



VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Regulaciones, leyes y prácticas de IoT a nivel global

Felix Uribe
University of Maryland Global Campus



VII CONGRESO DE INFORMÁTICA FORENSE & CIBERSEGURIDAD



Capacitaciones Pre y Post Congreso IFC-2023

Ocean
By H10 Hotels

26 al 29 de
Octubre del 2023

Descargo de Responsabilidad

Cualquier información relacionada con productos, procesos o servicios comerciales específicos por nombre comercial, marca registrada, fabricante u otro, no constituye ni implica mi respaldo, recomendación o favorecimiento de dicho producto u organización.

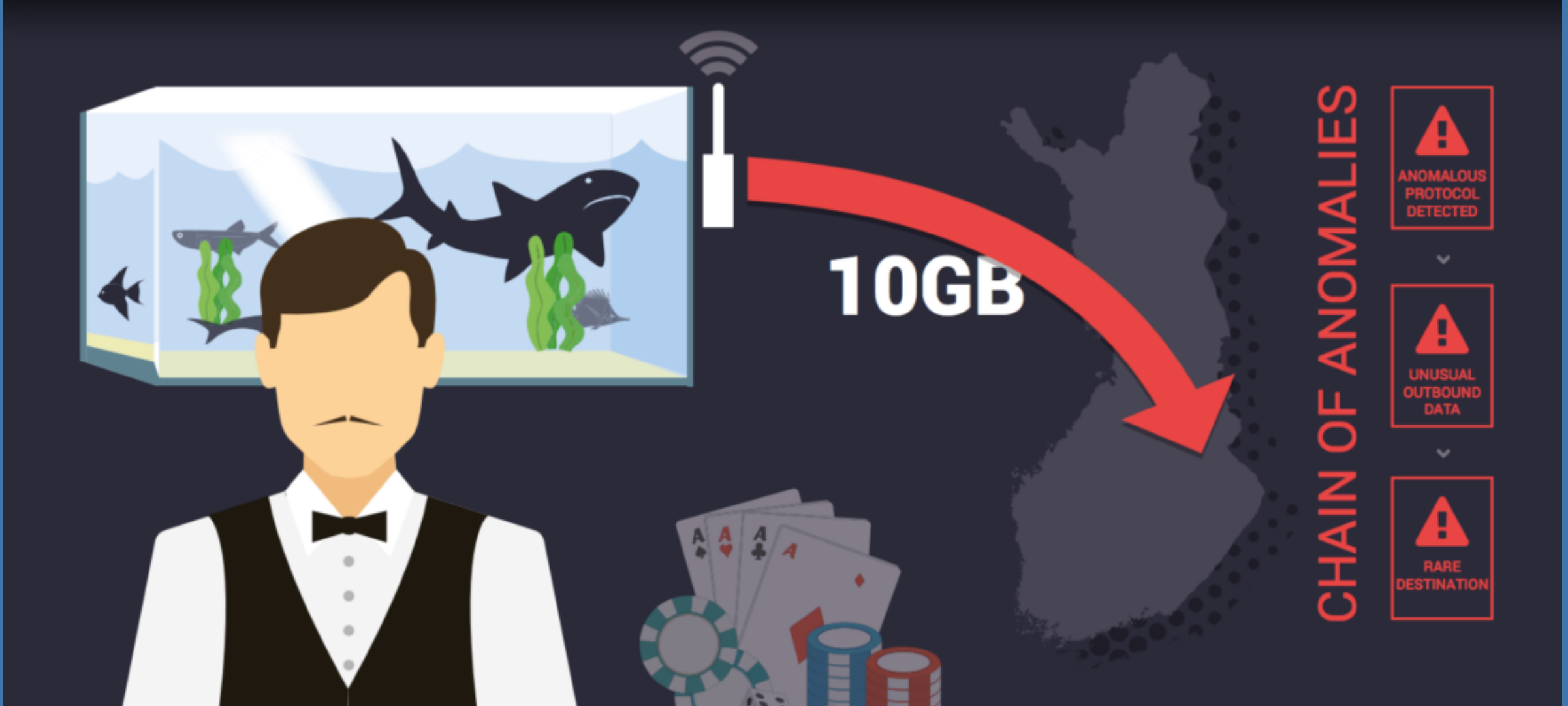


In the Beginning...



