CYBER DEVELOPMENTS IN THE WIRELESS AND COMMUNICATIONS WORLD

Michael F. Violette, P.E.
Washington Laboratories and American Certification Body

Introduction

The advent of several regulatory initiatives in 2025 will make their impact on the Wireless and Communications industry. It is well-known and well-publicized that hacking and subversion of communications and infrastructure by bad actors continues to rise. This is "felt" every day by consumers, public safety and services, defense and, by all rights, every sector of our modern society. The growing implementation of "connectivity everywhere, all-the-time" means that necessary measures must be taken at the device design, testing and integration into networks. The actions by bad-actors (for whatever gains they hope to achieve monetary, civic instability, pilfering of design…it goes on…means that security precautions are now more-than-necessary.

There are many reported instances of Cyber-Weaknesses and the industry and regulators are clawing back management of this space. In the US, a strong lead by the National Institute of Standards and Technologies (NIST) has been on the forefront of leading Cyber infrastructure protections. The NIST Cybersecurity Framework (CSF 2.0) is designed to support industry, government and other organizations. CSF 2.0 is becoming well-organized and accepted. I liken this to the early 1990s when the goals and objectives of Telecom Mutual Recognition Arrangments, well-intentioned and, one would say inspired—have been worked out and are working well.

As a quick aside, I recently purchased an electric shaver to beat back my stubble. I chuckled when a flyer in the packaging suggested that I download an app for the shaver. Huh? I'm not sure that an electric shaver needs to be IoT-ready, but evidently, someone does.

This article outlines recent and near-term Cyber-security protections that are being enacted by US, Canada, the European Union, among others. At the core, the balance of protections and free-trade are sometimes in-conflict or, at the least, trying to find a common ground.

A few of the Cyber-based efforts are below:

Cybersecurity Acts include (see footnotes)
[1]

1. **EU Cybersecurity Act**: Introduces an EU-wide certification framework for ICT products, services, and processes.
2. **Federal Information Security Modernization Act (FISMA)**: Provides a framework to protect government information operations against cybersecurity threats.

[1] https://www.jdsupra.com/legalnews/health-infrastructure-security-and-1139975/
https://www.cbo.gov/publication/59481.
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
Federal Information Security Modernization Act
https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

3. **Health Infrastructure Security and Accountability Act**: Sets stringent minimum cybersecurity standards and requires annual audits for compliance.

These are broad mandates driven by regulators, but supported by many industries and sectors that recognize the real risks of penetration of networks and devices for ill-gains.

NIST is taking strong positions on education and frameworks under the drive to provide cyber protections.

"The **NIST Cybersecurity Framework** (**CSF**) is a set of voluntary guidelines designed to help organizations assess and improve their ability to prevent, detect, and respond to cybersecurity risks. Developed by the U.S. National Institute of Standards and Technology (NIST), the framework was initially published in 2014 for critical infrastructure sectors but has since been widely adopted across various industries, including government and private enterprises globally. The framework integrates existing standards, guidelines, and best practices to provide a structured approach to cybersecurity risk management." https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

So far, voluntary, but in practice it is increasingly used by organization as a mandatory activity. This, especially in the government space is relied on and pushed to vendors if they want to have USGOV involvement.

As a private enterprise, our organization takes a strong protective attitude about the exposure of our operation to the Internet, balancing access with protections.

Entities have full-time teams that must continuously be vigilant against nominal hacking and viscous attacks. At any level, organizations that have exposure the Internet need to take measures to ensure immunity.

United States Cyber-Security Activity

There are broad and narrow protections that the US Government has taken at the Enterprise (business) level and at the device (consumer/user) level. Some include outright exclusion of some entities from achieving access to the US communications environment.

Principally and, in a view, unfortunately, are the threats that come with of our largest trading partner(s). These have percolated over time and have forced the US to take certain actions.

Some of these are draconian, but necessary to protect the integrity of communications and supply chain networks.

To wit, the FCC has published a "Covered List" of companies that are outed in a KDB 986446 D01 Covered Equipment Guidance v03 entitled "Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program" published in August 28, 2024. These companies are nearly exclusively from the People's Republic of China (PRC). This expands on a developing list of communications infrastructure providers who are banned from connecting their equipment to the US communications networks, notably (and historically Huawei and ZTE who, allegedly or positively connected to the PRC Peoples Liberation Army, PLA).

A list of these companies are found in the following Table, with a short description of their infraction and the date they were placed on said list. The most recent addition is **Kaspersky Lab, Inc.,** a Russian-owned entity that is based in Moscow. Needless to say, these concerns about the PRC and the Russian Federation are well-founded and rise to a level of National Security.

