Cyber-Security
for Product Compliance

Michael F. Violette, P.E.
Mike Urban
Christina Karlhoff
Neil O'Connor
Washington Laboratories, Ltd & American Certification Body
4840 Winchester Blvd, Suite 5
Frederick MD 21703

Agenda

Overview – Part I

- Background
- Definitions
- Three main Areas
  - Regulatory
  - Voluntary
  - Mandatory
- Compliance Procedures

Public Concerns

…research conducted by Consumer Reports indicates that more than half of consumers surveyed were concerned about the information collected by connected devices.

-Letter from Stacey Higginbotham, Policy Fellow, Consumer Reports, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, Attach. *CR IoT Security Label Summer Research* at 4 (filed Dec. 13, 2023) (*Consumer Reports Summer Research*).

Washington Labs & ACB

EMC, Environmental, Product Safety & Radio Frequency Expertise

Commercial

Consumer

Defense & Aerospace

Energy

Wireless Certifications

Internet of Things (IoT)

WL Project Experience

Over 20,000 projects since 1989

- NASA
- Raytheon
- US Army, Air Force & Navy
- General Electric
- Westinghouse
- Hughes Network System
- Applied Physics Laboratory
- Exelon
- 35+ Nuclear Power Plants
- Research Universities
- Over 500 individual clients

My Background

BSEE, Virginia Tech, 1984

Professional Engineer (Virginia)

iNARTE-Certified EMC Engineer

European Union Notified Body for Radio Equipment and EMC disciplines

IEEE Senior Member

Founder and Director, Washington Laboratories and American Certification Body

Developed related companies in China, Taiwan & EU

Background

Products, Testing and Certifications now Globalized

FCC De-regulated Product Certifications

CE Del

NPRM for (voluntary) Cyber-Labelling: Cyber-Labs!

Global demand for Security of Government and Consumer

European requirements emerging (RED, Cyber-resiliency)

Compliance Definitions

EMC: Electromagnetic Compatibility

- Emissions: Unwanted radiated and conducted electrical energy
- Immunity: Undesirable response to external electrical energy

Product Safety

- Protection from Electrical, Mechanical, Fire and Chemical Hazards

Environmental

- Restriction on Hazardous Substances

Radio Efficiency and Security

- Radio Equipment Directive (RED)

Now: Cybersecurity Protections

NIST

Formerly National Bureau of Standards

Standards-setting (physical standards, weight, length, mass, time, electrical quantities

Ten milli-ohm OHM @ 15C. 1887
Edison Machine Works*

One OHM @ 25C. Jan 25, 1939*

So Much More

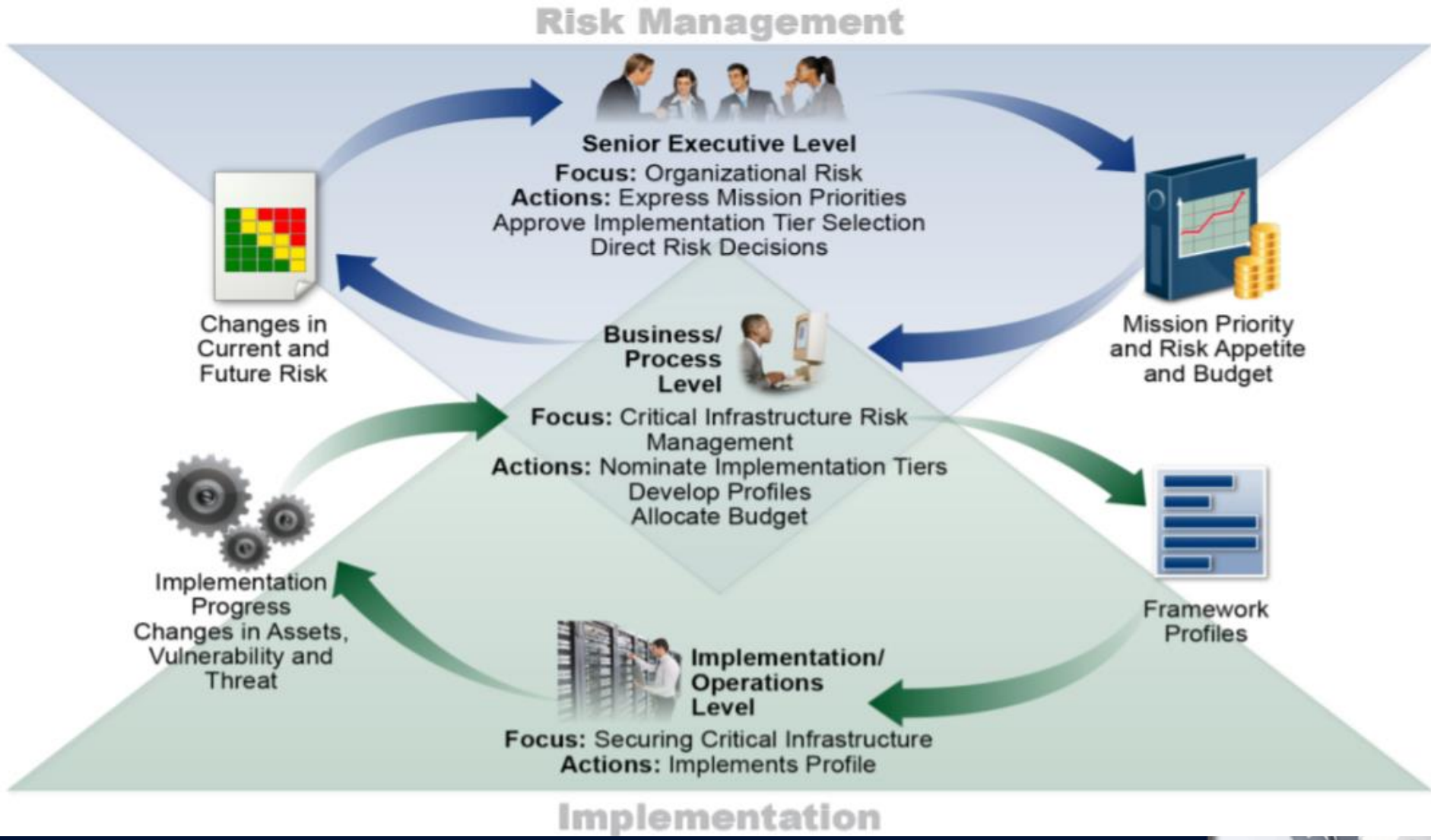
International Agreements, Procedures, Time!

