[redacted]

[redacted] Cyber-Threat Newsletter – 07 Oct 16

(b)(3) 10 USC 424

Patches & Updates of the Week:

(U) OpenSSL update creates new critical flaw

(U) The OpenSSL Project released a critical patch for a new flaw created as a result of an update to the cryptography library. OpenSSL announced an update last week that fixed 14 flaws. However, a patch for a memory corruption flaw (CVE-2016-6307) in the open-source library created a dangling pointer flaw (CVE-2016-6309). OpenSSL released a patch for the new flaw on Monday. The critical vulnerability was disclosed by Google information security engineer, Robert Święcki. "The patch applied to address CVE-2016-6307 resulted in an issue where if a message larger than approximately 16k is received then the underlying buffer to store the incoming message is reallocated and moved," the security advisory stated. "Unfortunately a dangling pointer to the old location is left which results in an attempt to write to the previously freed location." A recent report highlighted the difficulties faced by enterprises patching open source software and noted a rising number of attacks that were the result of software vendors being slow to update open source components in commercial software. (scmagazine.com, 27Sep16)

Threats & Vulnerabilities of the Week:

(U) Dridex spam now using password-protected Office documents

(U) Operators of the Dridex banking trojan are experimenting with a new technique of delivering spam to their victims, according to independent security researcher MalwareTech. The researcher has recently spotted a spam wave coming from legitimate but compromised websites, which the crooks were abusing to send spam to victims, most predominantly to users living in the UK. There are two new techniques employed by the Dridex crew in this campaign. The first is the use of compromised servers to send spam. Previously, the Dridex gang had relied on the Necurs botnet, a network of compromised computers. Because crooks used such a novel tactic, it took security firms some time to discover the new campaign and properly mark it as spam. The second technique is in the email themselves. "The malicious rtf (Word Document) has been encrypted with a password given in the email," MalwareTech noted. "This would prevent most automated systems from extracting and scanning the attachment for malicious code, as most aren't able to handle password extraction or document decryption." While security software may have difficulties analyzing and detecting the malicious files sent in this new campaign, users don't have any problems in finding the password and using it to open the RTF file. Once users open these files, they are asked to enable macro script execution with a clever message. When they execute, these macro scripts download and install the Dridex Loader, which is different from previous campaigns as well. "Overall this campaign does seem to pack a bit more of a punch tha[n] the ones we're used to, possibly with the intention of infect[ing] corporate systems with more advanced threat protection rather than home users," MalwareTech says. Previously, security researchers have discovered Dridex campaigns targeting smaller countries and found the first signs of the trojan preparing to target crypto-currency wallets. (Softpedia, 27Sep16)

(U) Voldemort ransomware rears its ugly head

(U) Bad actors with a taste for the Harry Potters franchise have unleashed a new strain of ransomware they've dubbed Voldemort, named for the villain of the book and movie series. The virus was named after a few files detected in its coding referred to voldemort.horcrux and Nagini.exe (Nagini is Voldemort's snake). The ransomware locks screens on targeted computers and places an image of Voldemort on the monitor before presenting victims with a ransom demand. And, in a departure from usual procedures, rather than demand payment in bitcoin, it demands a credit card payment. A dig through the strings in the executable code revealed that the actor behind this ransomware signed on as Colosseum. It was discovered by Michael Gillespie, a self-dubbed ransomware hunter, who said it's still under development. While it is not yet widely distributed, researchers warn it could spread. Anti-malware tools could help remove it, they said. (scmagazine.com, 27Sep16)

