శ్రీ వేపచేదు విద్యా పీఠము

VEPACHEDU EDUCATIONAL FOUNDATION

The Andhra Journal of Industrial News

IP and Industry News

Issue 152

Dr. Rao Vepachedu[1], JD, PhD, LLM

CONTENTS

Issue 152

5118 Kali Era, 2074 Vikramarka Era, 1938 Salivahana Era
Swasti Sri **DURMUKHI** (దుర్ముఖి) Year, **PUSHYA** Month
DECEMBER, 2016 AD (Published online JANUARY 1, 2017)

DESIGN PATENTS IN RUSSIA

Per new administrative regulations, rules, and requirements for design patents in Russia, effective January 2016, a group of designs belonging to the same class can be filed in one application if the group consists of 1) a design relating to a set of articles and one or more designs relating to (an) article(s) of said set; or 2) designs which are variants of the same article and differ from each other only by unessential features or features defining a color combination. However, an article and its visible parts in one application are no longer permitted and the number of images per design in an application is limited to seven. If the application includes more than seven, Rospatent issues a formal office action and asks the applicant to inform which seven images the applicant wants to keep in the application.

TAIWAN and TPP

Taiwan does not have a patent linkage system currently. However, to join the Trans-Pacific Strategic Economic Partnership Agreement (TPP), the Taiwan Food and Drug Administration (TFDA) has drafted amendments of the Pharmaceutical Affairs Act (PAA) and held public hearings the amendments on 27 January 2016. The amendments are related to patent listings, patent declarations certified by an applicant filing an Abbreviated New Drug Application (ANDA), notification of the ANDA filing by the ANDA applicant to the New Drug Application (NDA) holder, stay of issuing market approval to the generics by the TFDA, and marketing exclusivity provision conferred to the first ANDA applicant who successfully defends a patent infringement suit. These amendments benefit the multinational companies with patented drug formulations based in the US and the EU.

Issue 152

5118 Kali Era, 2074 Vikramarka Era, 1938 Salivahana Era
Swasti Sri **DURMUKHI** (దుర్ముఖి) Year, **PUSHYA** Month
DECEMBER, 2016 AD (Published online JANUARY 1, 2017)

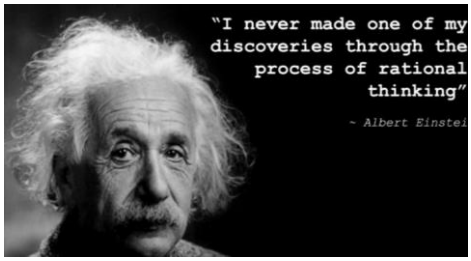
శ్రీ వేపచేదు విద్యా పీఠము

VEPACHEDU EDUCATIONAL FOUNDATION

The Andhra Journal of Industrial News

IP and Industry News

PRIVACY AND INTERNET OF THINGS, ARRAY OF THINGS & ARTIFICIAL INTELLIGENCE



Intelligence is the ability of an intelligent being to 1) learn, 2) infer general principles, 3) communicate in natural language, 4) plan, and 5) deal with new or unexpected problems. Scientists in the artificial intelligence (AI) create algorithms capable of learning, generalizing, communicating, planning, and extrapolating; but cannot yet determine which algorithm is better at any of these tasks. Devices and gadgets flood the marketplace for consumers who routinely switch from one brand to another because of alleged abilities and qualities. Some study the way algorithms interact with human beings, for example, using robots or avatars as the interaction test bed. Others study the mathematical foundations of the field, trying to find circumstances under which the performance of an algorithm can be guaranteed[2].

Learning - the acquisition of information, knowledge, or skill - through experience or education, which is fundamental to the rest of the abilities of the intelligent being. However, just learning alone is not enough to be intelligent, without the rest of the abilities.

Progress in information and communication technology (ICT) is changing the way human beings live, work, do business, educate, study, research, train, and entertain. An Information Society (IS) is a society in which the creation, distribution, and manipulation of information has become the most significant economic and cultural activity; in contrast to hunter-gatherer, nomadic, agrarian, industrial societies. The tools of the IS are computers and telecommunications. The communications technology would transform the world into a Global Village Of Information Society (GVOIS).

Internet Of Things (IOT)[3] is a global infrastructure for the GVOIS, enabling advanced services by interconnecting various objects based on existing and evolving interoperable information and communication technologies[4]. IOT

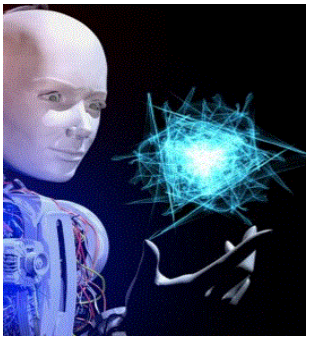
offers unparalleled opportunities to enhance efficiency, improve public safety, and support development. IOT is all about connectivity and capturing data using cellphones, tablets, connected vehicles and even things that the government has no access to, by embedding computational capability into everyday objects using pervasive or ubiquitous computing to enable them to communicate and perform useful tasks. Smart city planning[5] involves smart sensors and creating an IOT which converts inert objects into the dynamic world of information technology, encompassing technologies from sensors that monitor environmental conditions to RFID tags that can allow users to interact with objects using smart data in digital form actionable upon at the collection point for proper function. Smart data and smart sensors are crucial and integral to IOT environment to outfit objects including people with a unique identifier (UID) and the ability to transmit data over the Internet. For example, autonomous robots and smart cars need smart sensors for analysis of the data and to transmit smart data output instantaneously to actuators controlling the braking, delivery, steering, and guiding mechanisms.

Autonomous robots can also deliver goods using IOT, e.g., Redwood City in California started a pilot program of nine-month autonomous robotic delivery of parcels, groceries, and foods. Six-wheeled robots travel on city sidewalks, obey crosswalk signals, move out of the way of pedestrians, and deliver goods door-to-door. Delivery devices installed with nine cameras will help robots navigate the neighborhood and recognize people, animals, objects, and aids such as wheelchairs and scooters. Although designed for sidewalks, robots can negotiate small curbs[6]. Amazon has hired a former astronaut and some new engineers to make its Prime Air drone delivery service a reality. The company has also revealed new details about how far the drones can fly, and how much they can carry from Amazon's warehouse to your front door, Amazon is confident that Prime Air is possible[7].

