Welcome to the Cyveillance Weekly Trends Report

Greetings from Cyveillance, the leader in open source threat intelligence. Since threat intelligence is constantly evolving, we publish this newsletter to keep our customers updated on the latest threats to various industries. Each week, we’ll send you highlights from our analyst research reports. You can unsubscribe at any time. For the latest security news stories throughout the day, you can also follow us on Twitter, or to view the latest security articles from Cyveillance experts, subscribe to our blog.

In this Issue:

- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance / Healthcare
- Financial Services
- Global Intelligence
- Legal and Regulations

Top Incidents

Beyond Buzzwords: Defining Threat Intelligence and Why It Matters: In this webcast, the first in a two-part series, we’ll look at what defines threat intelligence, and why not knowing what it is can cost your organization and hurt your security posture.

What you’ll learn in this webcast:
- What characterizes true threat intelligence
- Why what you don’t know about threat intelligence could cost you
- How to evaluate threat intelligence solutions
Energy

- BusinessWeek.com reports that hedge fund billionaire Tom Steyer, a climate change activist and staunch opponent of the prospective 1,179-mile pipeline from Alberta, Canada, to Cushing, Okla., has hired retired Navy SEAL chief David “Dave” Cooper to assess how vulnerable the Keystone XL might be to deliberate sabotage. In a 14-page report made public today (but redacted to keep it from being a playbook for aspiring terrorists), Cooper concludes that a small group of evildoers could easily cause a catastrophic spill of millions of gallons of diluted bitumen, or tar sands crude, from the Keystone XL.

Agribusiness

- Greenpeace uses fake P&G badges to gain access P&G building. The incursion, which left P&G’s vaunted corporate security force looking uncharacteristically flat-footed, was the latest foray in Greenpeace’s seven-year campaign against the use of improperly sourced palm oil. A highly saturated vegetable fat derived from the fruit, or sometimes the kernel, of the oil palm, it is, in and of itself, a relatively innocuous substance, a common ingredient in everything from laundry detergent and cosmetics to candy bars and ice cream. In recent years, demand has spiked because of its popularity as a replacement for hydrogenated oils and as a source of biodiesel fuel, which, paradoxically, is often promoted as an environmentally sound alternative to fossil fuels.

Insurance/Healthcare

- The Office of the National Coordinator for Health IT has unveiled a plan setting new priorities for the next 10 years as the HITECH Act electronic health records incentive program, which has been its primary focus, nears completion.

Financial Services

- Security experts have uncovered new vectors for exploiting the Heartbleed vulnerability, which can impact enterprise wireless networks, Android devices, and other connected devices. Dubbed “Cupid,” the attack happens on TLS connections over the Extensible Authentication Protocol (EAP), an authentication framework typically used in wireless networks and peer-to-peer connections.

Global Intelligence

- New estimates on the Gameover Zeus and CryptoLocker botnets suggest that they have infected as many as one million PCs, says the Department of Justice (DOJ). Unconfirmed reports suggest that some Internet users have already been contacted by their ISPs. According to the DoJ, it now has court permission from US District Judge Arthur Schwab to allow it to continue communicating with at least 350,000 infected PCs.

Legal and Regulations

- The Office of the United States Trade Representative (USTR) released its annual Special 301 Report, which documents the efforts of trading partners to protect and enforce Intellectual Property Rights (IPR), on April 30. Of the 82 trading partners reviewed in the 2014 Report, USTR placed 10 countries on the Priority Watch List and 27 countries on the Watch List for IPR breaches including internet piracy and improper market supervision. China, India, and Russia were all listed on the Priority Watch List, which focuses increased bilateral attention on problem areas and brings targeted countries closer to a monitoring regime. In particular, USTR’s report continues to cite China for pressuring foreign stakeholders to transfer IPR to domestic entities, non-enforcement of IPR, and misappropriation of trade secrets. In contrast, USTR removed Italy and the Philippines from this year’s Watch List.
Energy

- The Lac-Megantic, Quebec oil train explosion continues to generate opposition, editorials and general concern over the growth of crude-by-rail in the United States and Canada, as well as calls for safety upgrades throughout the rail system.