(U) Spamhaus warns of a rise in IPv4 network hijacks

(U) Spamhaus, the organization that runs one of the Internet's largest, most accurate and up-to-date spam list, is warning against a spike in network hijacking events. Network or BGP hijacking occurs when an ISP falsely announces to other service providers that an IP range has been found on its network, when it has not. That ISP can then receive traffic destined for that range of IPs, but it can also send traffic on behalf of the hijacked network. While receiving hijacked traffic might be of interest for nation-state actors, as Bruce Schneier warned last week, sending traffic from a hijacked network is a spammer's dream. Spamhaus says that, in the past three years, BGP hijacks have grown in number, with most of these events occurring because of spammers, and not nation-state actors. The organization says this is happening because of the shrinking IPv4 space. As more IP ranges get blacklisted on Spamhaus, as well as on other IP blacklisting services, spammers are getting more desperate. In most cases, network hijacks occur when spammers find various methods of taking over legacy IP ranges, assigned to companies that don't seem to care about their IPv4 space. ARIN (American Registry for Internet Numbers) has also warned against an increase in IPv4 range hijacks in June, revealing that crooks are registering fake companies or re-registering old domain names in order to take over older IPv4 ranges. ARIN can do little about it since the 14,000 legacy IPv4 ranges it manages don't have an active contact person, so when someone reclaims the IP range, they have to follow procedure. Spamhaus detailed one such case on its blog yesterday, revealing that a known spam operator has managed to take over the IPv4 space of a legitimate company by impersonating its webmaster, who passed away a few years before the hijack. Using his name and an email address from a look-alike domain, the spammer managed to take over the IPv4 range and then route it through his desired ISP, where he was hosting a spam botnet. "Who can help stop these hijackings?" the Spamhaus team asks. "ARIN has stated that it must abide by procedures defined via its Policy Development Process, which sometimes can limit ARIN's ability to take action, even when notified of false information being added to its records." "It would seem that this activity will continue to be a problem until law enforcement starts to prosecute these criminal hijacking gangs and the spammers they conspire with," Spamhaus adds. (Softpedia, 27Sep16)

(U) New Mac trojan uses the Russian space program as a front

(U) Security researchers have found a new Mac OS X malware that appears to be targeting the aerospace industry. The Trojan, called Komplex, can download, execute, and delete files from an infected Mac, according to security firm Palo Alto Networks. Interestingly, the Trojan will also save a PDF document to the infected system concerning the Russian space program. The PDF document details planned Russian space projects from 2016 to 2025, but it acts as a decoy, Palo Alto Networks said in Monday blog post. In reality, the Trojan is a package of tools that will attempt to secretly communicate with its creators' command-and-control servers. This includes sending back data on the version, username, and process list running on the infected system. The Trojan can also receive instructions, and it will forward the results to the control servers. To infect its victims, the Trojan seems to be exploiting a known vulnerability in the MacKeeper antivirus software, according to Palo Alto Networks. That vulnerability can cause a Mac to execute remote commands when visiting specially crafted web pages. Victims might encounter this threat if they open a malicious link found an email. An elite Russian hacking team known as Sofacy Group or Fancy Bear may have developed the Trojan, Palo Alto Networks added. The security firm has said that the malicious coding in Komplex overlaps with another Trojan, called Carberp, which the hacking team used to target the US government through email phishing. It also noted that two internet domains used by the Komplex Trojan, apple-iclouds.net and itunes-helper.net, have been associated with other cyber attacks attributed to the Russian hacking group. Fancy Bear has lately been blamed for hacking other high-profile targets, including the Democratic National Committee, although finding the true culprits of any hack can be difficult. Nevertheless, security experts call the group among the best hacking teams in the world. Palo Alto Network said it doesn't know how many systems have been infected with the Komplex Trojan, but it has no reason to believe its part of a widespread attack. (IDG News Service, 26Sep16)

(U) MarsJoke ransomware distributed via Kelihos, targets US state, fed gov't agencies

(U) A large email campaign targeting state and local governments in the US as well as educational institutions distributes a new ransomware called MarsJoke via the popular Kelihos botnet, Proofpoint researchers discovered. The distribution methods closely mirror those of CryptFile2, researchers wrote in a blog post. Emails sent to potential victims contain URLs that link to a "file_6.exe" executable file, representing "a departure from the much more frequent attached document campaigns we have observed recently with a range of malware, including the widely distributed Locky ransomware," the researchers wrote, calling the email body used by the messages "convincing" and noting that the subject lines that referenced a national airline added "an air of legitimacy to the lures with stolen branding." Researchers gave the ransome its moniker after a string within its code that reads "HelloWorldItsJokeFromMars." They noted that the ransomware visually "mimics the style of CTB-Locker, including the helper application displayed to the user and the onion portal". (scmagazine.com, 26Sep16)

