EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

March 15, 2019 - Volume 11, Issue 6

Will There Be a Government Standard for IoT Security?

NIST offers its view on Internet of Things security guidelines, but lawmakers are pressing for mandates that would regulate cybersecurity for IoT devices

Federal agencies have been steadily adopting and deploying sensors as part of the Internet of Things, but the security of IoT devices has been a constant concern for government IT leaders, especially at the Pentagon. Now, there's more momentum than ever to make sure federal IoT environments are secured.

Last month, the National Institute of Standards and Technology released a draft interagency report on IoT cybersecurity standards, and concludes that without a standardized set of cybersecurity requirements, malicious actors could exploit security gaps and IoT systems could be vulnerable to cyberattacks.

NIST emphasizes the need for voluntary security standards, especially because the IoT industry is dynamic and in flux. However, there are legislative efforts underway designed to regulate certain standards of IT security for IoT systems in the government.

The report comes as several international initiatives to set IoT standards heat up. As FCW reports: "Security certification efforts underway in China and Europe, as well as a significant uptick this year in the use of botnet amplification attacks, has put U.S. agencies and industry in a race to set international baseline security standards for connected devices."

*(*Continued On The Following Page)*

NEWSLETTER NOTES

NIST Offers Guidance on IoT Security

The draft NIST report, which the agency is taking public comments on through April 18, notes that "while there is no universal definition of IoT, common elements exist among the many high-level definitions and descriptions for IoT." To NIST, IoT has two foundational elements: components connected by a network providing the potential for many-to-many relationships and some components with sensors and actuators that allow them to interact with the physical world.

"The growth of network-connected devices, systems, and services comprising the Internet of Things creates immense opportunities and benefits for our society," the report states. "However, to reap the great benefits of IoT and to minimize the potentially significant risks, these networked connected devices need to be secure and resilient. This depends in large part upon the timely availability and widespread adoption of clear and effective international cybersecurity standards."

The report describes five IoT technology application areas (and acknowledges the list is not exhaustive): connected vehicles, consumer IoT, health IoT, smart buildings and smart manufacturing. The report also describes 11 core cybersecurity areas and provides examples of relevant standards. The report notes that "cybersecurity for IoT is unique and will require tailoring of existing standards, as well as creation of new standards to address pop-up network connections, shared system components, the ability to change physical aspects of the environment, and related connections to safety."

Without standards, IoT systems could have gaps in many areas, including cryptographic techniques, cyber incident management, network security, information security management systems, software assurance and more. NIST recommends that agencies participate in the development of IoT security standards in standards-developing organizations and, based on each agency's mission, cite appropriate standards in agency procurements.

Additionally, NIST recommends that agencies "support the development of appropriate conformity assessment schemes to the requirements in such standards," citing the adoption of the Wi-Fi logo for products and devices that have been tested and certified by the Wi-Fi Alliance, a nonprofit member organization whose goal is to ensure that any device carrying the logo connects seamlessly to any Wi-Fi network. However, NIST says that adoption of standards must be undertaken carefully to be successful. "The decision on the type, independence and technical rigor of conformity assessment should be risk-based," the report says. "The need for confidence in conformity must be balanced with the cost to the public and private sectors, including their international operations and legal obligations. Successful conformity assessment provides the needed level of confidence, is efficient, and has a sustainable and scalable business model."

*(*Continued On The Following Column)*

Lawmakers Consider IoT Security Standards

Michael Hogan, the NIST official charged with editing the draft report, said at a public meeting of the Information Security and Privacy Advisory Board on March 16, that he was unsure of the need for mandatory IoT security certifications, according to FCW. He noted that Congress could pass legislation, but that NIST would be "neutral" on the issue, because it would be expensive and IoT is still evolving. "Maybe it needs to be done, but it's not trivial," Hogan said.

In August, a group of U.S. senators introduced a bill that would require vendors who supply the government with IoT devices "to ensure that their devices are patchable, do not include hard-coded passwords that can't be changed, and are free of known security vulnerabilities, among other basic requirements," according to a statement.