- Activists are blaming on fracking-related activities a 3.4-magnitude earthquake that took place near Greeley, CO.

- The Vancouver, WA City Council has voted to opposed a proposed oil export terminal. Concerns raised include contribution to climate change, increased rail traffic, and oil train safety concerns.

- Anarchists are calling for an anti-capitalist “black bloc” to crash Bill McKibben’s NYC People’s Climate March in September.

- Spanish activists protested the first major shipment of Canadian tar sands. Only about 50 protesters showed up for this protest, but promise to escalate their actions in the future.

- Article from NewsWire.ca discusses the ‘Assembly of Social Movements on Climate Change’, which for the first time ever, will include movements and groups from Quebec, Canada and First Nations, and aims to work together in implementing common strategies in the fight against climate change. The first meeting for the Assembly on Climate Change will take place in Montreal on Friday, June 6th 2014, and will continue in Ottawa on August 23rd during the Peoples’ Social Forum.

- EarthFirstJournal.org reports that Protests erupted in Spain last week at the site of the first major delivery of tar sands crude imported from Canada via the United States. According to a news report by EurActiv.com, an online news service focused on EU affairs, 600,000 barrels of Western Canada Select (WCS) crude were due to arrive at the port of Bilbao, Spain, imported by the Spanish oil company Repsol.

- Article from the National Post reports that the Canadian federal government is expanding its surveillance of public activities to include all known demonstrations across the country, a move that collects information even on the most mundane of protests by Canadians. The email requesting such information was sent out Tuesday by the Government Operations Centre in Ottawa to all federal departments.

- John Cherry, a contaminant hydrologist who recently chaired an expert federal panel on the impact of fracking in Canada, has called the shale gas industry “a mess” and warned that no Canadian jurisdiction has set up proper monitoring to protect groundwater in areas of intense oil and gas activity. The 72-year-old professor emeritus at Waterloo University, who has studied industrial contamination of groundwater for decades and developed effective monitoring tools, also issued a blunt warning: if government fails to fund adequate science on the mining technique or address legitimate public fears, then the shale gas industry could follow nuclear power and lose its social license to operate.

- BusinessWeek.com reports that hedge fund billionaire Tom Steyer, a climate change activist and staunch opponent of the prospective 1,179-mile pipeline from Alberta, Canada, to Cushing, Okla., has hired retired Navy SEAL chief David “Dave” Cooper to assess how vulnerable the Keystone XL might be to deliberate sabotage. In a 14-page report made public today (but redacted to keep it from being a playbook for aspiring terrorists), Cooper concludes that a small group of evildoers could easily cause a catastrophic spill of millions of gallons of diluted bitumen, or tar sands crude, from the Keystone XL.
MSBusiness.com has made a blog posted reporting that the state's Public Service Commission has become the first state agency to go on record to oppose storage of the nation's nuclear waste in Mississippi, according to Northern District Commissioner Brandon Presley. With a unanimous vote, the Commission passed a resolution calling on the federal government to cease consideration of any area in the state as a potential site for a national repository. The resolution cites Mississippi's longstanding, official policy objecting to waste storage in the state and demands re-consideration of the originally developed site at Yucca Mountain, Nev.

The Vancouver Observer has posted this article reporting that a group of 300 scientists have submitted an open letter to Prime Minister Harper urging him to reject a recent federal review recommending the passage of the oil sands pipeline. They state that the scientific basis of a recent Joint Review Panel report, which recommended in December that Enbridge's $7 billion pipeline be approved, was "deeply flawed" and "biased."

Nine activists have been detained in a protest staged by Greenpeace Mediterranean against the Nuclear Plants Summit in Istanbul on May 30. The activists had hung a 28 square-meter poster carrying the words “Nuclear disaster starts here” on the outside wall of the hotel in Şişli where the summit was held, and greeted attendees with the same poster at the building’s entrance. Greenpeace also hacked the hotel’s wireless Internet connection, so that when guests at the conference tried to connect to the Internet, they saw a message posted by the activist group. Volunteers who attempted to distribute cookies carrying messages against nuclear energy were prevented by security officials. The manager of Greenpeace Mediterranean campaigns in Turkey, Hilal Atıcı, said the conference aimed to catch the attention of companies involved in the building of the nuclear plant, adding that 64 percent of the Turkish people were against the project.