The Array Of Things[8] (AOT)[9] is an expansion of the IOT use in systematic data collection for urban planning, critical to the success of the project. The data include engineering, local facts, relief and topography of the natural environment, legal systems, statutory requirements, and rights. Fundamental to any city planning is the accuracy and reliability of the data from the basic survey. In the next 20 years, local governments are partnering with startups and major technology companies experimenting with IOT across all dimensions of urban life at the cost projected to be about $ 41 trillion.

The AOT project for cities that have partnerships with higher education or research institutions because those places have the technical expertise to make the data actionable[10]. That gives experience to faculty members and scientists while simultaneously opening up learning opportunities for students. Open data is part of the impetus for city-university partnerships, opening more data than ever before for useful applications, and good data analysis enables city officials to make informed decisions in urban planning[11]. The AOT will start with Chicago and expand to Seattle, and to Bristol and Newcastle in the UK.

In Chicago, the AOT project will set up two sensor nodes at intersections along Damen Avenue to collect real-time data from diverse objects ranging from the amount of carbon monoxide in the air to the number of pedestrians crossing the street, and from utility poles to garbage bins. AOT is a collaboration of the Computation Institute, the University of Chicago, Argonne National Laboratory, and the School of the Art Institute of Chicago. Eventually, 500 such nodes will be installed in the city by the end of 2018 to augment the existing data. The amount of data available to the government, the computing, continue to multiply, the growing smart cities trend with the installation of networks of sensors on everything. The potential applications for the project are limitless. Some early applications include air pollution maps, congestion tracking, flood damage prediction, and so on. Seattle plans on modifying the nodes to help collect hyperlocal data on rainfall, enabling the city to forecast the time place of a flood accurately and respond accordingly[12].



IOT is going to be everywhere, with sensors and communication technologies embedded in all things bringing the cyber security to the forefront[13], together with the dangers lurking in the form of Artificial Intelligence (AI)[14] such as a Samaritan to defeat the Machine exist and are inevitable (PERSON OF INTEREST IN THE PERPETUAL LINE-UP)[15]. The Samaritan (the bad guy) or the Machine (the good guy) will take over the world, sooner or later.

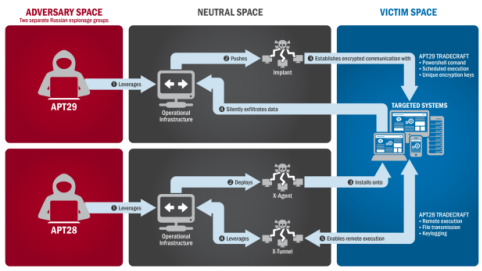
AI is capable of evaluating different system logs and traffic patterns within networks, and assessing different events triggered at firewalls or servers. AI can identify abnormalities such as failed passwords attempts or large amounts of data transferred to servers in different countries.

In 2016, Facebook has set a new world record by succeeding in transmitting data wirelessly at the speed of 20Gbps over a distance of 13 km between California and Malibu, which is essentially enough to steam almost 1,000 ultra high-definition videos at the same time, and much faster than any data transmission method we have today. Researchers have announced the development of robotic exoskeleton suits. Computer scientists have begun concentrating more efforts on building deep learning neural networks which are large webs of artificially intelligent classical computers that are trained using computer algorithms to solve complex problems in a similar way to the human central nervous system, and where different layers examine different parts of the problem to combine to produce an answer. US computer scientists have also managed to train a neural network to recognize faces from photographs, even if the images have been censored or blurred to hide the subject's identity. Meanwhile, in Finland, researchers have used neurobiology to train a neural network to learn to recognize and detect patterns all by itself, just like a human child would[16].

Researchers from Google, Harvard University, Lawrence Berkeley National Labs, Tufts University, UC Santa Barbara, and University College London successfully demonstrated the first ever completely scalable quantum simulation of a chemical reaction, showcasing a real-world use for quantum computers which could revolutionize multiple areas of research into medicine and materials[17]. Australian scientists have managed to develop the first ever qubit Fredkin gate, the universal gate required in all computing, while Oxford University has managed to develop quantum Fredkin gates that perform with record-breaking 99.9% precision. Scientists from the University of Sussex have invented a much simpler method of building quantum gates to replace laser beams with a voltage applied to microchips[18].

Progress in ICT and AI brings us data protection issues due to the possibility of hacking or steeling. Transfers of personal data are an important and necessary part of today's global digital economy. Many transactions involve the collection and use of personal data, for example, your name, phone number, birth date, home and email address, credit card number, national insurance or employee number, login name, gender and marital status, or any other kind of information that makes it possible to identify individuals. For instance, personal data may be collected by a company, for instance, when you buy goods or services online, when using social media or cloud storage services, or if you are an employee of a company to deal with personnel data.

The rapid pace of technological change and globalization have profoundly transformed the access to hackers, as explained above. As evidenced by recent breaches, hackers will do everything they can to break through firewalls and other security measures to gain access to vulnerable systems. Some hackers can stay undetected within systems for months and leave when they have captured the desired data.



About 4.5 million people who had their health and financial records exposed in a hack of the UCLA Health provider system. Yahoo confirmed one of the largest cyber security breaches ever, which compromised data associated with at least 500 million user accounts[19], and a different attack in 2013 compromised more than 1 billion accounts[20]. According to a Joint Analysis Report (JAR) entitled, GRIZZLY STEPPE – Russian Malicious Cyber Activity[21], the US Government confirms that two different RIS actors participated in the intrusion into a US political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

Both groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed crafting targeted spearphishing campaigns leveraging web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials. APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value. These groups use this information to craft highly targeted spearphishing campaigns. These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets.

The report further provides guidance in responding to unauthorized access to networks, suggesting to implement your security incident response and business continuity plan. It may take time for your organization's IT

professionals to isolate and remove threats to your systems and restore normal operations. Meanwhile, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures. Contact DHS or law enforcement immediately. NCCICCustomerService@hq.dhs.gov or 888-282-0870, the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance. The report further provides Detailed Mitigation Strategies[22].

Adding analytics and AI to the security mix may help prevent and detect future attacks. Based on the current gaps in security also adding the boom of the big data and analytics, the idea of use different ML algorithms that will help us to detect potential security breaches or misconfiguration in our environments take relevance[23].