The legislation, the Internet of Things Cybersecurity Improvement Act of 2017, directs the Office of Management and Budget to develop alternative network-level security requirements for devices with limited data processing and software functionality, the statement notes. That way, Reuters reports, agencies could ask OMB "for permission to buy some noncompliant devices if other controls, such as network segmentation, are in place." The legislation also would direct the Department of Homeland Security's National Protection and Programs Directorate to issue guidelines for each agency with respect to any connected device in use by the government and include policies and procedures for conducting research on the cybersecurity of an IoT device. Sens. Mark Warner, D-Va., and Cory Gardner, R-Colo., co-chairs of the Senate Cybersecurity Caucus, introduced the bill along with Sens. Ron Wyden, D-Ore., and Steve Daines, R-Mont. Meanwhile, Sen. Ed Markey, D-Mass., and Rep. Ted Lieu, D-Calif., have encouraged fellow lawmakers to move forward with their proposed bill, the Cyber Shield Act, which would create a voluntary cybersecurity certification program for IoT devices. "The IoT era could also be considered the 'Internet of Threats' era if appropriate cybersecurity safeguards are not in place," Markey said during a prerecorded video statement released during the Institute for Critical Infrastructure Technology's winter summit on Jan. 29, according to Federal News Radio.

The bill, if passed, would allow the Commerce Department to set up an advisory committee of cybersecurity experts from academia, industry and consumer advocacy groups to create cybersecurity standards for IoT devices

Federal News Radio reports: "Under the legislation, device manufacturers would voluntarily submit their products for evaluation. Products that meet the advisory board's cybersecurity standards would carry a cyber shield logo. The system has been compared to the Energy Star program developed by the Environmental Protection Agency more than 20 years ago."

Toward a Softer Brexit?

After British MPs rejected both Prime Minister Theresa May's deal yesterday, and a no-deal Brexit today, they appear to be whittling down the options. The Financial Times concludes that MPs finally must consider alternatives: Ahead of today's vote, the paper wrote that Parliament should slow things down, ask for an extension to the March 29 deadline, and start weighing softer Brexit plans akin to the Norway-style model of remaining in parts of EU like the tariff-free single market, but not the EU itself—and if no such deal can pass, hold a second referendum.

Brexiteers may have reason to be upset at the vote—Nigel Farage called it a "betrayal" of Brexit, in a Telegraph op-ed—but as Parliament progresses through its options, Guardian columnist Owen Jones asks that remainers start seeing more nuance and give a softer Brexit a chance: "While for a remainer like myself no Brexit is desirable, a chasm separates an economically manageable soft Brexit and the economic shock of no-deal Brexit," he writes.

Is Xi's Model Working?

Chinese President Xi Jinping has executed his vision of an expansive Chinese state, but the downsides of that model are becoming apparent, Elizabeth Economy writes at Foreign Affairs. Directives to local governments have been met with resistance, party interference has hurt private firms, and Belt and Road projects have raised concerns abroad over business practices.

All of that has weakened China's economy and spooked the international community, Economy writes. (One piece of supporting evidence, on the latter point: Europe is eyeing Chinese investments more skeptically, Le Monde reports.)

The answer, Economy writes, is for Xi to dial things back, offering a "level playing field" to foreign multinationals and easing up on repressive policies toward Chinese citizens. Economic growth at home and influence abroad may hang in the balance.

World Powers Are on a Collision Course

The age of great-power peace is over, Hal Brands and Charles Edel write in their new book, The Lessons of Tragedy: Statecraft and World Order, an excerpt of which The National Interest has published. Major world powers have gotten along since the Cold War, but now China, Russia, and Iran are not only growing more aggressive in their own respective neighborhoods, they're cooperating against the US, as Russia and China have on issues from energy to arms sales, and as Russia and Iran have in Syria.

Their aims aren't just regional. Though these three countries are working to upset the regional alliances America has put into place, what they want is to upend the American-led world order, more broadly.

That point has been made before, but Brands and Edel warn today's problems could escalate. The behavior of China, Russia, and Iran is a "warning light flashing on the dashboard" that presages "still-greater traumas to come," they write.