*National Institute of Standards and Technology Digital Collections, Gaithersburg, MD 20899

NIST


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Thu Mar 14 7:15:47
National Institute of Standard
time.gov
Relaunch to update
Inbox - Outlook W...
Box for China
FCC OET E-Filing
WLL Database
eCFR — Code of F...
VEC Email
Google Maps
SonicWALL - Virtu...
SonicWALL - Virtu...
YouTube
ALASKA DAYLIGHT TIME
AKDT (UTC-8)
03:15:47 A.M.
ALEUTIAN DAYLIGHT TIME
HADT (UTC-9)
02:15:47 A.M.
HAWAII STANDARD TIME
HST (UTC-10)
01:15:47 A.M.
SAMOA STANDARD TIME
SST (UTC-11)
12:15:47 A.M.
CHAMORRO STANDARD TIME
CHST (UTC+10)
09:15:47 P.M.
PACIFIC DAYLIGHT TIME
PDT (UTC-7)
04:15:47 A.M.
MOUNTAIN DAYLIGHT TIME
MDT (UTC-6)
05:15:47 A.M.
CENTRAL DAYLIGHT TIME
CDT (UTC-5)
06:15:47 A.M.
EASTERN DAYLIGHT TIME
EDT (UTC-4)
07:15:47 A.M.
ARIZONA MOUNTAIN STANDARD TIME
MST (UTC-7)
04:15:47 A.M.
24-Hour Clock Display
Coordinated Universal Time (UTC)
11:15:47
UTC IS ALWAYS DISPLAYED AS A 24-HOUR CLOCK.
Your Device's Clock (UTC-4)
Today: 03/14/2024
07:15:47 A.M.
Your clock is off by: +0.028 s
PUERTO RICO ATLANTIC STANDARD TIME
AST (UTC-4)
07:15:47 A.M.
About/Contact

Compliance Definitions



Standards

Standards are Essential

NIST CSF expands into standards

EU Standards emerging as Cyber-Resiliency act expand coverage of Radio Equipment Director

Asia markets are keen on protections

Global issue affecting many Billions of Devices and Trillions of $

NIST Revised Protections

Cybersecurity Maturaty Model Compliance (CMMC)

DoD-developed in 2019, applies across the FEDGOV

Protect controlled and uncontrolled information

Uncontrolled Sensitive Information (trade secrets, e.g.

- Estimates that the adversaries ”steal” $60 B/year

Levels:

1. Basic cyber-hygiene (anti-virus, strong pws)
2. Protection requiring additional controls
3. Extension of NIST 800-171 R2 (Rev2) 47 Security Controls that must be compliant
4. Contractors must be pro-active to protect info from advanced persistent threats
5. Additional 30 extra controls, including auditing

Cybersecurity Framework CSF 2.0

General protections for all industries (past ~20 years)

This voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk.