At the Windows Hardware Engineering Community (WinHEC) event in Shenzhen, China, Microsoft and Intel announced a partnership for Project Evo, where the two companies will work on efforts in security, artificial intelligence and Cortana[24], and more. Microsoft's AI research hit a milestone already by achieving human parity, meaning that its AI can understand conversational speech as well as humans. These could all be among the first steps in Cortana's transition to the core product in Microsoft's portfolio. The Intel and Microsoft partnership will also focus on improving security capabilities, the release said, especially biometric authentication features such as Windows Hello. These security advances will also help to protect devices against evolving threats, with Intel providing security analytics as well.

The globalised nature of data flow poses new challenges for data protection supervisory authorities, as data moves from one jurisdiction to another. Due to the global nature of our GVOIS, to be able to do business, multinational corporations have to deal with different laws of different countries. For instance, an American company may collect data when Europeans buy goods, services, use social media, or cloud storage services; A EU-

based company may have the personal data of a European employee collected by its US subsidiary or US service provider.

Due to differences in privacy laws the US and the EU have developed a mechanism called Safe Harbor requiring Europeans continue to benefit from a high level of protection for the personal data in the US. When Safe Harbor fell short in protecting the personal data of Europeans[25], a new mechanism called US-EU Privacy Shield instituted this year.

The Privacy Shield allows personal data to be transferred from the EU to a company in the US, provided that the US company processes the personal data according to a strong set of data protection rules and safeguards. The protection given to personal data applies regardless of whether you are an EU citizen or not. To transfer personal data from the EU to the US different tools are available such as contractual clauses, binding corporate rules and the Privacy Shield. If the Privacy Shield is used, US companies must first sign up to this framework with the US Department of Commerce (USDC). The obligation applying to companies under the Privacy Shield are contained in the Privacy Principles. The USDC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. To be able to certify, companies must have a privacy policy in line with the Privacy Principles. They must renew their membership to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

If you want to know if a company in the US is part of the Privacy Shield, you can check the Privacy Shield List on the website of the USDC[26]. This list will give you details of all the companies taking part in the Privacy Shield, the kind of personal data they use, and the kind of services they offer. You can also find a list of companies that are no longer part of the Privacy Shield, i.e., they are no longer allowed to receive your personal data under the Privacy Shield. Also, these companies may only keep your personal data if they commit to the USDC that they will continue to apply the Privacy Principles[27].

Thus, multinational companies having operation in both the US and the EU must operate under the US privacy laws and the US-EU Privacy Shield. To be able to do business with the EU-based companies and multinational companies having EU branche, US-based Service Providers need to provide the required protections under the US-EU Privacy Shield[28], effective 12 July 2016.

COMMISSION'S CYBERSECURITY RECOMMENDATIONS

Computing technologies have enormous potential to improve the lives of all human beings. The interconnectedness and openness of a globalized economy made possible by the Internet and broader digital ecosystem create unparalleled value for the entire humanity and economic prosperity. However, technological advancement is outpacing security. Resilience must be a core component of any cybersecurity strategy; today's dynamic cyber threat environment demands a risk management approach for responding to and recovering from an attack. Recognizing the extraordinary benefit interconnected technologies bring to our digital economy and equally mindful of the accompanying challenges posed by threats to the security of the cyber landscape, President Obama established a Commission on Enhancing National Cybersecurity and directed the Commission to assess the state of our nation's cybersecurity. He charged this group with developing actionable recommendations for securing the digital economy while protecting privacy, ensuring public safety and economic and national security, and fostering the discovery and development of new technical solutions. After due deliberations, the Commission has identified six major imperatives, which together contain a total of 16 recommendations and 53 associated action items.

IMPERATIVE 1: Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks

Recommendation 1.1 The private sector and the Administration should collaborate on a roadmap for improving the security of digital networks, in particular by achieving robustness against denial-of service, spoofing, and other attacks on users and the nation's network infrastructure.

Action Item 1.1.1 The President should direct senior federal executives to launch a private–public initiative, including provisions to undertake, monitor, track, and report on measurable progress in enabling agile, coordinated responses and mitigation of attacks on the users and the nation's network infrastructure. (SHORT TERM)

Recommendation 1.2 As our cyber and physical worlds increasingly converge, the federal government should work closely with the private sector to define and implement a new model for how to defend and secure this infrastructure.

Action Item 1.2.1 The President should create, through executive order, the National Cybersecurity Private–Public Program (NCP3) as a forum for addressing cybersecurity issues through a high-level, joint public—private collaboration. (SHORT TERM)

Action Item 1.2.2 The private sector and Administration should launch a joint cybersecurity operation program for the public and private sectors to collaborate on cybersecurity activities in order to identify, protect from, detect, respond to, and recover from cyber incidents affecting critical infrastructure (CI). (MEDIUM TERM)

Action Item 1.2.3 The federal government should provide companies the option to engage proactively and candidly in formal collaboration with the government to advance cyber risk management practices and to establish a well-coordinated joint defense plan based on the principles of the Cybersecurity Framework. (SHORT TERM)

Action Item 1.2.4 Federal agencies should expand the current implementation of the information-sharing strategy to include exchange of information on organizational interdependencies within the cyber supply chain. (SHORT TERM)

Action Item 1.2.5 With the increase in wireless network communications across all organizations, and the nation's growing reliance on the Global Positioning System (GPS) to provide positioning, navigation, and timing (PNT), cybersecurity strategies must specifically address the full range of risks across the electromagnetic spectrum. An immediate goal should be enhancing the nation's ability to detect and resolve purposeful wireless disruptions and to improve the resilience and reliability of wireless communications and PNT data. (SHORT TERM)

Recommendation 1.3: The next Administration should launch a national public–private initiative to achieve major security and privacy improvements by increasing the use of strong authentication to improve identity management.

Action Item 1.3.1: The next Administration should require that all Internet-based federal government services provided directly to citizens require the use of appropriately strong authentication. (SHORT TERM)

Action Item 1.3.2: The next Administration should direct that all federal agencies require the use of strong authentication by their employees, contractors, and others using federal systems+. (SHORT TERM)

Action Item 1.3.3: The government should serve as a source to validate identity attributes to address online identity challenges. (MEDIUM TERM)

Action Item 1.3.4: The next Administration should convene a body of experts from the private and public sectors to develop identity management requirements for devices and processes in support of specifying the sources of data. (SHORT TERM)

Recommendation 1.4: The next Administration should build on the success of the Cybersecurity Framework to reduce risk, both within and outside of critical infrastructure, by actively working to sustain and increase use of the Framework.