The following table shows the most recent list of companies in the Covered List.

Table 1. Covered List or Services

Covered Equipment or Services	Date of Inclusion on Covered List
Telecommunications equipment produced by **Huawei Technologies Company**, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced by **ZTE Corporation**, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by **Hytera Communications Corporation**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by **Hangzhou Hikvision Digital Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by **Dahua Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Information security products, solutions, and services supplied, directly or indirectly, by **AO Kaspersky Lab** or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by **China Mobile International USA Inc**. subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by **China Telecom (Americas) Corp.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by **Pacific Networks Corp** and its wholly-owned subsidiary **ComNet (USA) LLC** subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by **China Unicom (Americas) Operations Limited** subject to section 214 of the Communications Act of 1934.	September 20, 2022
Cybersecurity and anti-virus software produced or provided by **Kaspersky Lab, Inc.** or any of its successors and assignees, including equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software.	July 23, 2024

The last entry in the above table is a bit ironic, given their stated mission of cyber protections, but considering their origins, it is hardly surprising that they have "earned" a spot on the list.

Further, the FCC has recently implemented a **Cyber Trust Mark** Program that mandates that certain equipment (so far) show protections against attacks that compromise data, penetration protections and monetary losses. This particular action is mostly for the protection of consumer but may (and probably will) broaden to everything that gets Certified under the Equipment Authorization program. The

Equipment Authorization Program is a system that companies that have wireless equipment must file for Certification, exclusively through the system of the Telecommunications Certification Body (TCB) program which is tasked to test, review and certify devices (under the purview of the OET, of Office of Engineering and Technology).

The purpose of the Cyber Trust Mark is, again, to protect against compromising equipment that is exposed to the Internet. The program is still-evolving, in real ways, but will ultimately lead to protections for the US communications infrastructure. Details are here: https://www.fcc.gov/CyberTrustMark. For the moment it is voluntary, but expect that to change...

In this author's my opinion, it won't be long until this voluntary program will become mandatory for device approvals. This is in-step with the coming EU requirements for Radio Equipment under the Radio Equipment Directive and Cybersecurity Act, discussed in the next section.

What this means for device compliance is profound and must be considered for IoT-related devices that may be vulnerable (which is, to say, everything, from video systems to baby monitors to, apparently, electric razors. For me, I'm going back to the shaver my grandfather used to use, leather strop, lather and all).

The FCC's Cyber Trust Mark is shown here:

As is stated at the FCC's information page on this topic, the FCC is still "standing up" this comprehensive program. The rollout of this program is, likely, to be in the next year or two or by 2026. A structure is still being worked out wherein US-based firms (only, at this time) can issue the Cyber Trust Mark.

European Union Cyber-Security Activity

For context, the Radio Equipment Directive 214/53/EU has been a very successful program under the European Union that provides for a comprehensive route to protect the Radio Spectrum. The industry, regulators and society (although only a small percentage of the population knows this) rely on standard approaches to control interference, improve communications performance and ensure that the device in your hand will work across various networks. These networks include, among others, cellular systems, local WiFi, something called LoRa (Long Distance Radio) which extends, in a sense, the connectivity of IoT and other devices. In essence, the LoRa frequency ranges propagate farther than the WiFi and Cellular frequencies. This is handy for sensors and other communications implementations. A comprehensive overview is found here: https://www.thethingsnetwork.org/docs/lorawan/regional-parameters/. The long-distance record for data transmission is now 1336 km or 830 miles!

I digress, however, one can simply note that the cyber-protections must include a sometimes dizzying array of devices and technologies.

ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) was initially enacted

There has been a lot of work being done in the European Union (EU), most notably implementation of so-called Article 3.3 d/e/f of the Radio Equipment Directive (RED). An August 1, 2025 deadline approaches wherein this particular part of the RED comes into force. There is a strong movement to comply and opportunities lie for multinational players to help the industry maintain their market access, which is difficult enough in the practical realities of global product approvals.

Article 3.3 d/e/f deal with network security, protection of personal data and prevention of fraud. Article 3.3 d focuses on devices, primarily, to minimize the quasi-physical threats of compromising a device. Article 3.3 e is self-explanatory but not always easy. For example, how does a service provider or device manufacturer demonstrate that personal data is not subject to "spoofing." This, in a practical way, means solid firewalls as well as education of operators and users to not be fooled by poaching attacks. This is, in a way, tightly coupled with Article 3.3 f, which can occur if the proper protections are not imbued in the device design or the operation of the device. But humans are subject to being 'fooled' and the best a device manufacturer or operator can do is to limit damage in some cases or have backups or built-in protections.