ARMY CHOOSES MA CO. FOR SMALL GROUND ROBOT

WASHINGTON — The Army has chosen Waltham, Massachusetts-based QinetiQ North America to produce its new small ground robot following a head-to-head competition with the company's Boston-based neighbor Endeavor Robotics.

The serviced awarded a production contract for up to $152 million to QinetiQ on March 11 for its Common Robotic System - Individual or CRS-I program, which is its first small-sized — under 25 lbs — ground robot program of record, according to an Army statement from Fort Benning, Georgia.

Ultimately follow-on contracts and options could amount to roughly $400 million for roughly 3,000 robots.

Fort Benning is the home of the Maneuver Capabilities Development and Integration Directorate's Robotic Requirements Division and is where the capability requirements for CRS-I was born.

*(*Continued On The Following Page)*

The Army based its decision the robot's performance during an Engineering and Manufacturing Development run-off test at Aberdeen Test Center in October 2018.

The service wanted a ground robot that could be remotely operated, highly mobile and lightweight enough for a dismounted soldier to carry in a backpack, the statement notes. The robot will be controlled using a universal controller capable of controlling any unmanned air or ground platforms in the future.

The robot will come with a variety of payloads and an open architecture to add future capabilities as needed. Get the defense industry's most comprehensive news and information straight to your inbox. The plan is to field the first of the CRS-I systems in fiscal year 2020. The Army had whittled down the competition to QinetiQ and Endeavor in April 2018.

It is not known what exactly Endeavor brought to the competition as it kept its system under wraps at Association of the US Army's annual conference in October 2018 — literally shrouding it in a case at its booth on the showroom floor.

The CRS-I award is a major step toward the Army's push transform a hodgepodge petting zoo of 7,000 unmanned ground vehicles acquired during the wars in Iraq and Afghanistan to a streamlined collection of systems.

The Army plans to procure UGVs with just a few common chassis among them in small, medium and large ranges as well as a universal controller.

British Vote to Delay BREXIT

March 14 at 6:06 PM

LONDON — British lawmakers voted Thursday to seek to delay Brexit — maybe for weeks, maybe for months — after Prime Minister Theresa May's plans for leaving the European Union have been repeatedly rejected by a raucous Parliament trying to wrest control from her.

Since becoming prime minister, May had insisted that "Brexit means Brexit," that she would negotiate a good deal and that Britain would leave the European Union on March 29, 2019. The March date was a deadline the prime minister herself triggered when she — alongside the British Parliament — initiated Article 50 in the E.U. treaty two years ago.

Now Britain almost certainly will not leave the European Union in two weeks — unless E.U. leaders reject its request for an extension and it crashes out with no deal. The vote to delay Brexit passed 412 to 202.

For Russian Farmers, Sanctions Are a Gift

Russian President Vladimir Putin faces a lagging economy and, with it, the risk of popular discontent. But thanks to Western sanctions over his invasion of Ukraine—and, more specifically, Russian countersanctions that targeted Western food imports—Russia's domestic agriculture is booming, Judy Twigg writes at The National Interest.

The countersanctions have "put Russian farmers in the best shape they've ever been," she writes, reviving a sector that had collapsed in the 1990s, boosting Russia to become the world's top wheat exporter, and restoring some national pride in Russian agriculture.

A Post-Syria Rebirth for al-Qaeda?

While the world has focused on defeating ISIS, al-Qaeda may emerge from Syria's war with new momentum, writes Colin P. Clarke of the Foreign Policy Research Institute. Syria's war has been a "learning laboratory" for al-Qaeda to absorb lessons and refine tactics; it's also "expanded al-Qaeda's contacts, and, given the proliferation of jihadist groups worldwide – 67 active groups as of 2019 – there will be more opportunities for al-Qaeda to work with like-minded terrorists from North Africa to Southeast Asia," Clarke writes.