Action Item 1.4.1: NIST, in coordination with the NCP 3, should establish a Cybersecurity Framework Metrics Working Group (CFMWG) to develop industry-led, consensus-based metrics that may be used by (1) industry to voluntarily assess relative corporate risk, (2) the Department of Treasury and insurers to understand insurance coverage needs and standardize premiums, and (3) DHS to implement a nationwide voluntary incident reporting program for identifying cybersecurity gaps. This reporting program should include a cyber incident data and analysis repository (CIDAR). (SHORT TERM)

Action Item 1.4.2: All federal agencies should be required to use the Cybersecurity Framework. (SHORT TERM)

Action Item 1.4.3: Regulatory agencies should harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management—reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation. (SHORT TERM)

Action Item 1.4.4: The private sector should develop conformity assessment programs that are effective and efficient, and that support the international trade and business activities of US companies. (SHORT TERM) Action Item 1.4.5: The government should extend additional incentives to companies that have implemented cyber risk management principles and demonstrate collaborative engagement. (SHORT TERM)

Recommendation 1.5: The next Administration should develop concrete efforts to support and strengthen the cybersecurity of small and medium-sized businesses (SMBs).

Action Item 1.5.1: The National Institute of Standards and Technology (NIST) should expand its support of SMBs in using the Cybersecurity Framework and should assess its cost-effectiveness specifically for SMBs. (SHORT TERM)

Action Item 1.5.2: DHS and NIST, through the National Cybersecurity Center of Excellence (NCCoE), in collaboration with the private sector, should develop blueprints for how to integrate and use existing cybersecurity technologies, with a focus on meeting the needs of SMBs. (SHORT TERM)

Action Item 1.5.3: Sector-specific agencies (SSAs) and industry associations and organizations should collaborate to develop a program to review past public cyber-attacks to identify lessons learned from the event, including a focus on application to SMBs. (SHORT TERM)

Imperative 2: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy

Recommendation 2.1 The federal government and private-sector partners must join forces rapidly and purposefully to improve the security of the Internet of Things (IoT).

Action Item 2.1.1 To facilitate the development of secure IoT devices and systems, within 60 days the President should issue an executive order directing NIST to work with industry and voluntary standards organizations to identify existing standards, best practices, and gaps for deployments ranging from critical systems to consumer/commercial uses—and to jointly and rapidly agree on a comprehensive set of risk-based security standards, developing new standards where necessary. (SHORT TERM)

Action Item 2.1.2 Regulatory agencies should assess whether effective cybersecurity practices and technologies that are identified by the standards process in Action Item 2.1.1 are being effectively and promptly implemented to improve cybersecurity and should initiate any appropriate rule-making to address the gaps. (MEDIUM TERM)

Action Item 2.1.3 The Department of Justice should lead an interagency study with the Departments of Commerce and Homeland Security and work with the Federal Trade Commission, the Consumer Product Safety Commission, and interested private-sector parties to assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days. (SHORT TERM)

Action Item 2.1.4 The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) should develop and communicate guidelines for IoT cybersecurity and privacy best practices for rapid deployment and use. (SHORT TERM)

Recommendation 2.2 The federal government should make the development of usable, affordable, inherently secure, defensible, and resilient/recoverable systems its top priority for cybersecurity research and development (R&D) as a part of the overall R&D agenda.

Action Item 2.2.1 The Director of the Office of Science and Technology Policy (OSTP) should lead the development of an integrated government–private-sector cybersecurity roadmap for developing usable, affordable, inherently secure, resilient/recoverable, privacy-protecting, functional, and defensible systems. This effort should be backed by a significant R&D funding increase in the President's Budget Request for agencies supporting this roadmap. (SHORT TERM)

Action Item 2.2.2 The U.S. government should support cybersecurity-focused research into traditionally underfunded areas, including human factors and usability, policy, law, metrics, and the social impacts of privacy and security technologies, as well as issues specific to small and medium-sized businesses where research can provide practical solutions. (SHORT TERM)

Imperative 3: Prepare Consumers to Thrive in a Digital Age

Recommendation 3.1 Business leaders in the information technology and communications sectors need to work with consumer organizations and the Federal Trade Commission (FTC) to provide consumers with better information so that they can make informed decisions when purchasing and using connected products and services.

Action Item 3.1.1 To improve consumers' purchasing decisions, an independent organization should develop the equivalent of a cybersecurity "nutritional label" for technology products and services— ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand. (SHORT AND MEDIUM TERM)

Action Item 3.1.2. Within the first 100 days of the new Administration, the White House should convene a summit of business, education, consumer, and government leaders at all levels to plan for the launch of a new national cybersecurity awareness and engagement campaign. (SHORT TERM)

Action Item 3.1.3 The FTC should convene consumer organizations and industry stakeholders in an initiative to develop a standard template for documents that inform consumers of their cybersecurity roles and responsibilities as citizens in the digital economy—along with a "Consumer's Bill of Rights and Responsibilities for the Digital Age." (MEDIUM TERM)

Recommendation 3.2 The federal government should establish, strengthen, and broaden investments in research programs to improve the cybersecurity and usability of consumer products and digital technologies through greater understanding of human behaviors and their interactions with the Internet of Things (IoT) and other connected technologies.

Action Item 3.2.1 The next Administration and Congress should prioritize research on human behavior and cybersecurity, by the 2016 Federal Cybersecurity Research and Development Strategic Plan. (SHORT TERM)

Imperative 4: Build Cybersecurity Workforce Capabilities

Recommendation 4.1: The nation should proactively address workforce gaps through capacity building, while simultaneously investing in innovations—such as automation, machine learning, and artificial intelligence—that will redistribute the future required workforce.