Agribusiness

- RT reports that Russian lawmakers are requesting that the United Nations create an agency to "strictly control the turnover of GMO products", and to "scrutinize how consuming GMO foods would affect human health in the long run".

- In a June 2, 2014 article, Sustainable Pulse reports that representatives of the No Patents on Seeds! coalition have filed an opposition against a European patent, held by Monsanto, on conventionally bred tomatoes (EP1812575). The patent reportedly suggests that Monsanto engineered a strain of tomato, which activists claim has a natural resistance to a fungal disease - essentially accusing Monsanto of patenting a naturally occurring strain of tomatoes. Several major activist groups from across Europe have reportedly signed onto the opposition, and the coalition claims support from "several hundred other organisations". Please see supplemental URLs for the text of the opposition to the patent.

- A petition hosted on SumofUs.org accuses Monsanto of single-handedly planning to sue Vermont over the state's recently passed GMO labeling bill. The petition asks that Monsanto not do so. As of the writing of this report, it had collected 130,735 signatures, increasing at the rate of approximately 2,000 signatures per hour. The Food Fight Fund VT has also been established to help raise money for the impending legal battle between Vermont and the GMA.

- Greenpeace uses fake P&G badges to gain access P&G building. The incursion, which left P&G’s vaunted corporate security force looking uncharacteristically flat-footed, was the latest foray in Greenpeace’s seven-year campaign against the use of improperly sourced palm oil. A highly saturated vegetable fat derived from the fruit, or sometimes the kernel, of the oil palm, it is, in and of itself, a relatively innocuous substance, a common ingredient in everything from laundry detergent and cosmetics to candy bars
and ice cream. In recent years, demand has spiked because of its popularity as a replacement for hydrogenated oils and as a source of biodiesel fuel, which, paradoxically, is often promoted as an environmentally sound alternative to fossil fuels.

**Insurance**

- The Office of the National Coordinator for Health IT has unveiled a plan setting new priorities for the next 10 years as the HITECH Act electronic health records incentive program, which has been its primary focus, nears completion.

- Cyber security threats in the healthcare industry are continually on the rise, and the value of an identity data set is about $50 per patient record. So what can healthcare providers do to avoid these attacks?

- An undisclosed number of Hurley Medical Center employees' and retirees' names and Social Security numbers were mistakenly released when an email was sent on May 13, 2014, to explain an error that had been made in calculating some co-payments for the center's health care plan.

- Recent news that a Montana Department of Public Health and Human Services server had been hacked into served as a reminder that there are a number of different ways in which HIPAA covered entities can endure data breaches.

- Post-mastectomy products retailer Ladies First Choice recently began notifying 2,365 customers that their personal information was stolen by a former employee and provided to a competing company.

- Just less than a year after a Montana Department of Public Health and Human Services server was hacked into, the department is alerting both public program clients and employees that their data was inappropriately accessed.

- Josh Valdez has filed a whistleblower lawsuit in federal court alleging that, shortly after he took an executive level job in April 2010 expecting to improve medical services at two Puerto Rican Medicare Advantage health plans owned by a subsidiary of New Jersey company Aveta Inc., he discovered that the plans -- MMM Healthcare and PMC Medicare Choice -- had been cheating Medicare out of hundreds of millions of dollars for years.

- A major privacy breach at a Scarborough hospital is being investigated by Ontario’s privacy commissioner after the personal information of thousands of new mothers was leaked by hospital employees who were being paid by outside companies.

- The Union Labor Life Insurance Company, an affiliate of Ullico, recently announced that the personal information of 46,771 people may have been exposed when a laptop was stolen from the company’s offices in Silver Springs, Md.

- Local police are investigating a breach involving inappropriate access to about 600 patients’ records by a former employee at ProMedica Bay Park Hospital in Oregon, Ohio.

- Another healthcare data breach involving employees continues to grow, as the range of employees affected by the University of Pittsburgh Medical Center (UPMC) breach has grown from a reported 27,000 to potentially all 62,000 employees.
Activism

- Activists launched a petition demanding New York State representatives put an end to corporate tax “giveaways,” listing several leading U.S. banks as “corporate tax dodgers.”

