THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

THOMSON REUTERS®

Vol. 65, No. 4 February 1, 2023

Focus

¶ 19

FEATURE COMMENT: ‘Wile E.’ IoT: NIST SP 800-213 And Catching Up With The Internet Of Things Cybersecurity Improvement Act Of 2020

“*Beep beep*”—Road Runner

Be it running into a rock face, dropping off a cliff, getting blown up, or taking an anvil to the noggin, there was little that would/could stop Wile E. Coyote (*Road-Runnerus digestus*) from his pursuit of the fast moving Road Runner (*Velocitus tremenjus*), at least not in the 6–7 minute glimpses Saturday morning viewers were allotted. In each short, that quick thinking Road Runner (*Speedipus rex*) seemed just out of reach of Wile (*Hard-Headipus ravenus*). Despite the application of some pretty impressive technological and creative engineering (see, e.g., backpack refrigerator ski machine, rocket sled, etc.) and access to Acme’s nifty gadgets and gizmos (see, e.g., dehydrated boulders, explosive tennis balls, jet-propelled unicycle, etc.), his target was simply too fast or too agile for him to catch. That’s what happens when you let your quarry get too far ahead of you—it can be nigh impossible to catch up … without exploding.

Nowhere in commerce is this *Looney Tunes* philosophy on better display then the tension between technologic advancement and Government regulation. While the Federal Government and its agencies are capable of spotting issues, they can’t seem to right properly get out of their own way in time to address them. The examples of regulatory-technologic lag are far too legion to list, but one might suggest looking at the Federal Acquisition Computer Network from the mid-90s, to more recently with the proposed American Data Privacy and Protection Act, or maybe even the long-gestating Cybersecurity [Maturity(?)] Model Certification, which has been assessed and analyzed for what seems like years.

To this list, however, we must now add a newcomer in the explosive rise of Internet of Things (IoT) devices. Manufacturers and providers of a host of devices in the critical infrastructure and healthcare spaces are demanded to provide increased functionality, and the allure of IoT is inescapable. The concept of allowing electronic and automated devices to perform tasks that were either manual or mechanical work, while simultaneously collecting resultant data for increased improvement, is mother’s milk. It’s not going away.

The sheer volume, ease, and ubiquity of this largely unregulated technology has been repeatedly deemed to pose a significant risk to the U.S.’ critical infrastructure Government customers, specifically in the energy, healthcare and transportation sectors. To battle that threat, the Government planted its feet into the starting blocks with the Internet of Things Cybersecurity Improvement Act of 2020 to “establish minimum security standards for [IoT] devices owned and controlled by the federal government,” according to the CIO.gov Handbook. The challenge is whether the Government, unlike Wile E. (*Overconfidentii vulgaris*), is capable of catching up with the Road Runner (*Disappearialis quickius*) that is IoT adoption and proliferation.

There is, of course, a need to understand some basics about Internet of Things devices and their risk before addressing the aforementioned IoT Cybersecurity Improvement Act or discussing the actions the Government has taken or failed to take in line with that Act. Ultimately, however, the key issues surround how these requirements and Government actions/inactions impact the manufacturers and providers of IoT technology for Government customers. So grab a bowl of cereal and settle in, because here we go.

The Internet of Things (*Connecta Abunchus*)—The "Internet of Things" is one of those rare terms that is at once both gloriously vague and undeniably specific. In summary, the common threads of the definition include the following:

- A network of physical objects
- With embedded technology
- For the purpose of
- Connecting and exchanging data
- With other objects, devices, or systems.

Put more simply, IoT devices are "smart" devices that are connected by the internet, used to monitor and collect information from their environment, and then share that information with other devices or data collectors. The scope of that technology is multifaceted and spans from individuals (such as smart watches/wearables), to common office equipment and network devices, all the way up to the operation of major cities (Barcelona, for example, has employed an extensive sensor network to assess factors such as energy usage, noise, irrigation, etc.).

That diversity of scope is why IoT isn't going away. The trades, including data provided by Transforma Insights, predict that the number of IoT-connected devices will rise from roughly 10.07 billion in 2023 to over 25.4 billion in 2030. This means an ever-increasing amount of commercial and consumer products will find their way to somehow be connected to the internet. The drive toward interconnected technology is touted as a convenience for users, many of whom do not understand (or do not wish to understand) the backend machinations that gamify their oral hygiene, deliver music with their salt, or embed into flip-flops (yes, all of those are really a thing).