Evaluations of equipment and systems must include physical, data and protocols for "disaster recovery" which typically include some kind of Risk Assessment (RA) to ensure that procedures are in-place to limit damage, physical or otherwise, from pernicious effects of the intent of "bad actors," which can be domestic or foreign agents intent on disrupting or stealing from any manner of devices connected to the Internet, either directly or indirectly.

Eventually, the EU Cybersecurity Act will affect broad areas of the industry and nearly any internet device (connected directly or indirectly). This act affects large swaths of the industry and, in a read, is not voluntary, but will be mandatory for "ICT" devices, which includes just about everything.

Industry Actions

Regardless of the regulatory environment, Industry is taking on their own sets of protections, requiring that vendors demonstrate that suppliers have Cyber-protections in-place. This requires a set of internal and external measures that protect design and data integrity, especially when dealing with personal information. Vendors, more and more, have to build the operational infrastructure to manage the internal affairs. Sometimes, these might just be "checklists" or may be the stuff of audits and more scrutiny by third parties. It all depends on a few things, each one of these add a twist to staying in compliance.

1. Oversight by government or regulators
2. Internal policies
3. Industry trends

In our compliance world, Accreditation Bodies (ABs) may perform a role in having a third party, independent assessment. This activity often involves a mix of remote or on-site reviews of documentation, procedures, training or other proof of competence. A Certification Body (CB), notably under the FCC's Equipment Authorization Program has to comply with ISO 17065 and, potentially ISO 17025 for testing laboratories. ABs may follow ISO 17011 and Personnel Certification according to ISO 17024. Many of the same principles apply to the various ISO 170XX, but at the core is the demonstration of confidence.

This is extending into the Cyber space, with its particular focus on protections of networks, people and personal information. The framework of the assessment is the same with the particular focus depending on the intent and content of the standard that is being assessed.

Many companies are taking it into their own hands by requiring compliance with these ideals as a condition for working with them. It simply is what it is and it is for a good cause. In any event, it becomes a business decision: if a company wishes to work in this increasingly complex space of inter-connectedness, they must go through the actions and it is not capricious. It involves a management-level decision to move the organization in that direction. The implementation of procedures affects all levels of an operation, from design to communication to inventory to supply chain verification.

This last point may be a little tricky because a vulnerability exists at the chip-level: this is why suppliers on the Covered List are suspect because it is conceivable, if not already happening, that malicious code can be embedded in the firmware of a microprocessor or other critical data part that can listen and report-out activities of the user(s). For the integrator, there is practically no way to know this and that is the difficult part for manufacturers who have wider goals and implementations of the technologies.

This goes right to the heart of the protection of IoT devices: "Someone might be listening…"

International Cooperation

The ISO documents reference above are International Standard Organization documents, which implies that there are many organizations at the table. For the narrow purpose of the importance of US/EU trade, the ISO documents are key. It is not uncommon for individual countries to adopt the ISO requirements to suit their own National Standards structure, however in the majority of cases the text(s) are the same.

A success story: The European Union and North America (at least for now) have Mutual Recognition Arrangements (MRAs) which have allowed for a free flow of goods across the borders. The MRA include EMC and Radio regulations that have worked very well for US/Canada manufacturers.

Yet this structure does not only affect US/CN/EU trade, but the approvals are often used for market access for other countries wherein the regulatory structure is not in-place or the regulatory structures have not matured (and, depending on the size of the economy) may not be warranted. That is, these countries don't need a full-

blown regulatory structure and oftern rely on “CE Marking” or “FCC Certification” for placing products on the market.

These MRAs have been in-place for EMC and Radio equipment for a few decades, allowing access to markets under a combined mix of international and domestic regulations.

It remains to be seen if the MRAs will include some of these new Cyber provisions. For the moment, the FCC is requiring any entity that issues a Cyber Trust Mark approval be located in the US. Reciprocally, but perhaps malleable is the EU is not recognizing Notified Bodies for the Cyber approvals outside of the EU. In effect, each country/economy is becoming more focused on protecting their industries

Perhaps this will change, but with the current political climate in-flux, at the time of this posting, it is not sure how this will look in a few years, or even sooner, but as happens with most regulatory actions (and practically so) it won’t ever be rolled back.
Whatever the final outcomes (and they are NOT static, mind you) these frameworks are here to stay.