complex and often abstract concepts tangible and clear to maneuver units. At the same time, she said she is concerned that the Army has yet to fully analyze the future threats it will face and determine the emerging growth requirements and then prioritize the needed investments. (fcw.com 13Sep16)

(U) Justice Department group studying national security threats of internet-linked devices

(U) The US Justice Department has formed a threat analysis team to study potential national security challenges posed by self-driving cars, medical devices and other Internet-connected tools, a senior official said. The new group's goal is to secure the so-called "internet of things" from exploitation by "terrorist threats" and by others who might try to hack devices to cause loss of life or achieve political or economic gain, according to Assistant Attorney General John Carlin, head of the Justice Department's national security division. The impetus for the team, which has been informally active for about six months, was an understanding that the internet is vulnerable to cyber attacks partly because it was not designed with security in mind, Carlin told Reuters, after announcing the group on Thursday at the Intelligence and National Security Alliance conference in Washington. Carlin said the group, a small team of about five to 10 people, did "not want to be alarmist" about new technologies such as self-driving cars, but that it wanted to identify and address security challenges presented by the internet of things before they are exploited. He cited the July truck attack in Nice, France, in which 86 people were killed, as an example of how automated driving systems could present a national security threat if they were remotely hijacked. "The internet on wheels .. clearly is going to present national security risks as this transformation takes place," Carlin said. The Federal Bureau of Investigation and the National Highway Transportation Safety Administration (NHTSA) issued a bulletin in March warning that motor vehicles were "increasingly vulnerable" to hacking. In July 2015, Fiat Chrysler Automobiles NV recalled 1.4 million US vehicles to install software after a magazine report raised concerns about hacking, the first action of its kind for the auto industry. Carlin said he has been to Detroit twice in the past six months on trips that included visits with auto industry executives to discuss national security issues surrounding smart cars. The group is being led by Adam Hickey, acting deputy assistant attorney general of the national security division, and will include industry experts and partnerships with other federal agencies, a Justice Department spokesman said. (Reuters 09Sep16)

(U) Chrome to warn users of insecure HTTP sites that transmit passwords or credit card info

(U) With Chrome, Google is on a mission. A mission to make the internet a safer place. Its ultimate goal is to display a warning that HTTP sites (rather than HTTPS) are insecure, but this is a long-term plan and there are many stages to go. Starting at the beginning of next year in Chrome 56, the plan moves to its next stage. As of January 2017, any HTTP sites that transmit passwords or credit card details will be flagged up as being insecure. Studies show that users do not perceive the lack of a 'secure' icon as a warning, but also that users become blind to warnings that occur too frequently. Our plan to label HTTP sites more clearly and accurately as non-secure will take place in gradual steps, based on increasingly stringent criteria. Starting January 2017, Chrome 56 will label HTTP pages with password or credit card form fields as 'not secure', given their particularly sensitive nature. (BBC News 08Sep16)

(U) White House names First Chief Information Security Officer

(U) The White House named its first-ever chief information security officer Thursday, part of its broader effort to shore up cyber practices after last year's massive intrusion into federal background check databases. The administration named Gregory Touhill, the Homeland Security Department's deputy assistant secretary for cybersecurity and communications, and a retired Air Force brigadier general, to the top information security position. Grant Schneider, the National Security Council's cybersecurity policy director and former Defense Intelligence Agency chief information officer, was named acting deputy CISO. The White House's Cybersecurity National Action Plan, announced in February and overseen by US CIO Tony Scott, outlined the need for a federal CISO. That plan was issued alongside President Obama's 2017 budget, which proposed raising IT security spending by 35 percent. Those proposals came months after news surfaced that a massive hack into the records held by the Office of Personnel Management exposed sensitive information on more than 20 million people. » Get the best federal technology news and ideas delivered right to your inbox. Sign up here. In his new role, Touhill's responsibilities will include driving "cybersecurity policy, planning and implementation" across federal agencies, and also leading periodic reviews of agencies' progress, according to the White House blog post. The Cybersecurity National Action Plan noted the CISO would be involved with the White House's proposed $3.1 billion IT modernization fund -- a pot of money to which agencies could apply for specific technology projects. One of the CISO's most important roles will be to "pull together all of the people in the federal government and make sure we have a well-thought through and then executed strategy in terms of how all of those entities work together," Scott said at an April event. (NextGov 08Sep16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424