(U) Russian hacker collective targets over 85 leading US companies

(U) A group of hackers speaking Russian and using Russian servers are out hunting for American companies' user credentials, an exclusive story published on The Epoch Times claims. This group, allegedly not tied to any government and basically operating on its own, is targeting "at least" 85 companies, including Amazon, American Airlines, AT&T, Best Buy, Wells Fargo, DropBox, Dunking Donuts, Ebay, GoDaddy, Uber, Match.com, McDonald's, Office Depot, PayPal, Pizza Hut, Steam, and Apple Pay. Epoch Times broke the news after being approached by darknet investigator Ed Alexander, who apparently saw hackers "capturing card numbers and full identities", including answers to personal questions usually used during password recovery. Apparently, the first thing he did was take his iPhones off Apple Pay. He found customized cyberattack files, designed to target specific companies, and had configuration files for Sentry MBA, a popular "credential stuffing" tool. "In the case of credential stuffing, the most commonly used standalone management tool we have observed enabling attacks is called Sentry MBA", explain cybersecurity researchers at Shape Security. "A Sentry MBA config file contains, among other items, the URL for a website's login page, field markers to help navigate form elements, and rules for valid password constructions. A number of forums offer a wide variety of working configurations for various websites". (BetaNews, 26Sep16)

(U) Over 850,000 devices affected by unpatched Cisco zero-day

(U) A scan of Cisco networking devices from around the world has revealed that hundreds of thousands of devices are vulnerable to an unpatched security issue that allows attackers to retrieve data from the equipment's memory. Cisco has recently acknowledged that a cyber-offensive toolkit leaked online by a group of unknown hackers is also affecting its current device models after initial analysis said that only older (discontinued) PIX firewalls were affected. The tool, named BENINGCERTAIN, leaked in August when a group calling themselves The Shadow Brokers put it online along with tens of other hacking utilities they claim to have stolen from the server of a cyber-espionage entity named the Equation Group, which some security vendors said to be the NSA. Initial analysis by Mustafa Al-Bassam, aka tFlow, co-founder of the LulzSec hacking crew, showed how someone could use BENINGCERTAIN to extract VPN keys from Cisco PIX firewalls. Last week, a month after BENINGCERTAIN was leaked, Cisco announced that the tool was also effective against current devices running IOS, IOS XE, and IOS XR software. At the time of writing, there still is no patch available against BENINGCERTAIN (or Pix Pocket) exploitation. At the technical level, the exploit (CVE-2016-6415) employs a vulnerability in how the firmware of certain Cisco firewalls deals with IKEv1 and IKEv2 (Internet Key Exchange) packets. The Shadowserver Foundation, with the help of Cisco engineers, has conducted a scan of the entire Internet for Cisco devices vulnerable to this exploit. The scan is carried out at regular intervals, and according to the Shadowserver Foundation, on 25 September 2016, at 00:12 GMT, there were 850,803 vulnerable Cisco devices online. Over 250,000 of these devices are found in the US, followed by the Russian Federation, the UK, Canada, and Germany. The large number of devices, along with publicly available exploit code makes them easy-pickings for any threat actor that wants to compromise enterprise networks. Cisco has previously advised network admins to protect affected equipment by placing them behind firewalls. (Softpedia, 25Sep16)

(U) Hand-delivered hacking: malicious USBs left in mailboxes

(U) Julien Ascoet was already suspicious when he pulled the plain white envelope from his mailbox this past July. The letter had no stamp and was completely unmarked. Someone must have delivered it in person to Ascoet's home outside the French port city of Nantes. "I opened it gingerly," the software engineer said in an online chat Thursday. "You never know what's inside. I was remembering an episode of (police procedural drama) 'NCIS' where they found a similar envelope with anthrax." What Ascoet found was a memory stick with no note or explanation. It wasn't anthrax, but it could still be dangerous. Memory sticks, also called thumb drives or USBs, are sometimes used to spread malicious software from computer to computer. This USB was branded, but Ascoet said the device appeared used and that he doubted there was any connection between the brand and the mysterious delivery. Ascoet, who also works as a security researcher, eventually threw the device out -- although not before photographing it and posting the picture to Twitter. "Never EVER plug in such present," he said by way of caption. Stories like Ascoet's are anecdotal, but as web users get wise to rogue links and booby-trapped attachments, there are signs that cybercriminals are experimenting with hand-delivery of malware to people's homes. On Wednesday, Australian police drew international attention when they announced that "extremely harmful" memory sticks had been left in mailboxes across the suburban town of Pakenham, about 60 kilometers (37 miles) southeast of Melbourne. Pakenham Police Sgt. Guy Matheson said in a telephone interview Thursday that the unmarked thumb drives started showing up several days ago. Disguised as offers for Netflix or a similar service, Matheson said rogue programs lurking on the drives instead held victims' computers hostage, demanding a hefty payment in the electronic currency Bitcoin as ransom. Matheson said two or three people had fallen for the ruse. The technique of dropping a malicious USB somewhere and hoping someone will pick it up and plug it in has long been favored by spies to hack into hard-to-reach computers, said University of Manchester doctoral student Nikola Milosevic, who has studied the history of malware. "People are more likely to put USB stick into their computer than click a link or open file sent by the unknown person," Milosevic said in an email. "This type of attack has the potential to have a high success rate. (AP, 23Sep16)