Industry is responding to this demand, and forecasters at IoT Analytics are suggesting the IoT market size will have a compound annual growth rate (CAGR) of 22.0 percent, to $525 billion, over the course of the next 4–5 years. Notably, this CAGR forecast is actually lower than previously anticipated due, in large part, to a lagging microchip supply, labor shortages, and, for U.S. consumers, the pending domestic preference changes of manufactured products dictated by the Build America, Buy America Act.

For the U.S. Government, IoT devices have found a welcoming home for quite some time. Throughout the years, the Government Accountability Office has been monitoring its rise in the Federal Government. (See, e.g., *Internet of Things: Status and implications of an increasingly connected world* (GAO-17-75)). In 2020, GAO issued a report, *Internet of Things: Information on Use by Federal Agencies* (GAO-20-577), intended "to review the federal government's experience with IoT" and used the Department of Commerce, the Department of Homeland Security (DHS), Environmental Protection Agency, and NASA "as case studies" for the Government's then-adoption of IoT. The report reflected a need to assist agencies manage the cybersecurity risks associated with IoT (and industry-based operations technology (OT)), and highlighted the budding guidance and resources being provided by DHS's Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST). This included CISA guidance, programs, alerts and advisories addressing IoT and OT vulnerabilities, and NIST guidance and reports, such as NIST Interagency or Internal Reports (NISTIR) 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, to better educate agencies on the "rapidly evolving and expanding collection of diverse technologies that interact with the physical world."

Understanding IoT Risk (*Hackeri Scaricus*)—The risk posed by IoT devices is quite simple to analogize—it's the equivalent of unknowingly leaving a bay window wide open before you lock your doors in your house on your way out of town. There's a benefit in (a) having a window and (b) cracking it open, but that benefit turns to detriment when examined through the lens of security. To operate correctly, an IoT device creates a connection between it, a potentially insecure object, and a secure network. If or when that device is compromised, it can serve as a gateway—of information out of or bad actors on to—a network. Many of these devices are intentionally open-ended to facilitate the plug-n-play nature that consumers desire (think IoT connection types and low-power wide-area networks such as Bluetooth, Zigbee and Wi-Fi).

While every computer provides a possible ingress/egress point to a network, the inclusion of IoT devices, many of which are not intended to operate with encryption or similar fortifications, greatly increases a network's "attack surface" available for bad actors to exploit. Moreover, IoT devices, as identified by the Open Web Application Security Project, generally rely on lax security and networks or hardcoded (and publicly available) passwords to facilitate customer use and adoption. Add to these fundamentals a general lack of awareness as to what is happening with/around the device, a lack of timely patching/updates, and an overall inability for many of these low-power systems to employ sufficient encryption, and you have an "attack surface" that one can drive a train through—no black paint necessary.

These vulnerabilities can quickly lead to a parade of horribles for industries, contractors and agencies dealing with areas such as critical infrastructure, medical devices, and national security. Beyond a mere data breach, the nature of IoT devices is that they are generally *devices* that do/control/operate a *physical thing*. This means that if not properly protected it can result in:

- Device hijacking
- Data siphoning
- Denial of service attacks
- Device theft
- Device "spoofing."

A significant example of this was the 2016 Mirai botnet attack that, according to Elie Bursztein, leader of Google's anti-abuse research team, turned over 600,000 unsecure IoT devices into "zombie" servers that crippled websites through an immense denial of service attack. A self-replicating malware, Mirai attacked, then infected vulnerable IoT devices, then moved to find other ones it could corrupt. When fully amassed, each of these devices began sending data at particular websites that flooded servers with data estimated at a rate of one terabyte per second (Tbps). As a point of reference, if you've ever tried to download a movie before catching a plane, one Tbps is the equivalent of trying to download roughly 250 movies … per second. (It's a lot.) Moreover, as the devices that were targeted generally weren't managed or overseen by a network management tool, the individuals and businesses from which Mirai launched did not know their devices had been compromised or used as part of the attack. Making matters even more challenging, since the attacks all took place in the virtual background, devices infected by Mirai continued to operate normally or maybe a little glitchy.