It may be time for the West to recalibrate its approach to terrorism, as ISIS loses its territory and global jihad reaches a potential turning point. That's what David Gardner argues in the Financial Times: In 2014, ISIS was able to seize wide swaths of Syria and Iraq with fewer supporters than it has now, he writes, and we should anticipate what policies are helping and hurting before jihad sees another revival.

Trump says U.S. will ground Boeing jet involved in fatal crashes, following the lead of other nations

The move follows action this week by Canada, the European Union and other governments to ground the U.S.-made Boeing 737 Max 8 aircraft, which was involved in a crash Sunday that killed 157 people in Ethiopia.

The United States on Wednesday joined Canada, Europe, and nearly fifty other countries in banning the Boeing 737 Max aircraft from its airspace following Sunday's Ethiopian Airlines crash that killed 157 people.

President Donald Trump announced on Wednesday that he is issuing an order to ground all 737 Max aircraft effective immediately.

"We're going to be ordering an emergency order to ground all 737 Max 8 and the 737 Max 9 and planes associated with that line," the President said. "Any plane currently in the air will go to its destination and thereafter be grounded until further notice."

President Donald J. Trump to Award the Medal of Honor

Issued on: March 12, 2019

On Wednesday, March 27, 2019, President Donald J. Trump will award the Medal of Honor to Staff Sergeant Travis W. Atkins, United States Army, for conspicuous gallantry. To commemorate the selfless service and sacrifice of Staff Sergeant Atkins, his son Trevor Oliver and family will join the President at the White House.

Staff Sergeant Travis W. Atkins will receive the Medal of Honor posthumously for his actions of June 1, 2007, in support of IRAQI FREEDOM. While serving in Iraq with Company D, 2d Battalion, 14th Infantry Regiment, 2d Brigade Combat Team, 10th Mountain Division, Staff Sergeant Atkins engaged in hand-to hand combat with a suspected insurgent.

As he attempted to subdue the man, Staff Sergeant Atkins realized the insurgent was attempting to detonate a bomb strapped to his body. When he noticed the insurgent was about to trigger the suicide vest, Staff Sergeant Atkins tackled him, selflessly using his own body to shield his fellow soldiers from the imminent explosion. Staff Sergeant Atkins' heroic actions, at the cost of his life, saved the lives of three of his teammates.

*(*Continued On The Following Page)*

PERSONAL BACKGROUND:

On November 9, 2000, Atkins enlisted in the United States Army. He attended basic training at Fort Benning, Georgia, and was assigned to Company A, 3d Battalion, 327th Infantry Regiment, 1st Brigade, 101st Airborne Division (Air Assault) at Fort Campbell, Kentucky. He deployed to Iraq in 2003 and was later honorably discharged as a Sergeant. After attending the University of Montana, he re-enlisted in the Army in 2005 and deployed again to Iraq in August 2006. He was promoted to Staff Sergeant on May 1, 2007. Staff Sergeant Atkins is survived by his son, Trevor Oliver, of Coon Rapids, Minnesota, and his parents, John and Elaine Atkins of Bozeman, Montana.

Additional Information

THE MEDAL OF HONOR:

The Medal of Honor is awarded to members of the Armed Forces who distinguish themselves conspicuously by gallantry and intrepidity at the risk of their own lives above and beyond the call of duty while:

- engaged in an action against an enemy of the United States;
- engaged in military operations involving conflict with an opposing foreign force; or
- serving with friendly foreign forces engaged in an armed conflict against an opposing armed force in which the United States is not a belligerent party.

The meritorious conduct must involve great personal bravery or self-sacrifice so conspicuous as to clearly distinguish the individual above his or her comrades and must have involved risk of life. There must be incontestable proof of the performance of the meritorious conduct, and each recommendation for the award must be considered on the standard of extraordinary merit.

Congress Unveils Bipartisan Bill for IoT Cybersecurity Standards

March 14, 2019 - A group of bipartisan Senators and House members recently introduced legislation that would establish security requirements around IoT devices purchased by government agencies, such as the Department of Health and Human Services.