Action Item 4.1.1: The next President should initiate a national cybersecurity workforce program to train 100,000 new cybersecurity practitioners by 2020. (SHORT TERM)

Action Item 4.1.2: The next President should initiate a national cybersecurity apprenticeship program to train 50,000 new cybersecurity practitioners by 2020. (MEDIUM TERM)

Action Item 4.1.3: To better prepare students as individuals and future employees, federal programs supporting education at all levels should incorporate cybersecurity awareness for students as they are introduced to and provided with Internet-based devices. (SHORT TERM)

Action Item 4.1.4: The federal government should develop a mandatory training program to introduce managers and executives to cybersecurity risk management topics—even if their role is not focused on a cybersecurity mission area—so that they can create a culture of cybersecurity in their organizations. (SHORT TERM)

Action Item 4.1.5: The federal government, SLTT governments, and private-sector organizations should create an exchange program aimed at increasing the cybersecurity experience and capabilities of mid-level and senior-level employees. (SHORT TERM)

Action Item 4.1.6: The Office of Personnel Management (OPM) should establish a Presidential Cybersecurity Fellows program for federal civilian agencies with the goal of bringing on 200 cybersecurity specialists by 2020. (SHORT TERM)

Action Item 4.1.7: NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the Department of Education should work with private-sector organizations, universities, and professional societies to develop standardized interdisciplinary cybersecurity curricula that integrate with and expand existing efforts and programs. (MEDIUM TERM)

Action Item 4.1.8: In order to attract more students to pursue cybersecurity degree programs and enter the cybersecurity workforce in both the public and private sectors, incentives should be offered to reduce student debt or subsidize the cost of education through a public–private partnership. (MEDIUM TERM)

Imperative 5: Better Equip Government to Function Effectively and Securely in the Digital Age

Recommendation 5.1: The federal government should take advantage of its ability to share components of the information technology (IT) infrastructure by consolidating basic network operations.

Action Item 5.1.1: The Administration should establish a program to consolidate all civilian agencies' network connections (as well as those of appropriate government contractors) into a single consolidated network. This program and the consolidated network should be administered by the newly established cybersecurity and infrastructure protection agency described in Action Item 5.5.2. (MEDIUM TERM)

Recommendation 5.2: The President and Congress should promote technology adoption and accelerate the pace at which technology is refreshed within the federal sector.

Action Item 5.2.1: The Administration should expand on the recently proposed Information Technology Modernization Fund (ITMF) to enable agencies to fund technology investments by spreading costs over a predetermined period of time. The investments made under this fund should be integrated into a rolling 10-year strategic investment plan as part of a budget planning process similar to the Department of Defense (DoD) approach. (SHORT TERM)

Action Item 5.2.2: The General Services Administration (GSA) should lead efforts on integrating technology more effectively into government operations, working with Congress to reform federal procurement requirements and expanding the use of sharing standard service platforms. (MEDIUM TERM)

Recommendation 5.3: Move federal agencies from a cybersecurity requirements management approach to one based on enterprise risk management (ERM).

Action Item 5.3.1: The Office of Management and Budget (OMB) should require federal agencies to use the Cybersecurity Framework for any cybersecurity-related reporting, oversight, and policy review or creation. (SHORT TERM)

Action Item 5.3.2: In the first 100 days of the Administration, OMB should work with NIST and DHS to clarify agency and OMB responsibilities under the Federal Information Security Modernization Act (FISMA) to align with the Cybersecurity Framework. (SHORT TERM)

Action Item 5.3.3: OMB should integrate cybersecurity metrics with agency performance metrics, review these metrics biannually, and integrate metrics and associated performance with the annual budget process. (SHORT TERM) Recommendation 5.4: The federal government should better match cybersecurity responsibilities with the structure of and positions in the Executive Office of the President.

Action Item 5.4.1: The President should appoint and empower an Assistant to the President for Cybersecurity, reporting through the National Security Advisor, to lead national cybersecurity policy and coordinate implementation of cyber protection programs. (SHORT TERM)

Action Item 5.4.2: The Administration should clarify OMB's role—and specifically, that of the Federal Chief Information Officer (CIO), the Federal Chief Information Security Officer (CISO), and the Senior Advisor for Privacy—in managing cyber-security-related operations in all agencies. (SHORT TERM)

Recommendation 5.5: Government at all levels must clarify its cybersecurity mission responsibilities across departments and agencies to protect and defend against, respond to and recover from cyber incidents.

Action Item 5.5.1: The President should issue a National Cybersecurity Strategy within the first 180 days of his Administration. (SHORT TERM)

Action Item 5.5.2: Congress should consolidate cybersecurity and infrastructure protection functions under the oversight of a single federal agency, and ensure this agency has the appropriate capabilities and responsibilities to execute its mission. (SHORT TERM)

Action Item 5.5.3: The governors in each state should consider seeking necessary legislative authority and resources to train and equip the National Guard to serve as part of the nation's cybersecurity defense. (SHORT–MEDIUM TERM)

Imperative 6: Ensure an Open, Fair, Competitive, and Secure Global Digital Economy

Recommendation 6.1: The Administration should encourage and actively coordinate with the international community in creating and harmonizing cybersecurity policies and practices and common international agreements on cybersecurity law and global norms of behavior.

Action Item 6.1.1: Within the first 180 days of the next Administration, the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices. (SHORT TERM)

Action Item 6.1.2: The federal government should increase its engagement in the international standards arena to garner consensus from other nations and promote the use of sound, harmonized cybersecurity standards. (MEDIUM TERM)

Action Item 6.1.3: The Department of State should continue its work with like-minded nations to promote peacetime cybersecurity norms of behavior. (SHORT TERM)

Action Item 6.1.4: Congress should provide sufficient resources to the Department of Justice (DOJ) to fully staff and modernize the Mutual Legal Assistance Treaty (MLAT) process, including hiring engineers and investing in technology that enables efficiency. It should also amend U.S. law to facilitate trans-border access to electronic evidence for limited legitimate investigative purposes, and should provide resources for the development of a broader framework and standards to enable this trans-border access. (MEDIUM TERM)

Action Item 6.1.5: NIST and the Department of State should proactively seek international partners to extend the Cybersecurity Framework's approach to risk management to a broader international market. (SHORT TERM)

Action Item 6.1.6: The Department of State, DHS, and other agencies should continue to assist countries with cybersecurity capacity building in light of growing needs and recent developments. (SHORT TERM)

Issue 152

5118 Kali Era, 2074 Vikramarka Era, 1938 Salivahana Era
Swasti Sri **DURMUKHI** (దుర్ముఖి) Year, **PUSHYA** Month
DECEMBER, 2016 AD (Published online JANUARY 1, 2017)

THE RICH, THE POOR AND THE DIVIDE

> ***The average graduate from a top school is making nearly a hundred and twenty thousand dollars a year, the average graduate from a moderately selective school is making ninety thousand dollars[29].***

The admission[30] requirements of American colleges and universities have been the subject of considerable speculation and investigation since Harvard College first set up its requirements for admission in 1642. They adopted the College Entrance Examination Board tests as the principal basis for admission in 1905. As a result, virtually any academically gifted high school senior who could afford a private college had a straightforward shot at attending one. Soon the sons of wealthy WASP alumni were displaced by other communities, even when they were not desirable at the time. To solve this problem, Ivy Leagues required applicants to answer questions on Race and Color, Religious Preference, Maiden Name of Mother, Birthplace of Father, and what change, if any, has been made since birth in the name. As a result, the percentage of Jews at Harvard went down.

