[redacted] Cyber-Threat Newsletter – 14 Mar 16

Patches & Updates of the Week:

(U) Microsoft patches remote code execution flaws in Windows, IE, Edge, and Office
(U) Microsoft has fixed 39 vulnerabilities in multiple Windows components, Internet Explorer, Edge, Office and .NET Framework, many of which allow for remote code execution. The patches are grouped in 13 security bulletins, five of which are rated critical and the rest as important. According to researchers from security vendor Qualys, systems administrators should prioritize the MS16-023 security bulletin for Internet Explorer, which covers 13 critical vulnerabilities that can be exploited over the Web to fully take control of computers. Windows 10 users who prefer Microsoft Edge to Internet Explorer should prioritize MS16-024 instead, which covers 11 vulnerabilities in Microsoft's new browser, 10 of them critical. Interestingly, Qualys places the Microsoft Office security bulletin, MS16-029, next on its recommended priority list. This bulletin is rated as important, not critical, but does cover vulnerabilities that could result in remote code execution. On top of that, attackers commonly compromise computers by sending malicious Word documents packed with exploits. The next in line should be MS16-027, MS16-026 and MS16-028, which cover critical vulnerabilities in Windows components. The remaining bulletins all address vulnerabilities that are rated as important," Qualys CTO Wolfgang Kandek said in a blog post. "They come mostly into play when an escalation of privilege is required, so after one of the critical vulnerabilities was used to get into the target. You should address these vulnerabilities with the next 45 days to avoid this type of secondary use". (IDG News Service, 09Mar16)

(U) Cisco issues critical patch for Nexus switches to remove hardcoded credentials
(U) Cisco Systems has released software updates for its Nexus 3000 and 3500 switches in order to remove a default administrative account with static credentials that could allow remote attackers to compromise devices. The account is created at installation time by the Cisco NX-OS software that runs on these switches and it cannot be changed or deleted without affecting the system's functionality, Cisco said in an advisory. The company rated the issue as critical because authenticating with this account can provide attackers with access to a bash shell with root privileges, meaning that they can fully control the device. One factor that could potentially limit attacks is that on most NX-OS releases, the default account can only be accessed via Telnet, which is disabled by default. The exception is Nexus 3500 Platform Switches running Cisco NX-OS Software release 6.0 (2)A6 (1) where the account can also be accessed over SSH (Secure Shell). The affected devices are: Cisco Nexus 3000 Series switches running NX-OS 6.0 (2)U6 (1), 6.0 (2)U6 (2), 6.0 (2)U6 (3), 6.0 (2)U6 (4) and 6.0 (2)U6 (5) and Cisco Nexus 3500 Platform switches running NX-OS 6.0 (2)A6 (2), 6.0 (2)A6 (3), 6.0 (2)A6 (4), 6.0 (2)A6 (5) and 6.0 (2)A7 (1). Cisco has provided patched versions for all of these releases, but the company advises customers to upgrade to NX-OS 6.0 (2)U6 (5a) for Nexus 3000 switches and 6.0 (2)A7 (1a) or 6.0 (2)A6 (5a) for Nexus 3500 switches. That's because these versions also contain patches for two other high-impact vulnerabilities that could lead to denial-of-service conditions. (IDG News Service, 04Mar16)

Threats & Vulnerabilities of the Week:

(U) W97M/Downloader macro malware grows even more deceptive
(U) McAfee Labs has discovered a new deceptive technique that developers of the Word macro Trojan known as W97M/Downloader are using to avoid detection. According to an Intel Security/McAfee blog post, researchers found a variant of W97M/Downloader that builds off the already established tactic of hiding itself in Microsoft Office XML documents that contain compressed MSA Active Mime objects, which in turn extract encrypted OLE objects that automatically execute the malicious macro code. The new variant adds two brand new layers of trickery. First, the "malicious XML document is now hidden in a multipart MIME object distributed as .RTF or .DOC files that arrive via phishing or spam emails," the blog post explains. Secondly, the code that downloads and executes the final malware payload is not actually located in the macro, but rather in a very small (and thus difficult to spot) TextBox 1 object embedded in a form object. This final payload is a form of Dridex banking malware, which steals users' online banking credentials. Microsoft Office users can help protect themselves by disabling macros, McAfee advises. (scmagazine.com, 09Mar16)