[redacted] OGA

(U) Hackers sell tool to spread malware through torrent files

(U) Be careful with what you torrent. A new tool on the black market is helping hackers distribute malware through torrent files in exchange for a fee. On Tuesday, security researchers at InfoArmor said they discovered the so-called "RAUM" tool in underground forums. Popular torrent files, especially games, are packaged with malicious coding and then uploaded for unsuspecting users to download. Using torrents to infect computers is nothing new. But the makers of the RAUM tool have streamlined the whole process with a "Pay-Per-Install" model, according to InfoArmor. RAUM's developers have created a slick interface for their product. It can monitor the status of the malicious torrent files over popular sites such as The Pirate Bay and ExtraTorrent, which often act as a directory for users to download pirated content. "In some cases, the lifespan of these seeded malicious files exceeded 1.5 months and resulted in thousands of successful downloads," InfoArmor said. To infect more users, the makers of RAUM were also on the lookout for known uploaders of torrent files. They would then hijack their accounts, and use them to spread even more malicious torrent files. The RAUM tool has been found distributing ransomware such as CryptXXX, in addition to the Trojan Dridex -- which can steal a user's banking credentials -- and the password-lifting Pony spyware. The makers of RAUM are believed to be an Eastern European organized crime group known as Black Team, according to InfoArmor. The underground forums where the tool is sold are invite-only, with the verification process of new members quite strict. "InfoArmor strongly recommends that extreme caution be taken when visiting torrent trackers or downloading pirated digital content, operating systems and business software," the security firm said. (IDG News Service, 21Sep16)

Incidents of Interest:

(U) Top US universities hacked and injected with SEO spam
(U) An investigation has revealed that over 100 top US universities have been hacked and injected with SEO (search engine optimization) spam with the purpose of boosting the search engine ranking of an online gambling site. The infections are still active on many sites, even today, and consist of just two-three words inserted inside the page's text, linking back to the online gambling portal. Whoever has done this has been very careful not to attract the user and webmaster's attention. All links inserted on these sites are disguised to use the same text foreground and background color, and hide the link's underline. As such, the links blend in the page's background, but search engines will detect it and use it to calculate a better search engine ranking for the linked site, in this case, the online gambling portal. Israeli SEO firm eTraffic says it discovered the hacked sites after it investigated the mysterious apparition of a new online gambling service who managed to skyrocket to the first page of some Google search results for highly valuable keywords (search terms), such as "real money slots," or "slots." Their investigation revealed that countless of .edu and .gov websites were linking back to this new website, which is extremely peculiar since government and educational portals almost never link back to gambling sites. "Backlinks from TLD sites of .edu and .gov are highly coveted and possibly the most valued search engine optimization resource," eTraffic's Assaf Dudai explains. "Some of this [competitor gambling] site's links were coming from the most prestigious universities in the States, even one Ivy League -- Stanford." At this point, it was obvious to eTraffic that by the way links were disguised; someone had compromised these websites and inserted the URLs without the owner's knowledge. It may be totally plausible that the gambling site's operators had bought legitimate SEO services, and aren't currently aware that their service is promoted using this illegal technique. (Softpedia, 27Sep16)