- Activists held a rally in support of “$15/hr minimum wage” in Seattle, Washington on June 2nd.

- A local resident in Orange, NJ staged a break-in at her foreclosed home as a form of protest against a leading U.S. bank.

- Activists launched a petition calling on Illinois Representatives not to vote on the House Bill 5395 that would privatize evictions in the state.

- Housing activists in Minnesota began recruiting underwater homeowners for summer campaigns possibly targeting Wall Street.

- Activists opposing Israeli occupation of Palestine held protests against a leading U.S. financial services firm on July 9, demanding the firm stop selling “occupation-supporting products.”

- Housing activists will hold a town hall meeting in Decatur, GA on June 10th to address the predatory housing crisis in Atlanta.

- Housing activists in Springfield, Massachusetts gathered at Western Massachusetts Housing Court on June 9th to demand that a government-sponsored mortgage association turn a local resident’s property over to the community to be maintained as an affordable home as part of its contribution to the National Housing Trust Fund.

- A national activist organization launched a campaign to organize a mass-based political movement using boycotts and protests targeting Wall Street banks “that perpetrated massive fraud in mortgage modifications and illegal foreclosures.”

- Housing activists in Detroit, MI called on supporters to stand with a local resident and demanded that her mortgage company reinstate her mortgage and/or negotiate a settlement of her house.

- Housing activists in Minnesota are urging its supporters to call the CEO of a leading U.S. bank in support of a local family in Minneapolis, MN with demands to sell the house back to the family.

Information Security RisK

- A prominent hacktivist collective is calling on individuals to move-their-money out of national banks on July 31st. It’s possible that the hacktivist collective may launch cyber-attacks against financial firms on July 31st in correspondence with the move-your-money campaign.

- A hacker group recently breached the systems of a leading bank in India and leaked customer information.

- A new study revealed that malware creation is on the rise, with 160,000 new samples being spotted every single day, while Trojans are now responsible for four out of five (79.9 percent) infections around the world.

- Researchers warned that the Windows PowerShell scripting tool is being increasingly used by malicious actors not only for data theft, but also for ransomware attacks.
Experts believe cybercriminals are increasingly relying on PowerShell because this is not a common technique and IT administrators who are usually on the lookout for malicious binaries might overlook threats that abuse the scripting tool.

- A hacker claiming to be affiliated with infamous online collective Anonymous said the group is planning to launch DDoS (Distributed Denial of Service) attacks against various high profile sponsors of the forthcoming FIFA World Cup this month.

- Hackers stole nearly $2 million from the online bank accounts of Japanese businesses in April, a surge in theft that has prompted some Japanese banks to curtail online services and rethink compensation policies. Earlier this month, a senior official with Japan’s Financial Services Agency told regional bank executives that regulators were concerned that online theft could cause a chain of small business failures and bankruptcies.

- Security experts have uncovered new vectors for exploiting the Heartbleed vulnerability, which can impact enterprise wireless networks, Android devices, and other connected devices. Dubbed “Cupid,” the attack happens on TLS connections over the Extensible Authentication Protocol (EAP), an authentication framework typically used in wireless networks and peer-to-peer connections.

- The Federal Bureau of Investigation, Interpol and government agencies from several European countries took control of two computer networks allegedly used by hackers to steal banking information. The international operation targeted two systems: GameOver Zeus, which hackers from overseas use to steal data from U.S. banks; and CryptoLocker, which typically used to infect a computer and encrypt data so they become inaccessible.

- Researchers say the Molerats cyber-criminal gang has returned and is targeting various European governments and a US financial institution with Remote Access Trojans (RATs). The cyber espionage campaign was initiated by spear phishing emails containing an attachment laden with malware.

- The United States Computer Emergency Readiness Team issued an alert regarding GameOver Zeus (GOZ), a peer-to-peer (P2P) variant of the Zeus family of bank credential-stealing malware, which uses a decentralized network infrastructure of compromised personal computers and web servers to execute command-and-control. GOZ is often propagated through spam and phishing messages and primarily used by cybercriminals to harvest banking information, such as login credentials from a victim’s computer. Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks.