(U) KeRanger ransomware is actually Linux.Encoder ported for Macs
(U) A big surprise was revealed today by security researchers from Romanian antivirus company Bitdefender, who claim that the KeRanger Mac ransomware that appeared last weekend is actually a rewrite of the ransomware variant that's been plaguing Linux servers for the past five months. After going through their regular procedures of looking at all new threats that their security products come across on a daily basis, the Bitdefender malware analysis team discovered an interesting tidbit. By taking a close look at the KeRanger disassembly, Bitdefender's staff spotted a lot of functions that bore a similar name to something they've seen before, in the Linux.Encoder Linux ransomware. Linux.Encoder is ransomware family that was first discovered by Dr.Web, a Russian antivirus company last November. The ransomware only targeted Linux machines and looked to encrypt files specific to Web servers and source code repositories. Bitdefender's Senior E-Threat Analyst Bogdan Botezatu is suggesting two scenarios of how this might have happened. Either the Linux.Encoder developer decided to expand the code to support Mac on his own, or he may have licensed the code to another cybercrime group specialized in Mac OS X systems. (Softpedia, 09Mar16)

(U) Report: Ransomware will 'wreak havoc' on critical infrastructure.

(U) A new report gives a stark warning that ransomware will "wreak havoc on America's critical infrastructure community" in 2016. The report, published by the Institute for Critical Infrastructure Technology (ICIT), compiled reported incidents of ransomware and predicted that previously exploited vulnerabilities will soon be utilized to extract ransom. Unless hackers are state-sponsored or part of a well-organized cybergang, the individual attacker is often unsure of how to successfully capitalize on exploits. Attackers enter into revenue-sharing agreements with script kiddies, said James Scott, senior fellow at Institute for Critical Infrastructure Technology (ICIT), in speaking with SCMagazine.com. "A lot of these attackers are going to be capitalizing on vulnerabilities that they dialed in last year," he said. On ransomware dark web forums, attackers announce their positions at specific targets, and will sit in wait. "They are setting up alliances and trying to become more intertwined in the organizations." Check Point president Amnon Bar-Lev confirmed this trend. In speaking with SCMagazine.com, he said ransomware "is much more of a problem than people anticipate." The ICIT report projected that ransomware attacks will evolve, much as phishing attacks, once the domain of the least adept attackers, have since grown into complex spear phishing attacks. "The evidence suggests that the threat landscape is shifting towards more profitable sectors," the report noted. For instance, the Hollywood Presbyterian Medical Center attackers demanded 9000 Bitcoins ($3.6 million). After negotiation, the hospital paid 40 Bitcoins ($17,000). The ransomware attackers "did not demand the typical user ransom of $210-420". (scmagazine.com, 09Mar16)

(U) Hacking Internet-connected trucks and buses

(U) Among the things one can find with Shodan, the search engine for the Internet of Things, are trucks, buses and delivery vans that have been equipped with the Telematics Gateway Unit (TGU) device and a modem to connect to the Internet. What's more, security researcher Jose Carlos Norte says that this setup can be misused by malicious individuals to monitor and control these vehicles: discover their position, their speed, and so on, as well as to change some of those parameters, e.g. change the vehicle's route, or put up a geo-fence for it (he says he does not now what such a change would cause). "There are thousands of TGUs connected to the internet, with no authentication at all and with administrative interfaces through a web panel or a telnet session," he says, and claims anyone with a modicum of knowledge can hack into the CAN bus of the vehicles remotely via the TGU. Part of that knowledge is not hard to find, he points out, as the schematics and capabilities for these TGU units are available online. Shodan can also be used by anyone. "You can see this device is connected to the bus of the vehicle, to the ignition, to the battery… and the theoretical things that could cause are very scary," he noted, and added that he wasn't able to discover all the things that can be done because he didn't have a unit available and he wasn't going to do testing in the wild because it would be irresponsible -- and advised others not to try that. "The c4max smartbox is a TGU with powerful capabilities, a simple console on port 23, and is easy to identify while scaning the Internet," he noted. His scan yielded 733 open devices, but he says that number can vary. (helpnetsecurity.com, 09Mar16)