(U) Krebs back online with help from Google's Project Shield
(U) Three days after taking down his website because of a massive two-week-long DDoS attack, Brian Krebs has returned online with the help of Google's Project Shield initiative. Launched in February 2016, Project Shield is Google initiative that aims to provide technical support for smaller news organizations, human rights, and/or elections monitoring services. One of the services Project Shield provides is free DDoS protection, which Krebs desperately needed and that can easily cost a company or individual anywhere above $100,000 per year. For years Krebs, a famous investigative journalist who has exposed many cyber-crime campaigns, has benefited from free DDoS protection from Prolexic, a company later acquired by Akamai, who also honored this deal. After Krebs exposed vDos, the Internet's most popular DDoS-for-Hire service, his site was under a barrage of DDoS attacks for weeks. For the first hours, the attacks were small and even grew to 128 Gbps after a day. After ten days, the attacks reached mammoth levels, easily becoming the largest DDoS attack ever recorded at 620 Gbps. Two days after this mammoth DDoS attack hit, Akamai fended off the malicious traffic. But things eventually started breaking down, and the company started having technical problems that affected the operational service of its paying customers. As such, on Wednesday, the company unloaded Krebs' blog off their network. Krebs said he holds no grudge against Akamai for protecting its true customers. Since he knew his ISP couldn't handle all the traffic, Krebs took down his website for good, trying to avoid problems for innocent third-parties. Other DDoS mitigation services offered their help, but Krebs said that they only granted him two-three weeks of free protection, after which he needed to pay like all the other regular customers, a cost he couldn't afford. That's where Google stepped in to help, with a project that seemed like a PR stunt when it was first launched in February, but now has come to show its true worth. (Softpedia 25Sep16)

(U) Largest DDoS attack ever delivered by a botnet of hijacked IoT devices
(U) A giant botnet made up of hijacked internet-connected things like cameras, lightbulbs, and thermostats has launched the largest DDoS attack ever against a top security blogger, an attack so big Akamai had to cancel his account because defending it ate up too many resources. It wasn't that Akamai couldn't mitigate the attack -- it did so for three days -- but doing so became too costly, so the company made a business decision to cut the affected customer loose, says Andy Ellis the company's chief security officer. The delivery network has dropped protection for the Krebs on Security blog written by Brian Krebs after an attack delivering 665 Gbps of traffic overwhelmed his site Tuesday. The size of the attack was nearly double that of any Akamai had seen before. The massive Krebs on Security assault is the work of a botnet made up primarily of internet of things devices, according to Akamai. So many devices were used, in fact, that the attacker didn't have to employ common tactics that amplify the impact of individual devices, Ellis says. The number of machines in the latest botnet is still unknown, and could be as large as a million. "We're still trying to size it," he says. "We think that might be an overestimate but it's also possible that will be a real estimate once we get into the numbers." With estimates of 21 billion IoT devices by 2020, the scale of botnets that might be created by these relatively unprotected machines could be enormous, says Dave Lewis, a global security advocate for Akamai who spoke Thursday at the Security of Things Forum in Cambridge, Mass. "What if an attacker injects code into devices to create a Fitbit botnet?" he says. Researchers have already shown it's possible to wirelessly load malware onto a Fitbit in less than 10 seconds, he says, so the possibility isn't fantastic. Some of the attacking machines are running clients known to run on cameras, he says. "It's possible they are faking it or it's possible it's a camera that was doing these attacks," he says. "There are indicators that there are IoT devices here, at scale". The attack didn't use reflection or amplification, so all the traffic consisted of legitimate http requests to overwhelm Krebs's site, Ellis says. "It's not junk traffic." A lot of things about the attack are still unknown such as who's behind it and what method the botmasters used to infect the individual bots. Ellis says some other providers Akamai had contacted report similar but smaller attacks likely from the same botnet. Many of them were aimed toward gaming sites, and Krebs has written about such attacks, so there may be a connection there, he says. (Network World, 23Sep16)