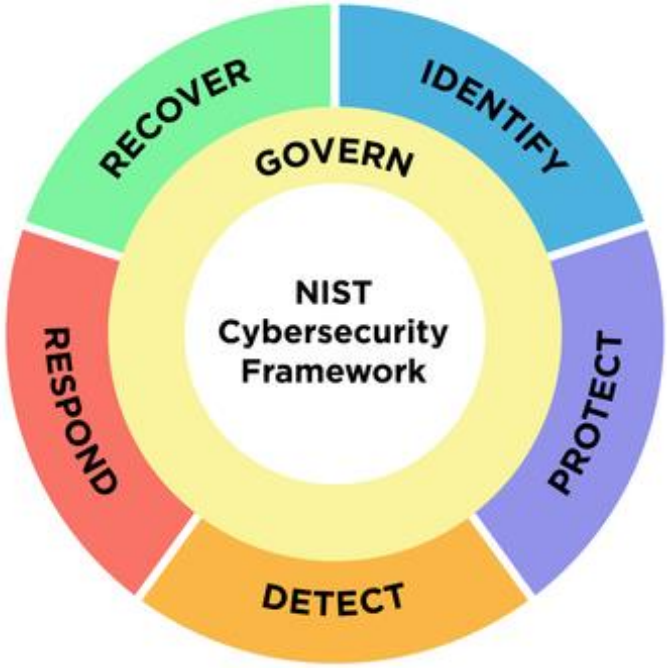
“The CSF provides high-level guidance, including a common language and a systematic methodology for managing cybersecurity risk across sectors and aiding communication between technical and nontechnical staff.”

Cybersecurity Framework CSF 2.0

Expanded to providing cybersecurity for all organizations regardless of type or size

Five Components:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover



Cybersecurity Framework CSF 2.0

Genomic data science is a field of study that enables researchers to use powerful computational and statistical methods to decode the functional information hidden in DNA sequence. Applied in the context of genomic medicine, these data science tools help researchers and clinicians uncover how differences in DNA affect human health and disease.

Human health and science

EUROPE: ETSI EN 303 645

ETSI EN 303 645 is a globally applicable standard for consumer IoT cyber security; it covers all consumer IoT devices while establishing a good security baseline. The standard is based on 13 high-level recommendations, used to establish 68 provisions, 33 mandatory requirements and 35 recommendations.

TS 103701 has emerged as a leading candidate for IoT security Conformance Assessment

TS 103 645

5 Cyber security provisions for consumer IoT

5.0 Reporting implementation

5.1 No universal default passwords

5.2 Implement a means to manage reports of vulnerabilities

5.3 Keep software updated

5.4 Securely store sensitive security parameters 5.5 Communicate securely

5.6 Minimize exposed attack surfaces

5.7 Ensure software integrity

5.8 Ensure that personal data is secure

5.9 Make systems resilient to outages

5.10 Examine system telemetry data

5.11 Make it easy for users to delete user data

5.12 Make installation and maintenance of devices easy

5.13 Validate input data

IOT Challenges

ETSI TS 204 645 v 3.1.1 addresses

High-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated

A non-exhaustive list of examples of consumer IoT:

connected children's toys and baby monitors;

connected smoke detectors, door locks and window sensors;

Further List

IoT gateways, base stations and hubs to which multiple devices connect;

smart cameras, smart speakers and smart TVs together with their remote controls;

wearable health trackers;

connected home automation and alarm systems, especially their gateways and hubs;

connected appliances, such as washing machines and fridges; and

ETSI TS 103 645

Doc. Nb. TS 103 645 Ver. **3.1.1** Ref. **RTS/CYBER-0090** Technical Body: CYBER Details and Download	**CYBER;** **Cyber Security for Consumer Internet of Things: Baseline Requirements** Securing Consumer IoT	**Published** Current Status: Publication (2024-01-15)
2 Doc. Nb. TS 103 645 Ver. **2.1.2** Ref. **RTS/CYBER-0049** Technical Body: CYBER Details and Download	**CYBER;** **Cyber Security for Consumer Internet of Things: Baseline Requirements** Securing Consumer IoT	**Published** Current Status: Publication (2020-06-29)
Doc. Nb. TS 103 645 Ver. **1.1.1** Ref. **DTS/CYBER-0039** Technical Body: CYBER Details and Download	**CYBER;** **Cyber Security for Consumer Internet of Things** Securing Consumer IoT	**Published** Current Status: Publication (2019-02-08)

EUROPE

Radio Equipment Directive

Article 3.1

(a) Health and safety
(b) EMC

Article 3.2 Radio spectrum efficiency

Notified Bodies

Article 3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

(a)-(c): Inter-compatibility/functionality provisions

Until now, most of the work on radio devices looked at the above provisions as it relates to device compliance to the above Articles 3.1 and 3.2(a)-(c).

As yet, there are no harmonized standards that have been published to guide evaluations of devices. Leave lthe interpretation of these requirements with the Notified Bodies (and others).

- What's a Notified Body?

Cyberesiliency Act

Article 3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

(a)-(c): Inter-compatibility/functionality provisions

Until now, most of the work on radio devices looked at the above provisions as it relates to device compliance to the above Articles 3.1 and 3.2(a)-(c).

As yet, there are no harmonized standards that have been published to guide evaluations of devices. Leave lthe interpretation of these requirements with the Notified Bodies (and others).

However, on 12 January 2022, the EU Com published the Delegated Regulation implementing EU RED Art 3.3 d), e), f) covering Cyber Security.

The legal date is comes into effect is 1 August 2023 with compliance by manufacturers by 1 August 2023 with the pre-amble to the document stating:

“Whereas:

(1) Protection of the network or its functioning from harm, protection of personal data and privacy of the user and of the subscriber and protection from fraud are elements that support protection against cybersecurity risks.