Introduced by Sens. Mark Warner (D-VA), Cory Gardner (R-CO), Maggie Hassan (D-NH), and Steve Daines (R-MT), alongside Reps. Robin Kelly (D-IL) and Will Hurd (R-TX), the Internet of Things Improvement Act would "use the purchasing power of the federal government to establish some minimum security standards for IoT devices."

The proposed bill would require NIST to issue recommendations that would address the minimum needs for the secure development, identity management, patching, and configuration of IoT devices. NIST would also be tasked with working alongside cybersecurity researchers and other industry experts to publish guidance around coordinated disclosures to ensure device vulnerabilities are addresses.

It would also direct the Office of Management and Budget to issue guidelines for each agency consistent with NIST's recommendations. OMB would be required to review those policies a minimum of every five years.

The bill would also require all devices purchased by the government to comply with those standards, while establishing the requirement for contractors and vendors providing IoT devices to the government to adopt coordinated vulnerability disclosure policies to ensure that data is disseminated when a flaw is found.

Indeed, a May 2018 Departments of Commerce and Homeland Security report stressed that the federal government should lead by example when it comes to IoT device security, by requiring agencies to only purchase secure and resilient devices.

Many IoT devices are currently being sold without appropriate safeguards or protections in place, "with the device market prioritizing convenience and price over security," Warner explained.

"The IoT landscape continues to expand, with most experts expecting tens of billions of devices to be operating on our networks within the next several years," Gardner said in a statement.

*(*Continued On The Following Page)*

"As these devices continue to transform our society and add countless new entry points into our networks, we need to make sure they are secure, particularly when they are integrated into the federal government's networks."

NIST will continue to be a key player in developing those standards and establishing guidelines that will improve IoT device security, explained Gardner. The legislation intends to build on those efforts.
The concern is that an estimated 30 million internet-connected devices in use by 2020, and Kelly said it's imperative to not "allow them to become a backdoor to hackers or tools for cyberattacks."

Further, these devices are often shipped with factory-set, hardcoded passwords, and often are unable or difficult to be patched or updated. The Congressional members said that as a result, these devices are used to launch DDoS attacks against websites, web-hosting servers, and internet infrastructure providers.

A recent Check Point study confirmed just that: IoT devices pose a serious risk to IT networks, especially in the healthcare sector. The researchers found the cause is the open source nature of IoT devices and the increase of their data collection, which makes them a prime target for hackers.

NIST also released its own report warning about the cybersecurity vulnerabilities found in IoT devices in October, stressing that IoT devices affect cybersecurity and privacy risks differently than traditional IT devices.

For Hurd, the proposed legislation will ensure "IoT devices [are] built with security in mind, not as an afterthought."

"By requiring the federal government to only purchase devices that meet certain cybersecurity standards, this bill will help protect federal agencies against hackers who are seeking to exploit internet of things devices in order to steal critical national security information and the private data of… Americans," Hassan said in a statement. The bill has support from a wide range of security leaders, including vendors Rapid7 and CTIA.

Warner has made a hard push for cybersecurity efforts across all sectors in recent months. In February, he sent a letter to the American Medical Association, HIMSS, and other healthcare stakeholders to ask these leaders to work with the federal government on short- and long-terms plans to reduce cybersecurity flaws in the healthcare sector.

A few days later, he asked for similar help and recommendations from federal agencies, such as HHS, the Food and Drug Administration, NIST, and others

Venezuela launches WTO challenge to U.S. sanctions

GENEVA (Reuters) - Venezuela has launched a complaint at the World Trade Organization to challenge U.S. sanctions, saying that a ban on travel by blacklisted individuals and trade restrictions break WTO rules, a WTO filing showed on Tuesday.

In its second-ever WTO complaint, filed on Dec. 28, Venezuela also cited U.S. rules on sales of gold and discriminatory treatment of Venezuela's debt and transactions in digital currency as breaches of the international rules.

There was no immediate reaction from the United States, which has been tightening sanctions against the government of President Nicolas Maduro in recent months, targeting senior officials and Maduro's wife and allies, as well as banning sales of Venezuelan gold.

On Tuesday it imposed sanctions on a Venezuelan currency exchange network that the U.S. Treasury said siphoned billions of dollars to corrupt government insiders.