(U) Phishing season in full swing as tax deadline looms

(U) Tax day is a little more than a month away, which means phishing season is in full swing. The IRS says it's seen a "surge" this year in phishing emails, with thieves baiting special hooks for payroll and human-resources workers in hopes of snagging a company's entire stash of employee Social Security numbers and other personal information. Meanwhile, tax-season phishing attacks against individuals are also up. Last month, the IRS said it had seen a quadrupling of phishing- and malware-related incidents for this year's tax season. Phishing peaks during tax season, partially because it's a time of year that many people are accustomed to entering their most personal information -- such as their Social Security number or bank account information -- on websites, Satnam Narang, senior security-response manager for security software maker Symantec, says. Thieves can then use that captured information to file a false return. Phishing also spikes around Christmas, with attacks in the form of fake delivery notifications. Thieves also often tie phishing emails to major sporting events, or natural disasters like overseas earthquakes, says Raj Samani, chief technology officer for Europe, the Middle East and Africa at Intel Security. "They're very much up with the latest news and information," Samani says. "If they can spend a little more time and get a 0.1 percent increase in click-throughs, then their campaign becomes hugely more profitable and successful." Narang adds that people should be wary of emails purported to be from banks, or other companies they do business with, but didn't opt into emails from. He also notes that banks generally don't include Web links in emails. Those links will likely take a person to a fake website where they will be asked to login and those credentials will ultimately be stolen, he says. And attacks don't just come in the form of email. They can come as text messages too, with those links often containing viruses, Samani says. "I think common sense goes a considerable long way," Samani says. He adds that with any email communications, it's always better to just go straight to the main website of the entity it purports to be from, just to be on the safe side. "I can't remember the last time I clicked on a link in an email," Samani says. "I just don't do it". (AP, 09Mar16)

~~(U//FOUO)~~ New ransomware compromises Mac users

~~(U//FOUO)~~ On 5 March, Palo Alto Networks researchers identified "KeRanger" as the first ransomware to successfully infect the Mac OS X operating system, according to press reports. On 4 March, unidentified attackers compromised the website of "Transmission," a BitTorrent file-sharing application, so that downloads included both Transmission and KeRanger software, which was signed with a valid Mac developer's certificate to bypass the Mac OS X built-in Gatekeeper protection system. About 6,500 users downloaded the infected software before Apple mitigated the issue. KeRanger encrypts files three days after infecting a computer, and the attackers were demanding one bitcoin—about $400—to restore the files. Palo Alto Networks said the attackers may also be trying to develop backdoor functionality and encrypt Apple's Time Machine backup feature. An Apple spokesman said the company has revoked the developer certificate so users can no longer install the affected app, and Transmission has released an infection-free version and published a warning on its website. (cio-today.com, 07Mar16 | Dow Jones Institutional News, 08Mar16 | The Boston Globe, 08Mar16)