The modern-day application began to take shape by the 1940s. In 1946, students were asked to submit references, a letter from their principal, and complete an admissions interview. During the ten-year period, 1946 to 1956, college entrance requirements reached a fairly uniform level. During the decade of the1960s, emphasis on environmental and non-intellective factors in the admission process increased. By the nineteen-sixties, Harvard's admissions system had evolved into a series of complex algorithms lumping all applicants into one of twenty-two dockets according to their geographical origin. In the nineteen-eighties, Harvard enforced a quota against Asians. Once adjusted for the preferences given to athletes and the children of alumni, Asians had no chance. If Harvard had too many Asians, it wouldn't be Harvard[31]. At this time Asians were Asians only, while the Indians of the Indian Continent were whites.

Today, the admissions committee asks students for a broad range of information, from extracurricular activities to financial-aid information, SAT and ACT scores, and also keeps track of a student's level of interest based on student's visit to the institution, a new fad in America. Almost every high school counselor in America advises the students to visit as many colleges as possible to determine whether a college is a right place for a student[32]. It is believed that visiting a college campus helps to get a sense of what a college and life at that college is like and helps decide whether the college is the right one for the prospective student. A campus visit not only will help to narrow down the choices but it can have benefits such as acting as a real motivator for the student to do well academically as well as in extracurricular activities. It will give a clearer picture about the college environment and

it can act as an ideal opportunity for parents and students to talk about this very important decision. They say a visit gives the chance to talk to students, faculty, and financial aid and admission officers[33].

Schools offer campus visit programs throughout the year for prospective students. Campus visit programs are free, although registration is required. However, travel and hotel costs are to be borne by the families. This fad can separate the haves and the have-nots of America, based on the report based on information collected in the 2016 and earlier Current Population Survey Annual Social and Economic Supplements (CPS ASEC) conducted by the US Census Bureau[34]. For instance, in 2015, 33.6% of children represented the population in families with income below 50% of their poverty threshold. Obviously, 33.6% of children will not be amking those expensive trips to various universities to gain an advantage in the selection process[35].

REFERENCES AND NOTES[36]

[1] Dr. Rao Vepachedu is a registered patent attorney with extensive experience in the management of intellectual property and extensive experience in research and teaching. He currently works for Cardinal Intellectual Property (CIP), Cardinal Risk Management (CRM), and Cardinal Law Group (CLG). In addition, he is the president of Vepachedu Educational Foundation Inc. (www.vepachedu.org), a 501(c) (3) educational foundation. For more information visit: www.linkedin.com/in/vepachedu; http://www.avvo.com/attorneys/60201-il-sreenivasarao-vepachedu-764535.html, and http://www.crm-ip.com/vepachedu.html. Contact: svepachedu@yahoo.com or rao.vepachedu@cardinal-ip.com: www.linkedin.com/in/vepachedu and http://www.crm-ip.com/vepachedu.html;

http://www.avvo.com/profile/dashboard.

[2] ARTIFICIAL INTELLIGENCE, ROBOTICS, AND CYBERNETICS: https://www.ece.illinois.edu/academics/ugrad/subdisciplines/robotics.asp

[3] The Internet of Things, Opportunities and Applications across Industries: http://www.sas.com/en_us/offers/sem/iia-internet-of-things-108110.html?keyword=internet+of+things&matchtype=p&publisher=google&gclid=CPTXtc2M7dACFVKewAod5IAPpw

[4] What is the Internet of Things? http://www.govtech.com/fs/What-is-the-Internet-of-Things.html

[5] The Urban Internet of Things, Surveying Innovations Across City Systems: http://datasmart.ash.harvard.edu/news/article/the-urban-internet-of-things-727

[6] Autonomous Delivery Robots to Hit Redwood City, Calif., Streets in December: http://www.govtech.com/fs/Autonomous-Delivery-Robots-to-Hit-Redwood-City-Calif-Streets-in-December.html

[7] Amazon 'beefs up' Prime Air drone delivery service with new staff and a Nasa astronaut: http://www.ibtimes.co.uk/amazon-beefs-prime-air-drone-delivery-service-new-staff-nasa-astronaut-1538812

[8] 'Array of Things' Expands to Cities with Research Partnerships http://www.govtech.com/Array-of-Things-Expands-to-Cities-with-Research-Partnerships.html

[9] Array of Things Introductory Video: https://news.uchicago.edu/multimedia/array-things-introductory-video

[10] Do Universities, Research Institutions Hold the Key to Open Data's Next Chapter? http://www.govtech.com/dc/articles/Do-Universities-Research-Institutions-Hold-the-Key-to-Open-Datas-Next-Chapter.html

[11] Bauer, City Planning for Civil Engineers, Environmental Engineers, and Surveyors, CRC Press, September 22, 2009
Ceder, Public Transit Planning and Operation: Modeling, Practice and Behavior, Second Edition, CRC Press, July 17, 2015

[12] Expanding Array of Things Aims to Help Put Data to Work for Cities: http://www.govtech.com/fs/insights/Expanding-Array-of-Things-Aims-to-Help-Put-Data-to-Work-for-

Cities.html?utm_source=related&utm_medium=direct&utm_campaign=Expanding-Array-of-Things-Aims-to-Help-Put-Data-to-Work-for-Cities

[13] CYBERSECURITY COMMISSION'S RECOMMENDATIONS TO THE NEXT ADMINISTRATION: https://www.linkedin.com/pulse/cybersecurity-commissions-recommendations-next-rao-vepachedu?trk=mp-author-card

[14] A Very Short History Of Artificial Intelligence (AI): http://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/#16a59cd4188d

Top 20 Artificial Intelligence Engineering Schools in the US 2016: http://www.computersciencedegreehub.com/best/artificial-intelligence-engineering-schools/