Unfortunately, the potential threats posed by IoT, such as the Mirai botnet attack, largely remain. Only recently has industry begun to design IoT devices with security in mind or with the ability of users to manage/protect those devices, and the networks upon which they operate, from attack. That these devices were growing increasingly present in the Federal Government began raising concerns that were finally acted upon.

The IoT Cybersecurity Improvement Act of 2020 (*Gotadu Sumthinigus*)—In apparent recognition of the need to balance the benefits of digital transformation and "the highest level of cybersecurity at agencies in the executive branch," the Internet of Things Cybersecurity Improvement Act of 2020 (the "IoT Act" or "the Act") was signed into law on Dec. 4, 2020 (P.L. 116-207, 134 Stat. 1001 (2020)). The IoT Act sought to strengthen the Federal Government's cybersecurity posture as it pertains to the acquisition and operation of IoT devices. In the terms of the Act, IoT devices are devices with at least one sensor or component for interacting directly with the physical world, have at least one network interface, and are not conventional information technology devices, such as smartphones and laptops. Furthermore, IoT devices are defined as being capable of functioning on their own, rather than merely acting as a component to another device.

The IoT Act contains several provisions intended to strengthen the Federal Government's procurement and use of IoT devices and to secure the Government's IT infrastructure. Provided with four deadlines, the Federal Government was directed to act with purpose to "take specified steps to increase cybersecurity for Internet of Things (IoT) devices." However, like many of the plans concocted by Wile E. Coyote, this effort appears already to be heading right off a cliff.

First, the IoT Act required NIST to develop new security standards and guidelines for IoT devices for the Federal Government. In particular, NIST was required to establish, no later than 90 days after the IoT Act's enactment (i.e., March 4, 2021), standards and guidelines on the appropriate use and management of IoT devices, including minimum information security requirements for managing cybersecurity risks associated with IoT devices.

With those standards and guidelines in place, the IoT Act mandated the Office of Management and Budget to then conduct a comprehensive review of federal agency information security policies and principles. OMB was to conduct this review no later than 180 days after the NIST guidelines were published (i.e., Aug. 31, 2021), and issue policies and principles, as necessary and in consultation with the director of CISA, to ensure agency policies were consistent. Notably, any IoT principle or policy issued by OMB would not apply to national security systems.

Most importantly for contractors, the IoT Act also directed NIST to develop guidelines for the reporting, coordinating, publishing, and receiving of information about a security vulnerability (and resolution of said vulnerability) relating to information systems, and IoT devices, owned or controlled by an agency. This required NIST to establish guidelines for contractors, and subcontractors at any tier, providing to an agency an information system (including an IoT device), to receive information about a potential security vulnerability relating to the information system (or IoT device) and give them a means to disseminate information on the resolution of that identified security vulnerability. NIST was to publish these guidelines, in consultation with the secretary of homeland security, no later than 180 days (i.e., June 3, 2021) after the IoT Act's enactment. Once published, the secretary of homeland security, in consultation with the director of OMB, would administer the implementation of the guidelines, providing operational and technical assistance, as needed.

Not without some teeth, the IoT Act provides a real kicker in discussing "Prohibition on Procurement and Use." Two years after the date of enactment (i.e., Dec. 4, 2022), an agency head

> is prohibited from procuring or obtaining, renewing a contract to procure or obtain, or using an Internet of Things device, if the Chief Information Officer (CIO) of that agency determines during [a statutorily regulated IT-acquisition contract review] for such device that the use of such device prevents compliance with the standards and guidelines developed under [the to-be-developed NIST guidelines found in the IoT Act] section 4 or the guidelines published under section 5 with respect to such device.

Such prohibition applies to all contracts and subcontracts "in amounts not greater than the simplified acquisition threshold." Of course, the Act provides that an agency head may waive that prohibition, but only after the CIO of that agency determines that waiver is necessary (1) in the interest of national security, (2) for research purposes, or (3) because the IoT device is secured using "alternative and effective methods appropriate to the function of such device." The IoT Act tasked the director of OMB with establishing a standardized process for the CIO of each agency to follow in determining whether waiver may be granted.