(U) Cerber ransomware sold as a service, speaks to victims

(U) A new file-encrypting ransomware program called Cerber has taken creepiness for victims, but also affordability for criminals, to a new level. In terms of functionality Cerber is not very different than other ransomware threats. It encrypts files with the strong AES-256 algorithm and targets dozens of file types, including documents, pictures, audio files, videos, archives and backups. The program encrypts file contents and file names and changes the original extensions to .cerber. It can also scan for and encrypt available network shares even if they are not mapped to a drive letter in the computer. Once the encryption process is done, Cerber will drop three files on the victim's desktop named "# DECRYPT MY FILES #." They contain the ransom demand and instructions on how to pay it. One of those files is in TXT format, one is HTML and the third contains a VBS (Visual Basic Scripting). The VBS file is unusual. According to Lawrence Abrams, administrator of the technical support forum BleepingComputer.com, the file contains text-to-speech code that converts text into an audio message. "When the above script is executed, your computer will speak a message stating that your computer's files were encrypted and will repeat itself numerous times," Abrams said in a blog post. According to Cyber intelligence outfit SenseCy, Cerber's creators are selling the ransomware as a service on a private Russian-language forum. This makes it available to low-level criminals who might not have the coding skills or resources to create their own ransomware. It also means that this threat could see widespread distribution. (IDG News Service, 04Mar16)

(U) New attack steals email decryption keys by capturing computer sounds

(U) Scientists use smartphone to extract secret key of nearby PC running PGP app. The researchers -- from Tel Aviv University, Technion and The University of Adelaide -- recently published a separate paper that showed how to extract secret ECDH keys from a standard laptop even when it was locked in an adjacent room. The attack is able to obtain the key in seconds. A separate side-channel attack against RSA secret keys was devised in 2013. Unlike the one against mobile phones, it uses sound emitted by the electronics, rather than electromagnetic emanation or power consumption. At the moment, the attack would require a hacker to have physical possession of -- or at least have a cable or probe in close physical proximity to -- a vulnerable mobile device while it performed enough operations to measure "a few thousand ECDSA signatures." The length of time required would depend on the specific application being targeted. The requirements might make the hack impractical in some settings, as long as device owners take care to closely inspect USB cables before plugging them in and look for probes near their phones. Still, averting attacks may sometimes prove difficult, since cables or probes could be disguised to conceal what they're doing. For that reason, while the vulnerabilities probably don't pose an immediate threat to end users, they should nonetheless be a top concern for developers. The researchers have been working with the vendors of the specific software they analyzed to help them evaluate and mitigate the risk to their users. (ars technical, 03Mar16)

(U) Windows built-in PDF reader exposes Edge browser to hacking

(U) WinRT PDF, the default PDF reader for Windows 10, opens Edge users to a new series of attacks that are incredibly similar to how Flash, Java, and Acrobat exposed Web users for the past few years. The Windows Runtime (WinRT) PDF Renderer library, or just WinRT PDF, is a powerful component built into recent Windows OS versions that allows developers to easily integrate a PDF viewing feature inside their apps. The library is used for many apps distributed via the Windows Store, the default Reader App included in Windows 8 and 8.1, and even with Edge, Microsoft's latest Web browser. Mark Vincent Yason, security researcher with IBM's X-Force Advanced Research team has discovered that WinRT PDF can be leveraged in drive-by attacks in the same way attackers used Flash or Java in the past. Since WinRT PDF is Edge's default PDF reader, any PDF file embedded inside a Web page will be opened within the library. A clever attacker can contain a WinRT PDF exploit within his PDF file, which could be secretly opened using an iframe positioned off screen with CSS. All that an attacker needs to do is to find and create a database of WinRT vulnerabilities it could leverage to distribute his malware via this new attack surface. "A major factor that will affect when and how often we see in-the-wild exploits for WinRT PDF vulnerabilities depends on how difficult it is to exploit them," Mr. Yason explains. He says that because Windows 10 implemented former EMET features such as ASLR protection and Control Flow Guard, "makes the development of exploits for WinRT PDF vulnerabilities time-consuming and therefore costly for an attacker." Mr. Yason will be presenting a more in-depth presentation of this attack surface at this year's RSA security conference in San Francisco. (Softpedia, 03Mar16)

Incidents of Interest:

OGA

(U) Only 6,500 Mac users were exposed to the KeRanger ransomware

(U) Ever since the news about the first-ever fully functional OS X ransomware piece came to light over the weekend, Mac users have been fervently scanning their computers, especially those using the Transmission BitTorrent client, the app through which the ransomware spread. All this debacle happened because the Transmission project's website was hacked, and their legitimate Mac client replaced with one that included the KeRanger ransomware. The good news is that, according to the Transmission team, from the moment when their website was hacked and up to when the KeRanger infection was discovered, only around 6,500 users downloaded the infected binaries. The infected version was Transmission 2.90, and thanks to Palo Alto Networks, it was quickly detected and dissected. Apple also answered the bell, and thanks to a series of updates to its XProtect anti-malware suite, most Mac users were protected and the ransomware rendered harmless. The Transmission project quickly put out a clean version of their Mac client with version 2.91 and yesterday also released version 2.92, which includes a built-in KeRanger remover. (Softpedia, 09Mar16)

OGA

(U) Einstein and cyber workforce priorities for DHS

(U) DHS Secretary Jeh Johnson said one of his goals is to have Einstein 3A in place at civilian agencies by the end of the year. In what will likely be his last budget presentation before the Senate, Homeland Security Secretary Jeh Johnson said implementing the Einstein cybersecurity system across government, attracting capable cyber defenders and ensuring the success of the Department of Homeland Security's unified acquisition and management programs are among his top targets for the year and into the future. "One of my top goals is to have federal civilian agencies have [Einstein 3A] in place before the end of the year," Johnson testified at a Senate Homeland Security and Governmental Affairs Committee hearing on DHS' proposed $40.6 billion budget for fiscal 2017. Echoing remarks he made in February during his "state of the agency" speech, Johnson told lawmakers on 8 March that further investment in Einstein and the Continuous Diagnostics and Mitigation program was critical to federal agencies. Although some members of the committee pressured Johnson on border security issues such as the surging levels of unaccompanied minors crossing the US/Mexico border, they seemed satisfied with the department's plans for pushing ahead with Einstein and CDM. They were also substantially more agreeable on DHS' plan to transform the National Protection and Programs Directorate into an information hub. Committee Chairman Ron Johnson (R-Wis.) said he supported the plan to turn the directorate into a more streamlined cybersecurity agency. (fcw.com, 09Mar16)

(U) US cyber professionals test skills in exercise meant to stop attacks

(U) More than 1,000 cybersecurity professionals are participating in a Homeland Security Department simulation this week that tests their ability to deal with often-crippling cyberattacks. The event focuses on health care systems and retail sectors and follows recent high-profile breaches in those industries. Officials said the tests include participants from eight state governments. Organizers wouldn't preview their tests ahead of time, but said they're meant to test human responses and grade experts' ability to share information. Officials from five countries will be observing the drill, although the Homeland Security Department wouldn't say which ones. (AP, 09Mar16)

(U) IRS finally pulls offline ID Protection Service exploited by hackers

(U) After last year's massive data breach at the US Internal Revenue Service, the agency gave secret codes to the taxpayers whose personal information had been compromised. These "Identity Protection PINs" were to be included on future tax returns as an extra layer of security, since hackers had already stolen their Social Security numbers. Now, the IRS says identity thieves have stolen at least 800 of those PINs through its online retrieval service, and it has taken that service offline. In a statement released Monday 7 March, the IRS said it had sent PINs by mail to 2.7 million people for this tax season. Of those, 130,000 had used the online tool to retrieve their PINs before it was shut down. The thieves who stole 800 PINs subsequently used them to file fraudulent tax returns, which the IRS says were flagged and stopped. As we reported last week, the compromised PIN retrieval system used the same method of authentication, known as "knowledge-based authentication," that led to last year's breach of the agency's "Get Transcript" service. Despite the original breach, a report by the Government Accountability Office that pointed out the weaknesses in the PIN retrieval system, and questions last year from Quartz that raised doubts about the safety of the system, the IRS left it in place. The thieves presumably got into the PIN retrieval service this tax season the same way they got into the Get Transcript system last year. They were able to correctly answer authentication questions that KBA is based on, such as "On which of the following streets have you lived?" or "What is your total scheduled monthly mortgage payment?" The IRS shut down its "Get Transcript" service shortly after the data breach -- nine months ago -- and still hasn't brought up a new system to replace it. In its statement on Monday, the IRS said shutting down the PIN retrieval system is "part of its ongoing security review." The agency has not yet said when either system will be brought back up, or whether they'll continue to use KBA. President Barack Obama signed an executive order in 2014 mandating that all federal agencies implement multi-factor authentication to improve security. And although KBA does not meet the standards laid out in that order, the IRS seemed to be investing further into the method as of last spring. According to a report by Federal News Radio, the agency put out a request for quotations to federal contractors in April, saying it was looking to build upon its KBA systems, and invest $130 million. The IRS did not respond to questions from Quartz this week about where that request stands, and whether it's been altered following the continued exploitation of KBA on its website. During an investigation into the original breach last August, Quartz asked the IRS what it was planning to do about the PIN service's authentication system, since it appeared to be using KBA, the system that had already been hacked. At the time, the agency would not confirm the method of authentication, but said it was taking "a number of steps to protect taxpayers and Identity Protection (IP) PINs." (NextGov, 08Mar16)