- Researchers say a recently discovered bug in the GnuTLS cryptographic code library leaves Linux vulnerable. Maliciously configured servers can exploit the bug by sending malformed data to devices as they establish encrypted HTTPS connections. Devices that rely on an unpatched version of GnuTLS can then be remotely hijacked by malicious code of the attacker’s choosing.

- Researchers have identified a new strain of PoS malware called Soraya that can scrape memory and has the ability to intercept information sent from Web forms, a specialty of the Zeus malware family.

- Researchers have identified the first file-encrypting strain of ransomware that infects Android smartphones. The malware, dubbed Android/Simplocker by ESET, scans the SD card in a handset for certain types of files, encrypts them, and demands a ransom to decrypt the data. The ransom message is written in Russian, with payment demanded in Ukrainian hryvnias. Victims are falsely accused of "viewing and distributing child pornography, zoophilia and other perversions", and that the device is locked-down as a result.

**Legal, Litigation, Regulatory Risk**
The city of Los Angeles is suing multiple leading U.S. investment banks for mortgage discrimination that the city says led to a wave of foreclosures that blighted neighborhoods, reduced property taxes and increased the need for costly city services.

The U.S. Attorney’s office in Manhattan is investigating at least five banks over whether they overcharged the government for expenses incurred during foreclosures on federally backed home loans.

The Massachusetts Attorney General sued two major government-sponsored mortgage companies for refusing to engage in “foreclosure buyback programs” and violating the state’s 2012 foreclosure prevention law.

The SEC is developing new rules targeting high-speed traders, less transparent trading venues and order-routing practices, a move designed to promote fairness for investors, shine more light on the markets and bolster stability. The SEC said it has numerous regulatory proposals in the works, including an "anti-disruptive trading" rule to rein in aggressive short-term trading by high-frequency traders during vulnerable market conditions, and a plan to force more proprietary trading shops to register with regulators and open their books for inspection.

Operational Risk

- A U.S. private corporation that acts as a self-regulatory organization began providing data indicating the activity levels in each alternative trading system (ATS), including all market facilities commonly called “dark pools.” The information is intended to shed light on the securities that are traded in each dark pool. Under the organization's new transparency initiative, the public will now be able to see the total shares traded each week by security in each ATS or dark pool. This data will be provided to the non-professional investing public free of charge and is available through FINRA's website.

Reputational Risk

- An article co-published by a consumer group and a non-profit advocacy think tank in Washington, D.C. last week claimed that many leading U.S. financial companies are using offshore tax heavens to hide billions of dollars in taxable revenues. The article advocated that to end tax haven abuse, Congress should end incentives for companies to shift profits offshore, close the most egregious offshore loopholes, strengthen tax enforcement, and increase transparency.

- An environmental activist group continued to criticize banks for profiting from mountaintop removal coal mining.

Global Intelligence

China

- Reuters reported that supervisors and managers are playing an increasingly larger role in Chinese labor activism rather than frontline workers. This was mainly based on observations of the large-scale Yue Yuen shoe factory strike in Dongguan, Guangdong, where supervisors were the first to challenge senior plant leaders about social insurance contributions that became the focus of the dispute.

- Reuters reported on the negative response from Chinese state media against U.S tech companies such as Google, Apple, and Cisco; companies that People’s Daily says threatens the cyber-security of China and its Internet users.

- A Chinese news outlet reports a foreign trade company in Changsu City, China
experience a hacker attack and demanding ransom to be paid in Bitcoin instead of money.

- A Chinese news outlet reports online transaction and payment system has become the target of hackers in China over the recent years.

- A Chinese security news outlet reports TCL official website has been hacked and the hacker offered to sell TCL official website for 800RMB (Renmenbi). TCL Corporation is a Chinese multinational electronics company.

**Germany**

- The Federal Central Tax Office (Bundeszentralamt für Steuern, BZSt) is warning against a wave of phishing emails which claim to come from Germany’s central tax authority. The emails announce a tax refund for the targeted victims. The BZSt points out that it would never contact taxpayers about tax refunds (as this is a matter of local tax offices) or ask about bank account or credit card information via email.