[15] PERSON OF INTEREST IN THE PERPETUAL LINE-UP: https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=PERSON+OF+INTEREST+IN+THE+PERPETUAL+LINE-UP

PERSON OF INTEREST http://www.cbs.com/shows/person_of_interest/

[16] The best technology breakthroughs in 2016 from quantum computing to AI: http://www.ibtimes.co.uk/best-technology-breakthroughs-2016-quantum-computing-ai-1598710

[17] Google boasts quantum computing breakthrough with first display of real-world use. http://www.ibtimes.co.uk/google-boasts-quantum-computing-breakthrough-first-display-real-world-use-1571823

[18] The best technology breakthroughs in 2016 from quantum computing to AI: http://www.ibtimes.co.uk/best-technology-breakthroughs-2016-quantum-computing-ai-1598710

[19] Yahoo says 500 million accounts stolen: http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/

[20] Yahoo Says 1 Billion User Accounts Were Hacked: http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

[21] Joint Analysis Report (JAR) entitled, GRIZZLY STEPPE – Russian Malicious Cyber Activity: https://assets.documentcloud.org/documents/3248231/Report-on-Russian-Hacking.pdf

[22] *Id*

Detailed Mitigation Strategies

Protect Against SQL Injection and Other Attacks on Web Services

Routinely evaluate known and published vulnerabilities, perform software updates and technology refreshes periodically, and audit external-facing systems for known Web application vulnerabilities. Take steps to harden both Web applications and the servers hosting them to reduce the risk of network intrusion via this vector.1

• Use and configure available firewalls to block attacks.

• Take steps to further secure Windows systems such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.

• Monitor and remove any unauthorized code present in any www directories.

• Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) and response to these protocols as much as possible.

• Remove non-required HTTP verbs from Web servers as typical Web servers and applications only require GET, POST, and HEAD.

• Where possible, minimize server fingerprinting by configuring Web servers to avoid responding with banners identifying the server software and version number.
• Secure both the operating system and the application.
• Update and patch production servers regularly.
• Disable potentially harmful SQL-stored procedure calls.
• Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
• Consider using type-safe stored procedures and prepared statements.
• Perform regular audits of transaction logs for suspicious activity.
• Perform penetration testing against Web services.
• Ensure error messages are generic and do not expose too much information.

Phishing and Spearphishing

• Implement a Sender Policy Framework (SPF) record for your organization's Domain Name System (DNS) zone file to minimize risks relating to the receipt of spoofed messages.
• Educate users to be suspicious of unsolicited phone calls, social media interactions, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
• Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
• Do not reveal personal or financial information in social media or email, and do not respond to solicitations for this information. This includes following links sent in email.
• Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL often includes a variation in spelling or a different domain than the valid website (e.g., .com vs. .net).
• If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
• Take advantage of anti-phishing features offered by your email client and web browser.
• Patch all systems for critical vulnerabilities, prioritizing timely patching of software that processes Internet data, such as web browsers, browser plugins, and document readers.

Permissions, Privileges, and Access Controls

• Reduce privileges to only those needed for a user's duties.
• Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
• Carefully consider the risks before granting administrative rights to users on their own machines.

Issue 152
5118 Kali Era, 2074 Vikramarka Era, 1938 Salivahana Era
Swasti Sri **DURMUKHI** (దుర్ముఖి) Year, **PUSHYA** Month
DECEMBER, 2016 AD (Published online JANUARY 1, 2017)

• Scrub and verify all administrator accounts regularly.
• Configure Group Policy to restrict all users to only one login session, where possible.
• Enforce secure network authentication where possible.
• Instruct administrators to use non-privileged accounts for standard functions such as Web browsing or checking Web mail.
Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
• Configure firewalls to disallow RDP traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary VPN with lower privileges.
• Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.
• Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. This can be indicative of failed intrusion activity.
• If remote access between zones is an unavoidable business need, log and monitor these connections closely.
• In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.
Credentials
• Enforce a tiered administrative model with dedicated administrator workstations and separate administrative accounts that are used exclusively for each tier to prevent tools, such as Mimikatz, for credential theft from harvesting domain-level credentials.
• Implement multi-factor authentication (e.g., smart cards) or at minimum ensure users choose complex passwords that change regularly.
• Be aware that some services (e.g., FTP, telnet, and .rlogin) transmit user credentials in clear text. Minimize the use of these services where possible or consider more secure alternatives.
• Properly secure password files by making hashed passwords more difficult to acquire. Password hashes can be cracked within seconds using freely available tools. Consider restricting access to sensitive password hashes by using a shadow password file or equivalent on UNIX systems.
• Replace or modify services so that all user credentials are passed through an encrypted channel.
• Avoid password policies that reduce the overall strength of credentials. Policies to avoid include lack of password expiration date, lack of lockout policy, low or disabled password complexity requirements, and password history set to zero.
• Ensure that users are not re-using passwords between zones by setting policies and conducting regular audits.
• Use unique passwords for local accounts for each device.
Logging Practices
• Ensure event logging (applications, events, login activities, security attributes, etc.) is turned on or monitored for identification of security issues.

Issue 152

5118 Kali Era, 2074 Vikramarka Era, 1938 Salivahana Era
Swasti Sri **DURMUKHI** (దుర్ముఖి) Year, **PUSHYA** Month
DECEMBER, 2016 AD (Published online JANUARY 1, 2017)

• Configure network logs to provide enough information to assist in quickly developing an accurate determination of a security incident.
• Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
• Secure logs, potentially in a centralized location, and protect them from modification.
• Prepare an incident response plan that can be rapidly implemented in case of a cyber intrusion.