Finally, the director of OMB was to, in consultation with the secretary of homeland security, "develop and oversee the implementation of policies and principles, standards or guides as may be necessary to address security vulnerabilities of information systems (including [IoT] devices)" no later than two years (i.e., Dec. 4, 2022) after the IoT Act's enactment. The IoT Act stated that the Federal Acquisition Regulation was to be revised "as necessary to implement any standards and guidelines promulgated in this section."

Action Taken by NIST (*Signa Rex*)—Legal deadlines notwithstanding, since the enactment of the IoT Act, NIST has carried out its mandate, issuing several publications on IoT cybersecurity. In November 2021, NIST issued Special Publications (SPs) 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, and 800-213A, *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog*. The documents, created pursuant to § 4 of the IoT Act, provide guidelines and advice to "help organizations consider how an IoT device they plan to acquire can integrate into a system" and give agencies a helpful "catalog of internet of things (IoT) device cybersecurity capabilities [ ] and non-technical supporting capabilities that can help organizations as they use Special Publication (SP) 800-213 to determine and establish device cybersecurity requirements."

More specifically, while NIST SP 800-213A serves as technical manual to assess the specifics of "device cybersecurity requirements to determine those appropriate to support the security controls implemented on their system and in their organization," the instructions found in NIST SP 800-213 help agencies assess and plan whether to use them in the first place. NIST SP 800-213 recognizes the allure of IoT devices but cautions agency acquisition and IT professionals to take care when purchasing and implementing IoT devices for their projects and/or networks. The SP reminds agencies that "the increasing scale, heterogeneity, and pace of IoT deployment motivates a focus on security requirement support below the information system level, at the system element level." Effectively, NIST is telling agencies that IoT devices are generally placed into systems *after* that system has already been deployed. Accordingly, risk management principles demand that the IoT device's security be independently assessed before being plugged into the existing system or network. The SP warns that this can be challenging, as many/most IoT devices do not have the "features and functions that are common in conventional information technology (IT) equipment." In assessing the cybersecurity considerations of whether to include an IoT device, the SP suggests agencies ask the following questions:

- What is the benefit of the IoT device and how will it be utilized?
- What data is collected (i.e., Personal data, Confidential organizational/Federal Government data, or Environmental data)?
- In what technologies will the data be stored and how will it be transmitted?
- In what geographic areas will the IoT-collected data be shared and/or stored?
- With what other third parties will data from, or about, the IoT devices be shared and/or stored?

With those questions answered and the ramifications understood, the SP suggests additional inquiry and a more exacting examination into:

- Might the device interfere with other aspects of operations or system functionality? (i.e., privacy or safety risks? system reliability or resiliency?)
- Would the IoT device introduce unacceptable risks to the organization or result in noncompliance with cybersecurity requirements?
- Does the IoT device have known security and/or privacy vulnerabilities?
- What organization-specific information is important to defining key device cybersecurity requirements?
- Does the IoT device lack key device cybersecurity requirements?
- Will the implementation or maturity of device cybersecurity capabilities and/or nontechnical supporting capabilities fail to satisfy key device cybersecurity requirements?
- What are the physical, logical access, network, and other requirements of the IoT device and how do they relate to key device cybersecurity requirements?

While NIST SP 800-213 goes into much greater detail as to the scope of these agency-facing questions, NIST was also tasked by the IoT Act to address the identification and reporting of vulnerabilities found in those devices, as well as other traditional IT systems. Accordingly, as mandated by § 5 of the IoT Act, NIST also published SP 800-216, *Recommendations for Federal Vulnerability Disclosure Guidelines*, which remains in draft at this writing. NIST SP 800-216 seeks to establish a flexible federal-vulnerability-disclosure framework that allows for the reporting of known or suspected security vulnerabilities in digital products. Its guidance offers the Federal Coordination Board ("a group of cooperating entities that collectively provide flexible, high-level vulnerability disclosure coordination among government agencies") as the primary interface for vulnerability disclosure reporting and oversight and taking a key role in addressing vulnerability disclosure in the Federal Government. To that end, NIST proposed to handle vulnerabilities by allowing for local resolution support while ensuring Federal Government oversight that could be applied to any software, hardware, and digital services under Federal Government control, including new vulnerabilities found in IoT, industrial control systems, medical devices, and traditional IT vulnerabilities.