**North America**

- CWA reported that CWA members joined by student activists from United Students Against Sweatshops and AFL-CIO union supporters leafleted outside the T-Mobile US annual meeting in Bellevue, Washington. The goal is to show shareholders and the public that T-Mobile is another documented labor law violator.

- The Chicago Tribune reported that McDonald has opened an office in San Francisco to attract Silicon Valley talent better and help it better connect with customers online.

- The Washington Post reported that around 20 demonstrators from a local union took up post outside the Moscone Center ahead of Apple CEO Tim Cook's speech at the Moscone Center. The demonstrator chanted and passed out flyers claiming that Apple is hurting its local community by not paying its fair share of state taxes. Sam Kehinde, who organized the protest as part of a larger campaign targeted at major tech companies. Kehinde, a former security worker, has campaigned against Apple and Google in the past over the companies' decisions to work with a firm that he says doesn't pay security officers fairly. According to the article, Kehinde is planning a similar protest at Google's developers conference later this month.

- Toner News reported that HP announced that it plans to lay off up to 50,000 employees as it strives to "re-engineer the workforce to be more competitive and meet its objectives."

- QSR Web reported that the Seattle's City Council unanimously approved a minimum wage increase to $15/hour. Mayor Ed Murray is expected to sign its passage which would give Seattle the highest minimum wage in the U.S. The International Franchise Association said it plans to file a lawsuit to overturn Seattle's plan, calling it "unfair and discriminatory."

- Mother Jones reported that data obtained from the Labor Department by Mother Jones shows that top Silicon tech firms lag far behind the general population in diversity, and that while Google is average in its recruitment of women, it has even fewer African-American and Latino employees than other major tech firms.

- TimesUnion reported that Google's Motorola Mobility handset unit announced Friday that it will shutter its North Texas factory by the end of the year.

- New estimates on the Gameover Zeus and CryptoLocker botnets suggest that they have infected as many as one million PCs, says the Department of Justice (DOJ). Unconfirmed reports suggest that some Internet users have already been contacted by their ISPs. According to the DoJ, it now has court permission from US District Judge Arthur Schwab to allow it to continue communicating with at least 350,000 infected PCs.
Malaysia

- A Malaysian news outlet reports Malaysia Airlines' Workers Union called for Malaysia Airline System (MAS) CEO to resign due its poor financial performance and the pressure with the fate of Flight MH370 still unknown after 3 months.

- A Malaysian news outlet reports a health product company was fined by the Petaling Jaya Magistrate Court for violating minimum wage regulation that require full-time employees to be paid a minimum of RM900 a month in Peninsular Malaysia.

- A Malaysian human right activist named Charles Hector post a joint statement of 47 civil society organizations, trade unions and concerned groups on his blog demanding several workers and trade union rights should be prioritized for the well being of the worker and their family.

Vietnam

- ChaoBuoiSang.Net, a local media source, reported that over 8,000 tons of domestic waste are generated every day in Ho Chi Minh City and much of it is deposited in 50 rubbish dumps before it is carried away to waste treatment plants, only three of which meet sanitation standards.

- Info.VN, a local media source, reported that Vietnam will have 19 information technology parks by 2020. The country now has seven IT parks spread over an area of 700,000sq.m. They house 200 enterprises who employ 35,000 engineers and programmers.

- VNExpress reported that the VNese government may be replacing its identification cards and the identity card may be issued at the time of birth. On 6/4/2014 the VNese government presented a proposal to replace its current identification card system to the National Assembly. If approved, the proposal will go into effect on 7/1/2015.

- Tuoi Tre News, a local VNese media source, reported that the government is proposing financial support to workers who are out of work due to destruction of their workplace during the recent riots. The speculated financial support will equal to the workers’ salary, or at least the region’s minimum wage, from 5/12/2014 up until when the businesses are operational again, but no later than 7/1/2014.

Legal and Regulations

- The CFPB on May 6 proposed amendments to its Regulation P (Privacy of Consumer Financial Information) that would allow companies, including banks, that limit their consumer data-sharing and meet other requirements to post their annual privacy notices online rather than delivering them individually. Comments on the proposed amendments are due by July 14, 2014.