(U) State-sponsored actors suspected in historic Yahoo breach; at least 500 million accounts affected
(U) On the cusp of a $4.8 billion acquisition by Verizon, Internet company Yahoo today disclosed an immense data breach in which a state-sponsored actor is believed to have broken into the company's network in late 2014 and stolen a copy of account information belonging to at least 500 million users. According to a company statement, stolen information may have included names, email address telephone numbers, birth dates, hashed passwords and, in some instances, encrypted or unencrypted security questions and answers. For remediation purposes, Yahoo is invalidating these unencrypted security Q&As. Unprotected passwords, payment card data and bank account information were not affected, the company asserted, also noting that there is no evidence that the network intruders still have a foothold in their systems. The technology news site Recode had reported on Thursday that Yahoo would be imminently disclosing a major breach. Yet the announcement still managed to stun observers, after earlier reports had theorized that Yahoo would be confirming a previously reported 2012 data breach that may have affected around 200 million accounts. News of that apparent 2012 breach came last August, when Yahoo confirmed to Motherboard that it was aware of a hacker with the online moniker "Peace" who was claiming to sell stolen Yahoo user data and credentials on a dark web marketplace. While the report indicated that the data appeared genuine, Yahoo never confirmed the authenticity of the hack or forced a password reset for its users. Yahoo stated that it is taking steps to notify potentially affected users, but it is also recommending that users change their passwords if they haven't since 2014. The company statement also recommended that customers "avoid clicking on links or downloading attachments from suspicious emails and that they be cautious of unsolicited communications that ask for personal information." In the wake of the announcement, observers have speculated that the incident might drive down Yahoo's value and negatively impact its impending purchase by Verizon -- a deal announced last July. In this instance, "a Yahoo breach may lead to lawsuits, which puts a significant liability on Yahoo's balance sheet that may reduce its value to Verizon. Additionally, a breach could cause a major hit to Yahoo's reputation that again may reduce its value and may reflect poorly on Verizon," added Grossman. Recode printed the following statement from Verizon-owned AOL: "Within the last two days, we were notified of Yahoo's security incident. We understand that Yahoo is conducting an active investigation of this matter, but we otherwise have limited information and understanding of the impact. We will evaluate as the investigation continues through the lens of overall Verizon interests, including consumers, customers, shareholders and related communities. Until then, we are not in position to further comment." The announcement also prompted calls for better password management and data stewardship on the part of both companies and customers. Yahoo account holders, for instance, may now want to change passwords for not just Yahoo, but any other online service with which they registered the same credentials. Otherwise, those web services will be just as susceptible to the attackers. "The industry has been warning users for years that they need different complex passwords for each account they use online. The problem is that many consumers have dozens of accounts and remembering that many passwords is hard," said Brad Bussie, director of product management at data security software company STEALTHbits Technologies. Others expressed concern as to why Yahoo did not come forward sooner. (scmagazine.com, 22Sep16)

Items of Interest

(U) New draft of cyber response plan nearly ready for release
(U) The Department of Homeland Security is nearly ready to release a draft of the National Cyber Incident Response Plan that has been anticipated and debated for months. The latest version, which was shared with stakeholders for final comment, moves the NCIRP from the interim draft status under which it's languished since 2009 and inches it closer to a final plan. FCW obtained a copy of that stakeholder release, which runs just over 50 pages with appendices. The draft NCIRP follows the July release of Presidential Policy Directive 41, which outlines the roles and responsibilities of government agencies in responding to cyber incidents. The NCIRP is designed to fill in details PPD-41 left unaddressed, especially regarding private-sector responsibilities. "This update to the NCIRP focuses on discrete, critical content revisions," the introduction to the document states. "While the focus of the NCIRP is on cyber incident response efforts, there is a broader architecture outlined within the National Preparedness System that establishes how the whole community prevents, protects against, mitigates, responds to and recovers from all threats and hazards." The plan's stated purpose is "to provide guidance to enable a coordinated whole-of-nation approach to response activities and coordination with stakeholders during a significant cyber incident impacting critical infrastructure." One area not addressed in detail in PPD-41 is the role of the private sector in the response to a significant cyber incident. It goes on to say that "private entities that have a mandatory reporting requirement should assure that they report incidents that meet the required reporting thresholds even if they may otherwise mitigate the event. In most cases, these incidents are considered routine and are mitigated by the company using internal resources or with the assistance of contracted services providers." The draft also outlines a series of cross-cutting core capabilities and threat response, asset response and intelligence support capabilities. And it highlights coordinating structures and operational response protocols. PPD-41 identified federal agencies that would take the lead in responding to cyber incidents that have health, safety or national security implications. Those agencies will coordinate their activities through Cyber Unified Coordination Groups, and the NCIRP provides greater detail on the members and roles of those groups. An industry expert with intimate knowledge of the draft process said it is a significant step forward from PPD-41. A great deal of time was spent determining what capabilities must be in place and who can best provide those capabilities, the expert said -- whether that is the Federal Emergency Management Agency, the National Guard or the private sector. The source told FCW the draft plan takes into account the fact that there are industry capabilities that the government simply doesn't have, and the appropriate industry representatives must be identified and on standby for possible response. The source added that DHS took seriously the concerns and input of industry, and although not everyone is happy, the private sector generally views the draft in a positive light. However, as with PPD-41, experts inside and outside government say that until the system is activated in response to a cyber incident, it is impossible to tell whether the lines of coordination and communication have been properly connected and will function as anticipated. The draft will soon enter a 30-day comment phase. The goal is to have a finalized NCIRP before the start of the next presidential administration. (fcw.com, 27Sep16)