With a task greater than just examining the impact of IoT on the Federal Government, NIST also turned its sights on helping manufacturers and contractors better understand the rubric within which agencies will be acquiring IoT.

Impacts on Manufacturers (*Makesa Lottastufficus*)—In its drive to address the security of IoT devices, NIST also updated and furthered its NISTIR 8259 series in an effort to facilitate a meeting of the minds between the Government and IoT device designers in the area of IoT cybersecurity for federal agencies. Like all things NIST, absent regulatory requirements (i.e., Defense FAR Supplement 252.204-7012/NIST SP 800-171), NIST guidelines are not regulations in and by themselves. They do, however, provide insight into what/how the Federal Government will examine or assess security standards. To that end:

- NISTIR 8259, *Foundational Cybersecurity*

Activities for IoT Device Manufacturers, gives manufacturers recommendations for improving the security of their IoT devices to help customers meet their cybersecurity needs and goals. Covering the entire lifespan of an IoT device, from creation to deployment, this IR provides a list of recommendations, activities, and support IoT device manufacturers should provide, including elements such as secure development/security by design, identity management, patching, and configuration management.

- NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*, applies the best practices from a variety of industry standards (e.g.,Cellular Telecommunications and Internet Association, National Electrical Manufacturers Association, Broadband Internet Technical Advisory Group, Industrial Internet Consortium, etc.) to provide a common starting point of six device cybersecurity capabilities that may be needed by many customers in many IoT use cases to support various cybersecurity risk mitigation goals. These include:
  1. Device Identification: The IoT device can be uniquely identified logically and physically.
  2. Device Configuration: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.
  3. Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
  4. Logical Access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
  5. Software Update: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.
  6. Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.
- NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*, suggests the starting point for non-technical support capabilities provided by manufacturers and/or third parties (i.e., supporting entities) that can assist customers' cybersecurity risk mitigation goals. These four core capabilities include:
  1. Documentation: The ability for the manufacturer and/or the manufacturer's supporting entity, to create, gather, and store information relevant to cybersecurity of the IoT device prior to customer purchase, and throughout the development of a device and its subsequent lifecycle.
  2. Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive information and queries from the customer and others related to cybersecurity of the IoT device.
  3. Information Dissemination: The ability for the manufacturer and/or supporting entity to broadcast and distribute (e.g., to the customer or others in the IoT device ecosystem) information related to cybersecurity of the IoT device.
  4. Education and Awareness: The ability for the manufacturer and/or supporting entity to create awareness of and educate customers and others in the IoT device ecosystem about cybersecurity-related information, considerations, features, etc. of the IoT device.
- NISTIR 8259C (draft), *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*, describes the method of profiling the baselines in NISTIR 8259A and NISTIR 8259B to create a more detailed set of capabilities responding to the security concerns of a specific industry/sector into which the IoT devices would be sold. This profile is based on three central concepts:
  1. Device-centricity—focusing on cybersecurity at the device level and not just at the network level.
  2. Cybersecurity focus—recognizing that while IoT device functionality may sometimes trump security concerns, cybersecurity still needs to be considered.

3. Minimal Securability—identifying that manner and support needed for a customer to integrate the device into a secure system.

- NISTIR 8259D (withdrawn), *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*, provided a now-withdrawn examination of the needs of the federal marketplace against the requirements of NIST SP 800-53. Based on feedback received to the draft, NIST withdrew NISTIR 8259D as a standalone document, and instead, included it as an appendix to SP 800-213A with updated content. The appendix provides useful insight into the environment IoT device manufacturers may find themselves when selling to a savvy federal customer.

The IoT Report Card (*Actus Tardi*)—In reviewing the status of the Act and the Federal Government's security stance related to IoT, GAO recently identified some significant issues in the IoT Act's execution. On Dec. 1, 2022, GAO issued its report, as required under §§ 7 and 8 of the IoT Act, on the current state of implementing the requirements under the IoT Act and broader IoT efforts. The report, *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices* (GAO-23-105327), noted that while NIST has issued IoT device cybersecurity guidance, as mandated by § 4 of the IoT Act, and also its draft recommendation on reporting security vulnerabilities, in response to § 5 of the IoT Act, OMB appears to be having trouble with their rocket skates.