- The US Treasury and the Internal Revenue Service (IRS) have announced that calendar years 2014 and 2015 will be regarded as a transition period for the purposes of IRS enforcement and administration with respect to the implementation of the Foreign Account Tax Compliance Act (FATCA).

- The Office of the United States Trade Representative (USTR) released its annual Special 301 Report, which documents the efforts of trading partners to protect and enforce Intellectual Property Rights (IPR), on April 30. Of the 82 trading partners reviewed in the 2014 Report, USTR placed 10 countries on the Priority Watch List and 27 countries on the Watch List for IPR breaches including internet piracy and improper market supervision. China, India, and Russia were all listed on the Priority Watch List,
which focuses increased bilateral attention on problem areas and brings targeted countries closer to a monitoring regime. In particular, USTR's report continues to cite China for pressuring foreign stakeholders to transfer IPR to domestic entities, non-enforcement of IPR, and misappropriation of trade secrets. In contrast, USTR removed Italy and the Philippines from this year's Watch List.

- Canada recently enacted “Anti-Spam” legislation (CASL) affecting all businesses – even those based in the United States – sending commercial electronic messages to individuals in Canada. CASL becomes effective July 1, 2014. Violations of CASL may result in monetary fines of up to $10 million (Canadian) for businesses, and $1 million for individuals. Businesses directing commercial messages toward clients in Canada should make sure they obtain consent to send such messages, maintain accurate and up-to-date lists of individuals to whom they send such messages, and devise an “unsubscribe” mechanism by which individuals may express their wish to no longer receive such commercial messages. For more information about how CASL may impact your business, please review Canada's publically-available resources regarding CASL here.

- The Canadian Government recently introduced Bill C-31, the Economic Action Plan Act 2014, No.1. This omnibus bill includes changes to a wide variety of laws in Canada. The potential amendments to Canada's Trade-marks Act will have a significant impact on brand owners, as well as intellectual property practitioners worldwide. The bill is intended to ensure that Canada meets its international trademark obligations outlined in the Singapore Treaty on the Law of Trade-marks, the Nice Agreement, and the Madrid Protocol. Now is a good time to review your Canadian trademark portfolio and work with your counsel to make sure your brands are protected.

Healthcare

On May 28, 2014 the House Energy and Commerce Subcommittee on Health approved by voice vote three bipartisan public health bills.

1. H.R. 4299, “Improving Regulatory Transparency for New Medical Therapies Act,” which is intended to improve the Drug Enforcement Agency scheduling process for new FDA-approved drugs under the Controlled Substances Act and the registration process for the use of controlled substances in clinical trials to allow treatments to get to patients in a more timely and predictable manner.

2. H.R. 4709, “Ensuring Patient Access and Effective Drug Enforcement Act,” which would amend the Controlled Substances Act to clarify definitions, allow parties to submit a corrective action plan prior to revocation or suspension of a registration, and require a report identifying how collaboration between agencies and stakeholders can benefit patient access to medications and prevent diversion and abuse of controlled substances.


- Expressing a commitment to helping develop new drugs, the Center for Drug Evaluation and Research ("CDER") continues to tweak its regulatory processes, including recently finalized guidance on its expedited review programs. In a recent blog post, CDER Director Janet Woodcock discussed other achievements and expressed support for "Special Medical Use or Limited Population" policies that would allow new drug sponsors to seek initial approval for use in a specific subgroup of patients.
As part of an international initiative to shore up the integrity of the global drug supply chain, FDA and the U.S. Customs and Border Protection ("CBP") collaborated to crack down on websites and distributors marketing unapproved prescription drugs to American consumers. In May, the two agencies conducted extensive inspections of mail facilities in New York, Los Angeles, and Chicago, where many prescription drug packages enter the country. More than 580 packages were seized or detained, and FDA also informed internet service providers and registries of 1,975 websites that they are selling products in violation of federal law. This program corresponded with an annual Interpol initiative known as Operation Pangea VII, through which 111 countries collaborate to identify the manufacturers and distributors of illegal drug products and medical devices sold over the internet.