(U) Windows 10 will soon run Edge in a virtual machine to keep you safe
(U) Microsoft has announced that the next major update to Windows 10 will run its Edge browser in a lightweight virtual machine. Running the update in a virtual machine will make exploiting the browser and attacking the operating system or compromising user data more challenging. Called Windows Defender Application Guard for Microsoft Edge, the new capability builds on the virtual machine-based security that was first introduced last summer in Windows 10. Windows 10's Virtualization Based Security (VBS) uses small virtual machines and the Hyper-V hypervisor to isolate certain critical data and processes from the rest of the system. The most important of these is Credential Guard, which stores network credentials and password hashes in an isolated virtual machine. This isolation prevents the popular MimiKatz tool from harvesting those password hashes. In turn, it also prevents a hacker from breaking into one machine and then using stolen credentials to spread to other machines on the same network. The Edge browser already creates a secure sandbox for its processes, a technique that tries to limit the damage that can be done when malicious code runs within the browser. The sandbox has limited access to the rest of the system and its data, so successful exploits need to break free from the sandbox's constraints. Credential Guard's virtual machine is very small and lightweight, running only a relatively simple process to manage credentials. Application Guard will go much further by running large parts of the Edge browser within a virtual machine. This virtual machine won't, however, need a full operating system running inside it -- just a minimal set of Windows features required to run the browser. Because Application Guard is running in a virtual machine it will have a much higher barrier between it and the host platform. It can't see other processes, it can't access local storage, it can't access any other installed applications, and, critically, it can't attack the kernel of the host system. In its first iteration, Application Guard will only be available for Edge. Microsoft won't provide an API or let other applications use it. As with other VBS features, Application Guard will also only be available to users of Windows 10 Enterprise, with administrative control through group policies. Administrators will be able to mark some sites as trusted, and those sites won't use the virtual machine. Admins also be able to control whether untrusted sites can use the clipboard or print. This virtualization also likely comes at some performance cost, although Microsoft is not saying just what that performance cost is right now. Application Guard will become available later this year in Insider builds of Windows, hitting a stable version some time in 2017. (ars technical, 26Sep16)

(U) CIA commits to the cloud
(U) CIA's aim in moving to the cloud was to collect information in a private cloud behind an intelligence community firewall where it could be preserved forever. In 2013, FCW reported that the CIA had signed a cloud computing contract with e-commerce giant Amazon worth as much as $600 million over 10 years. The deal, which had survived months of protests by rival IBM, marked a watershed moment in overcoming agency reluctance to consider cloud technology for sensitive and mission-critical systems. In fact, the CIA's aim was to collect information in a private cloud behind an intelligence community firewall where it could be preserved forever. "The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time," CIA Chief Technology Officer Gus Hunt said at the time. "Since you can't connect dots you don't have, it drives us into a mode of...fundamentally [trying] to collect everything and hang on to it forever." The project also provided a reference model for other agencies looking for ways to bring their operational data into the cloud. That's been the case for members of the intelligence community, the group of 17 agencies for which the CIA has helped manage the Amazon Web Services acquisition. Last summer, National Security Agency officials said the new cloud infrastructure was already helping intelligence agencies smooth the transition from older legacy systems, making them easier to secure. The project went live in August 2014, and industry experts say its success so far will encourage other agencies to forge new cloud partnerships. (fcw.com, 26Sep16)