(U) Pentagon releases cyber implementation plan

(U) The Defense Department CIO has released an "implementation plan" to help codify its increased attention to fundamental cybersecurity practices in recent months. The DOD Cybersecurity Discipline Implementation Plan prioritizes identity authentication, reducing DOD networks' attack surface, device hardening and the alignment of computer network defenders with DOD IT systems and networks. Inspection reports from recent network intrusions have "revealed department-wide, systemic shortfalls in implementing basic cybersecurity requirements," the plan states. The document, which was amended in February and publicly released within the last week, goes hand-in-hand with a DOD cyber scorecard that grades various agencies' IT security and is reviewed monthly by Defense Secretary Ash Carter. Whereas the scorecard is a more strategic, bird's eye view for Carter, the new implementation plan targets compliance further down the chain of command. Commanders and supervisors at all levels will report their implementation progress through the Defense Readiness Reporting System. The implementation plan lays out a series of tasks for DOD officials, organized against the four aforementioned priorities. For example, officials are charged with making sure their internal web servers require official Public Key Infrastructure authentication; with ensuring proper configuration of physical and virtual servers; with disconnecting all Internet-facing web servers and web applications without "an operational requirement"; and with ensuring proper incident response plans are in place. If officials determine it is not possible to comply with the document's requirements for operational reasons, they may be given an exception via a DOD risk management committee. (fcw.com, 08Mar16)

(U) Verizon Wireless hit by $1.4 million super cookie fine

(U) USA based Verizon Wireless has been fined USD1.4 million by the telecoms regulator for using so called "super cookies" without customer's consent. These unique, undeletable identifiers -- referred to as UIDH -- are inserted into web traffic and used to identify customers in order to deliver targeted ads from Verizon and other third parties. As a result of the investigation and settlement, Verizon Wireless is notifying consumers about its targeted advertising programs, will obtain customers' opt-in consent before sharing UIDH with third parties, and will obtain customers' opt-in or opt-out consent before sharing UIDH internally within the Verizon corporate family. "Consumers care about privacy and should have a say in how their personal information is used, especially when it comes to who knows what they're doing online," said FCC Enforcement Bureau Chief Travis LeBlanc. "Privacy and innovation are not incompatible." The regulator's investigation found that Verizon Wireless began inserting super cookies into consumer Internet traffic as early as December 2012, but failed to disclose this practice until October 2014. After acknowledging its use of UIDH, Verizon Wireless asserted that third-party advertising companies were unlikely to use these so-called "supercookies" to build consumer profiles or for any other purpose. In January 2015, however, news reports claimed that a Verizon Wireless advertising partner used super cookies for unauthorized purposes -- restoring cookie IDs that users had cleared from their browsers by associating them with Verizon Wireless's UIDH, in effect overriding customers' privacy choices. The following month, Verizon Wireless acknowledged the concerns raised by these news reports and committed to work with its partners to address the issue. It was not until late March 2015, over two years after Verizon Wireless first began inserting UIDH, that the company updated its privacy policy to disclose its use of UIDH and began to offer consumers the opportunity to opt-out of the insertion of unique identifier headers into their Internet traffic. Under the terms of the settlement, the company must also pay a fine of $1,350,000 and adopt a three-year compliance plan. (cellular-news, 08Mar16)