Although NIST's IoT cybersecurity guidance and draft vulnerability disclosure guidelines may have arrived later than directed, OMB has yet to complete any of the mandates imposed on it by the IoT Act. First, once NIST had issued its IoT cybersecurity guidelines, OMB was directed to review agency information security policies and principles, and issue any policies and principles necessary to ensure agency policies were consistent with the NIST guidelines. The GAO report notes that "[t]o date, OMB has not yet developed guidance on security vulnerabilities. Consistent with the act, it is to do so if deemed necessary." An inauspicious start when the IoT Act directed OMB to develop and oversee the implementation of any security vulnerability policies, principles, standards, or guidelines no later than Dec. 4, 2022.

What GAO does point out is that OMB has not yet established a standardized waiver process for agency CIOs to utilize if the procurement of non-compliant IoT devices qualifies for a waiver under the Act. As noted above, as of Dec. 4, 2022, the IoT Act prohibits the head of an agency from procuring an IoT device if the agency CIO determines that such a device does not comply with the (now-existing) NIST standards and guidelines issued under §§ 4 or 5 of the Act. Although these guidelines have been issued, OMB has not established a standardized waiver process. The result is a classic *Looney Tunes* setup where Wile E. Coyote (the Federal Government), using various traps and barriers at its disposal (NIST, OMB, etc.), tries to catch the elusive Road Runner (IoT devices) who is set to arrive on Dec. 4, 2022. Unfortunately, all of its planning is for naught, as the time has come and gone without the trap sprung. Cue the sad trombone and the reset.

OMB's delay in establishing a standardized waiver process presents challenges to both contractors and agencies alike. Without a standardized process, agencies are at risk of haphazardly granting or denying IoT device waivers. An inconsistent waiver regime will subject the contractor community to unnecessary costs and burdens as they attempt to reconcile conflicting standards. As GAO puts it, "any inconsistencies in agencies' non-standardized processes may increase the risk of inconsistencies in waiver decisions."

The Takeaways (*Magnum Consilium*)—All told, when OMB is finally up and running after the tail of IoT, the guidance provided by NIST suggests that IoT device manufacturers should be prepared to respond to Federal Government purchaser questions and confusion. Beyond merely providing guidance on the specifics of the device and how it works, manufacturers (and their sales staff) may also need to field questions related to the device's secure development, supply chain, vulnerability management, and maintenance/updates/patching. To that end, manufacturers who provide or intend to provide IoT functionality should be prepared to answer the following key questions:

- Does the manufacturer use secure development in the creation of its IoT devices?
- Does the manufacturer use secure supply chain practices to support its operations?

- How robust and mature are the manufacturer's vulnerability disclosure and remediation practices?
- What should customers expect related to the delivery of software updates/patches in response to discovered vulnerabilities?

In advance of receiving those questions, manufacturers and contractors should take it upon themselves to prepare their staff and their technology to understand and adopt the core competencies of secure IoT devices. Cybersecurity by design and a clear understanding of IoT device vulnerability disclosure procedures are likely to be nonnegotiable, so designs, features, and functionality all need to be assessed with NIST in mind. And note that just because those IoT devices may presently be in the hands of federal customers, the law prohibits agencies from "renewing" contracts that fail to meet the NIST guidelines and (eventual) OMB policy.

Contrary to what you may believe, in the 73 years that Wile E. Coyote has been chasing the Road Runner (yes, you read that right—73 years), the Road Runner was eventually caught. Once. (See "Soup or Sonic," May 31, 1980). After a series of events that led to the Road Runner growing to immense size, it simply stopped and granted the now-tiny Wile E. Coyote his life's ambition—to catch him. The incredulous coyote then asked (via signage of course) "Okay, wise guys,—You always wanted me to catch him. Now what do I do?" The same may be true for IoT. As it grows and grows, there may finally come a window that will eventually permit regulations to catch up. But as and if cybersecurity remains a critical point of concern with procuring agencies, it can't take decades. And, as *Looney Tunes* may have demonstrated decades ago, it will likely be the result of industry's lead.

In conclusion, we'd be criminally remiss if we did not end with …"That's all folks!"

♦

This Feature Comment was written for The Government Contractor by* Alexander Major *and* Philip Lee. *Mr. Major is a partner and co-leader of the Government Contracts & Global Trade Practice Group at McCarter & English, LLP. Mr. Lee is an associate in that group.