(U) House passes IT modernization bill
(U) The House of Representatives today passed the Modernizing Government Technology Act of 2016, a bill to authorize funds to replace legacy IT, on a voice vote. Lead sponsor Rep. Will Hurd (R-Texas), chairman of the Oversight and Government Reform Committee's IT Subcommittee, cited the hack of Office of Personnel Management systems as a driving force behind the new bill. A yearlong investigation of the hack identified "a pressing need for federal agencies to modernize legacy IT in order to mitigate the cybersecurity threat inherent in unsupported, end-of-life IT systems and applications," Hurd said a speech on the House floor. "We have too many old things on our network." The bill combines a cloud funding measure that originated in the Senate and was pushed in the House by Hurd with an Obama administration-backed bill that calls for a $3.1 billion government-wide revolving fund to retire and replace legacy systems. The MGT Act does not appropriate new money, but it does authorize working capital funds at the 24 agencies governed by the Chief Financial Officers Act to drive IT modernization and bank the savings achieved from retiring expensive legacy IT and shifting to managed services. It also authorizes a government-wide revolving fund to be managed by the General Services Administration. The bill leaves it to appropriators to work out the dollars and cents of the agency and government-wide funds. A spokesperson for Minority Whip Rep. Steny Hoyer (D-Md.) told FCW that the target for the government-wide fund is still $3 billion. On the Senate side, the Modernizing Outdated and Vulnerable Equipment and Information Technology Act of 2016 still has not seen activity in the Homeland Security and Governmental Affairs Committee. When the combined House bill was introduced on 15 September, a staffer for sponsor Sen. Jerry Moran (R-Kan.) told FCW that work is underway to see how an IT modernization bill could pass the Senate. The spokesperson said Moran is "encouraged by the House's swift action on the bill. (fcw.com, 22Sep16)

(U) Air Force reports making progress on cybersecurity without additional funding
(U) The US Air Force is reporting progress in its mission to give its weapons the same amount of cybersecurity protection as is received by the service's IT infrastructure under a year-old program called Task Force Cyber Secure. Gen. Ellen Pawlikowski, commander of the Air Force Materiel Command, said that the Air Force has been able to take meaningful action to secure its weapons systems after nailing down seven key focus areas, according to Federal News Radio. One of the objectives is to have security included in a weapons system during development and another giving cybersecurity training to purchasing personnel. "We spent a couple years acting like Chicken Little and really didn't do anything to get at this issue of our weapons systems," Pawlikowski said Wednesday at the Air Force Association's annual symposium in National Harbor, Maryland. (scmagazine.com, 22Sep16)

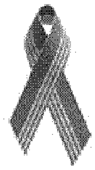
(U) We have to start thinking about cybersecurity in space

(U) With all the difficulties we've been having with securing computer systems on Earth, the cybersecurity of space-related technology is surely the last thing on security experts' minds. But it shouldn't be, say David Livingstone and Patricia Lewis, two fellows of the international security department at UK-based think-tank Chatham House. "Because so much of human activity is now dependent on space-based assets and infrastructure, most countries' critical infrastructure is potentially vulnerable to cyberattacks in that domain. An insecure environment in space will hinder economic development and increase risks to societies, particularly in crucial sectors such as communications, transport, energy, financial transactions, agriculture, food and other resources management, environmental and weather monitoring, and defense," they noted in a recently released paper. "Space-related cybersecurity gaps and weaknesses therefore need to be addressed as a matter of urgency." Cybersecurity in space includes satellites, rockets, space-based systems and vehicles, and space-stations, but also ground stations (satellite control centres), and associated networks and data centres -- all of which could be targeted by hackers. "Possible cyberthreats against space-based systems include state-to-state and military actions; well-resourced organized criminal elements seeking financial gain; terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions; and individual hackers who want to fanfare their skills," the researchers believe." The researchers are realistic, and know that all threats and risks can't be eliminated, but mitigation through security-by-design and risk management should be a goal. Who should spearhead policy changes and response to space cyberthreats? Not governments, the researchers argue, as "highly regulated institutional responses" typical of them are not nearly enough agile, flexible, nor fast to address the problem. "An international multi-stakeholder space cybersecurity regime -- based on an international community of the willing, and shared risk assessments and threat responses -- is likely to provide the best opportunity for developing a sectoral response to match the range of threats," they say, especially when space is slowly becoming a domain of not only wealthy states, but also less wealthy ones, as well as international organizations, corporations and individuals. International cooperation in this effort is of crucial importance, not only because most satellites orbit the Earth and its communications are effected via ground stations disseminated across the planet, but also because they are usually constructed with components manufactured by different countries. Another thing that such an effort should avoid is basing policies on technology alone. "An over-reliance on technical fixes is why cybersecurity controls failed to make an effective impact on cyberthreats in the late 1990s and early 2000s," they noted. "An effective regime requires a comprehensive technological response that is integrated into a wider circle of knowledge, understanding and collaboration." For more specific recommendations for the establishment of such a cybersecurity regime, check out the paper. (helpnetsecurity.com, 22Sep16)

[redacted]

(b)(3) 10 USC ⊥ 424

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



[redacted]

(b)(3) 10 USC ⊥ 424