(U) Book 'Dark Territory' chronicles how NSA hacked DoD command-control systems in four days

(U) In what was the first-ever high-level exercise testing the US military's ability to defend itself against a cyberattack, the NSA in 1997 hacked into the DoD's entire network in just four days, using nothing but commercially available equipment and software, according to a new book by Pulitzer Prize-winning journalist Fred Kaplan. In an excerpt published by Slate, the book, Dark Territory: The Secret History of Cyber War, reports that the secret NSA "Red Team" behind the clandestine exercise, dubbed "Eligible Receiver," was able to hack into the National Military Command Center on the very first day of the operation. Many of the compromised DoD's systems didn't require log-in credentials or the passwords were exceedingly simplistic, the book continued. NSA succeeded in proving they could disrupt America's command-control systems, shutting down and intercepting lines of communications, deleting files, and reformatting hard drives. The agency even found evidence that outside hackers had already penetrated some systems. (scmagazine.com, 07Mar16)

(U) Navy workforce memo separates cyber from IT

(U) The Defense Department has been restructuring its workforce in recent years to adapt to the challenges of its heavy reliance on cyberspace for missions. The Department of the Navy took a significant step on that front in a recent policy memo from Navy Secretary Ray Mabus that differentiates the IT and cybersecurity workforces. The memo, dated 10 February but released on a public-facing DOD website this week, establishes two workforce categories -- Cyber IT and Cybersecurity -- around which commanders are supposed to build training and credentialing. A cyber IT professional is defined as someone who builds, operates and maintains IT networks. Those duties include the retirement of legacy systems. A cybersecurity professional, on the other hand, is someone who defends and preserves data, networks and network-centric capabilities. Those duties include the "integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities," the memo states. The memo does not cover the DON cyber personnel who are allowed to conduct hacking operations on adversaries. The memo also addresses the so-called insider threat, which DOD officials have taken a keen interest in after the leaks of classified information by former National Security Agency contractor Edward Snowden. Anyone with privileged access to DON systems must adhere to a special agreement, and privileged access should be revoked when it is no longer needed, the memo states. The instruction applies to all DON installations, including those under the Marine Corps' charge. (fcw.com, 04Mar16)

(U) DARPA as the model for military cyber innovation

(U) After a tense week at the RSA Conference, during which government officials made impassioned overtures to private sector talent, federal officials are coming to realize that cooperation with the private sector may bear little resemblance to a traditional recruiting model. The Defense Advanced Research Projects Agency (DARPA) has provided the most successful model for public-private cooperation. During a talk at last week's RSA Conference, Defense Secretary Ashton Carter said the Defense Department will launch initiatives similar to the Innovation Advisory Board and 'Hack the Pentagon' program that receive government funding, but are organized through diverse structures such as grants, contractors, procurement, or other methods. "How much of it will it be a traditional military organization?" he said. The next generation of military innovation is more likely to resemble DARPA's model than a traditional military structure. One of DARPA's most public and ambitious projects, the Cyber Grand Challenge, has recruited teams of hackers and researchers from all over the world to create automated solutions to software vulnerabilities. The teams are competing against each other in writing programs that aim to change the balance of power between security professionals and remote attackers by writing code that discovers flaws. "Attackers have the concrete and inexpensive task of finding a single flaw to break a system," the Cyber Grand Challenge website stated. "Defenders on the other hand are required to anticipate and deny any possible flaw -- a goal both difficult to measure and expensive to achieve. Only automation can upend these economics." Each of the teams will present in August at the DEF CON Conference in Las Vegas. (scmagazine.com, 03Mar16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424