Almost 2 million Venezuelans have fled since 2015, driven out by food and medicine shortages, hyperinflation, and violent crime. Thousands have made their way to south Florida.

Maduro, who denies limiting political freedoms, has said he is the victim of an "economic war" led by the United States.

The United States has 60 days to answer Venezuela's WTO complaint, after which time Maduro's government could ask the WTO to adjudicate.

But Washington is unlikely to fear any such legal escalation, partly because the WTO allows exceptions to its rules if there are "essential security interests".

U.S. probes FAA approval of Boeing plane: WSJ
Citing national security at the WTO used to be unthinkable, but the taboo has been broken in disputes between Russia and Ukraine and between Qatar and several of its neighbors, and last year the United States also used national security to justify its steel and aluminum tariffs.

Even if Venezuela presses its case at the WTO, it is unclear if the WTO dispute settlement system will be able to help, because a U.S. block on new judicial appointments means the WTO system is set to be paralyzed from December 2019, and disputes filed now are likely to end up in legal limbo.

If the paralysis takes hold, trade experts say disputes could end up being decided by diplomatic negotiation rather than by judges.

Events and Training

■ Export Control Briefing, Long Beach, CA
March 21, 2019, 8:30am to 10:30am
Speakers: Karen Nies-Vogel, Director of the Office of Exporter Services, Kimberly Orr, DVM, Ph.D., Senior Biological Licensing Officer
Register here: https://2016.export.gov/california/irvine/events/tdy2/index.asp

Registration is also open for BIS seminars across the United States. Details below.

■ *Complying with U.S. Export Controls* –
April 3-4, 2019, Denver, Colorado
Registration: $500 (members)/$550 (non-members)

■ *Complying with U.S. Export Controls*
April 17-18, 2019, Scottsdale, Arizona
Registration: $595

■ Complying with U.S. Export Controls
April 23-24, 2019, Portsmouth, New Hampshire
Registration: $550 through March 18th and $575 after

■ Complying with U.S. Export Controls
April 30-May 1, 2019, Orange County, California
Registration: $500

■ Complying with U.S. Export Controls
June 5-6, 2019, Seattle, Washington
Registration: $550

■ Complying with U.S. Export Controls
June 11-12, 2019, Detroit, Michigan
Registration: $580

■ How to Build an Export Compliance Program
June 13, 2019, Detroit, Michigan
Registration: $290

■ 2019 Annual Conference on Export Policy – Registration coming soon
July 9-11, 2019, Washington, D.C.

(*Continued On The Following Column)

"Complying with U.S. Export Controls" is a two-day program led by BIS's professional counseling staff and provides an in-depth examination of the Export Administration Regulations (EAR). The program will cover the information exporters need to know to comply with U.S. export control requirements under these regulations. We will focus on what items and activities are subject to the EAR; steps to take to determine the export licensing requirements for your item, how to determine your export control classification number (ECCN), when you can export or reexport without applying for a license, export clearance procedures and record keeping requirements, and real life examples in applying this information. Presenters will conduct a number of "hands-on" exercises that will prepare you to apply the regulations to your own company's export activities.

"How to Build an Export Compliance Program" is a one-day program that provides an overview of the steps a company may take to implement an internal Export Compliance Program. Agenda topics include guidance on how to establish an Export Compliance Program, strategies to enhance your company's compliance program, how to avoid common compliance errors, and how to build a solid framework for your company's compliance program. This program includes small group discussion, hands-on exercises, compliance peer networking, and provides a written example of an export compliance program as well as the Office of Exporter Services January, 2018 revised Export Compliance Guidelines to assist in developing your compliance program. Recommended prerequisite: Essentials of U.S. Export Controls or Complying with U.S. Export Controls or equivalent experience.

For general information about the BIS Seminar Program contact the Outreach and Educational Services Division at OESDSeminar@bis.doc.gov or (202) 482-6031 or the BIS Western Regional Office at (949) 660-0144 or (408) 998-8806.

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

"Stay positive, work hard, make it happen."