How to Enhance Your Organization's Cybersecurity Posture

DHS offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Other resources include:

• The Cyber Security Advisors (CSA) program bolsters cybersecurity preparedness, risk mitigation, and incident response capabilities of critical infrastructure entities and more closely aligns them with the Federal Government. CSAs are DHS personnel assigned to districts throughout the country and territories, with at least one advisor in each of the 10 CSA regions, which mirror the Federal Emergency Management Agency regions. For more information, email cyberadvisor@hq.dhs.gov.
• Cyber Resilience Review (CRR) is a no-cost, voluntary assessment to evaluate and enhance cybersecurity within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators of an entity's operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress and crisis. Visit https://www.cert.org/resilience/rmm.html to learn more about the CERT Resilience Management Model.
• Enhanced Cybersecurity Services (ECS) helps critical infrastructure owners and operators protect their systems by sharing sensitive and classified cyber threat information with Commercial Service Providers (CSPs) and Operational Implementers (OIs). CSPs then use the cyber threat information to protect CI customers. OIs use the threat information to protect internal networks. For more information, email ECS_Program@hq.dhs.gov.
• The Cybersecurity Information Sharing and Collaboration Program (CISCP) is a voluntary information-sharing and collaboration program between and among critical
infrastructure partners and the Federal Government. For more information, email
CISCP@us-cert.gov.
• The Automated Indicator Sharing (AIS) initiative is a DHS effort to create a system where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS will not eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

AIS participants connect to a DHS-managed system in the NCCIC that allows bidirectional sharing of cyber threat indicators. A server housed at each participant's location allows each to exchange indicators with the NCCIC. Participants will not only

receive DHS-developed indicators, but can share indicators they have observed in their own network defense efforts, which DHS will then share with all AIS participants. For more information, visit https://www.dhs.gov/ais.

• The Cybersecurity Framework (Framework), developed by the National Institute of Standards and Technology (NIST) in collaboration with the public and private sectors, is a tool that can improve the cybersecurity readiness of entities. The Framework enables entities, regardless of size, degree of cyber risk, or cyber sophistication, to apply principles and best practices of risk management to improve the security and resiliency of critical infrastructure. The Framework provides standards, guidelines, and practices that are working effectively today. It consists of three parts—the Framework Core, the Framework Profile, and Framework Implementation Tiers—and emphasizes five functions: Identify, Protect, Detect, Respond, and Recover. Use of the Framework is strictly voluntary. For more information, visit https://www.nist.gov/cyberframework or email cyberframework@nist.gov.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. Include the JAR reference number (JAR-16-20296) in the subject line of all email correspondence. For any questions related to this report, please contact NCCIC or the FBI.

NCCIC:
Phone: +1-888-282-0780
Email: NCCICCustomerService@hq.dhs.gov

FBI:
Phone: +1-855-292-3937
Email: cywatch@ic.fbi.gov

Feedback

NCCIC continuously strives to improve its products and services. You can help by answering a few short questions about this product at the following URL:
https://www.us-cert.gov/forms/feedback.

[23] SECURITY FROM THE BIG DATA AND ANALYTICS PERSPECTIVE: https://allthingsopen.org/talk/security-from-the-big-data-and-analytics-perspective/

Stop a healthcare data breach with help from analytics, AI: http://searchhealthit.techtarget.com/tip/Stop-a-healthcare-data-breach-with-help-from-analytics-AI

IBM and Cisco snuggle up to add Watson AI and edge analytics to the IoT: http://www.theinquirer.net/inquirer/news/2460414/ibm-and-cisco-snuggle-up-to-add-watson-ai-and-edge-analytics-to-the-iot

[24] The story of Cortana, Microsoft's Siri killer: http://www.theverge.com/2014/4/2/5570866/cortana-windows-phone-8-1-digital-assistant

Cortana vs. Siri vs. Google Now: An early look at how Cortana stacks up (hands-on): https://www.cnet.com/news/cortana-vs-siri-vs-google-now/

[25] EU Court Says Data-Transfer Pact With U.S. Violates Privacy: http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361
Safe Harbor Is Dead; Long Live the Privacy Shield: http://www.americanbar.org/publications/blt/2016/05/09_alvarez.html
[26] Privacy Shield: https://www.privacyshield.gov/welcome
[27] GUIDE TO THE US-EU PRIVACY SHIELD: http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf
[28] How will the EU's reform adapt data protection rules to new technological developments?
http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_technological_developments_2016_en.pdf
[29] GETTING IN, The social logic of Ivy League admissions, A CRITIC AT LARGE, THE NEW YORKER, OCTOBER 10, 2005
[30] How Getting Into College Became Such a Long, Frenzied, Competitive Process
College Admissions: A Lesson in History
The evolution of college admission Requirements
Review: The History of University Admissions
[31] GETTING IN, The social logic of Ivy League admissions, A CRITIC AT LARGE, THE NEW YORKER, OCTOBER 10, 2005
[32] Campus Visits and College Interviews, https://www.amazon.com/Campus-Visits-College-Interviews-Board/dp/0874479886
[33] Big Future: Campus Visit Checklist
HOW IMPORTANT IS A CAMPUS VISIT?
http://www.selectingcolleges.com/home/col/page_180/how_important_is_a_campus_visit_2.html
BENEFITS OF CAMPUS VISITS: http://stemstudy.com/benefits-of-campus-visits/
[34] Income and Poverty in the United States: 2015; Current Population Reports:
http://www.census.gov/content/dam/Census/library/publications/2016/demo/p60-256.pdf
[35] *Id,* pg 18
[36] In addition to the primary sources cited above, additional references include:
New York Times, Washington Post, Mercury News, Bayarea.com, Deccan Chronicle, the Hindu, Hindustan Times, Times of India, AP, Reuters, AFP, The Guardian, Pravda, Spiegel, Connexion, etc.

Disclaimer *All information is intended for your general knowledge only and is not a substitute for medical advice or treatment for special medical conditions or any specific health issues or starting a new fitness regimen.*

> *"Where the mind is without fear and the head is held high, Where knowledge is free Where the world has not been broken up into fragments, By narrow domestic walls."* Rabindranath Tagore (1861-1941), Gitanjali, 1912.

One World One Family
AUM! SWASTI!

Issue 152

5118 Kali Era, 2074 Vikramarka Era, 1938 Salivahana Era
Swasti Sri **DURMUKHI** (దుర్ముఖి) Year, **PUSHYA** Month
DECEMBER, 2016 AD (Published online JANUARY 1, 2017)

Om! Asatoma Sadgamaya, Tamasoma Jyotirgamaya, Mrityorma Amritamgamaya, Om Shantih, Shantih, Shantih! (Aum! Lead the world from wrong path to the right path, from ignorance to knowledge, from mortality to immortality, and peace!)
SWASTI! AUM!

Issue 152

5118 Kali Era, 2074 Vikramarka Era, 1938 Salivahana Era
Swasti Sri **DURMUKHI** (దుర్ముఖి) Year, **PUSHYA** Month
DECEMBER, 2016 AD (Published online JANUARY 1, 2017)