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

??????

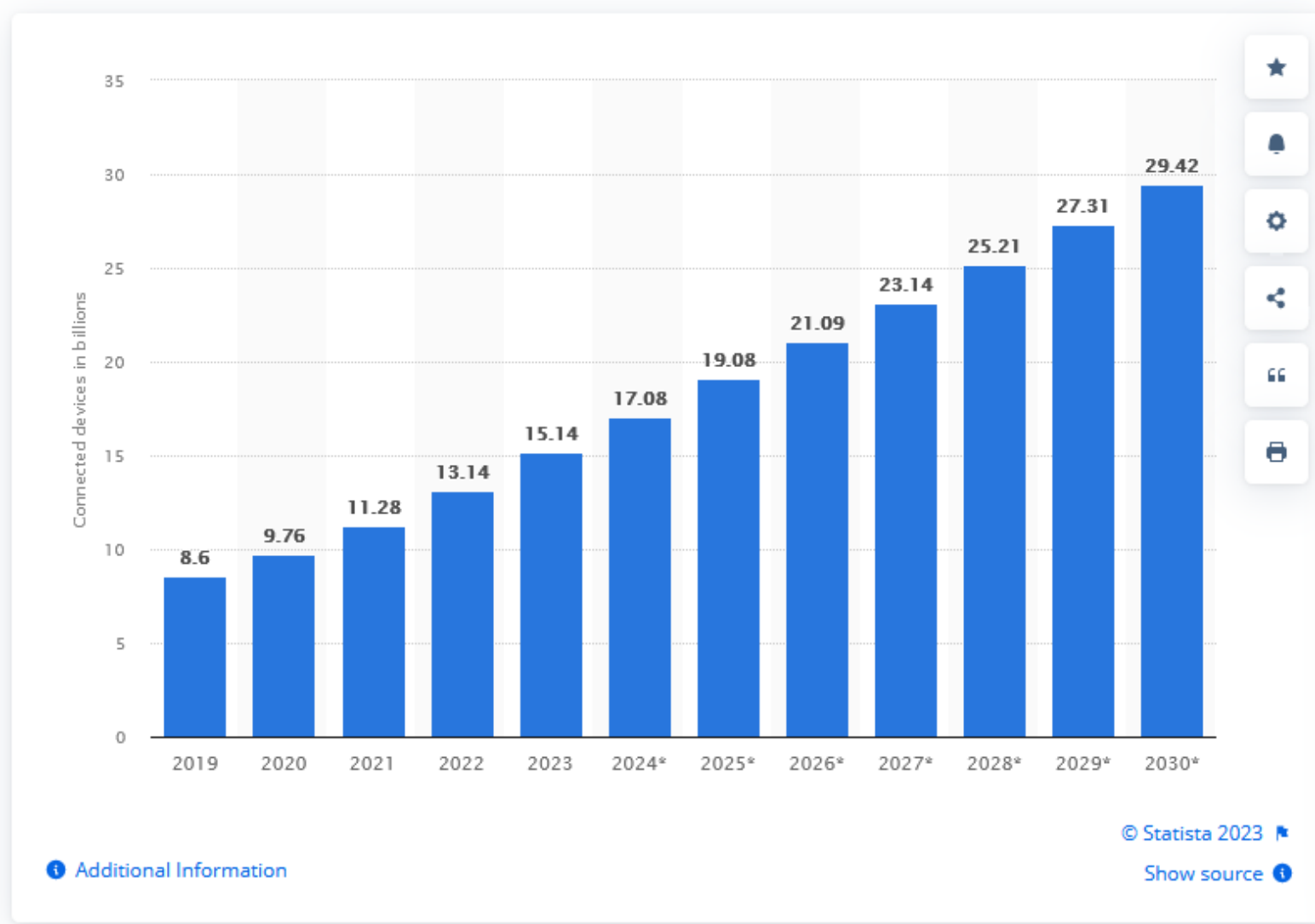


Source: <https://reefbuilders.com/2017/08/07/aquarium-controller-used-to-hack-casino/>

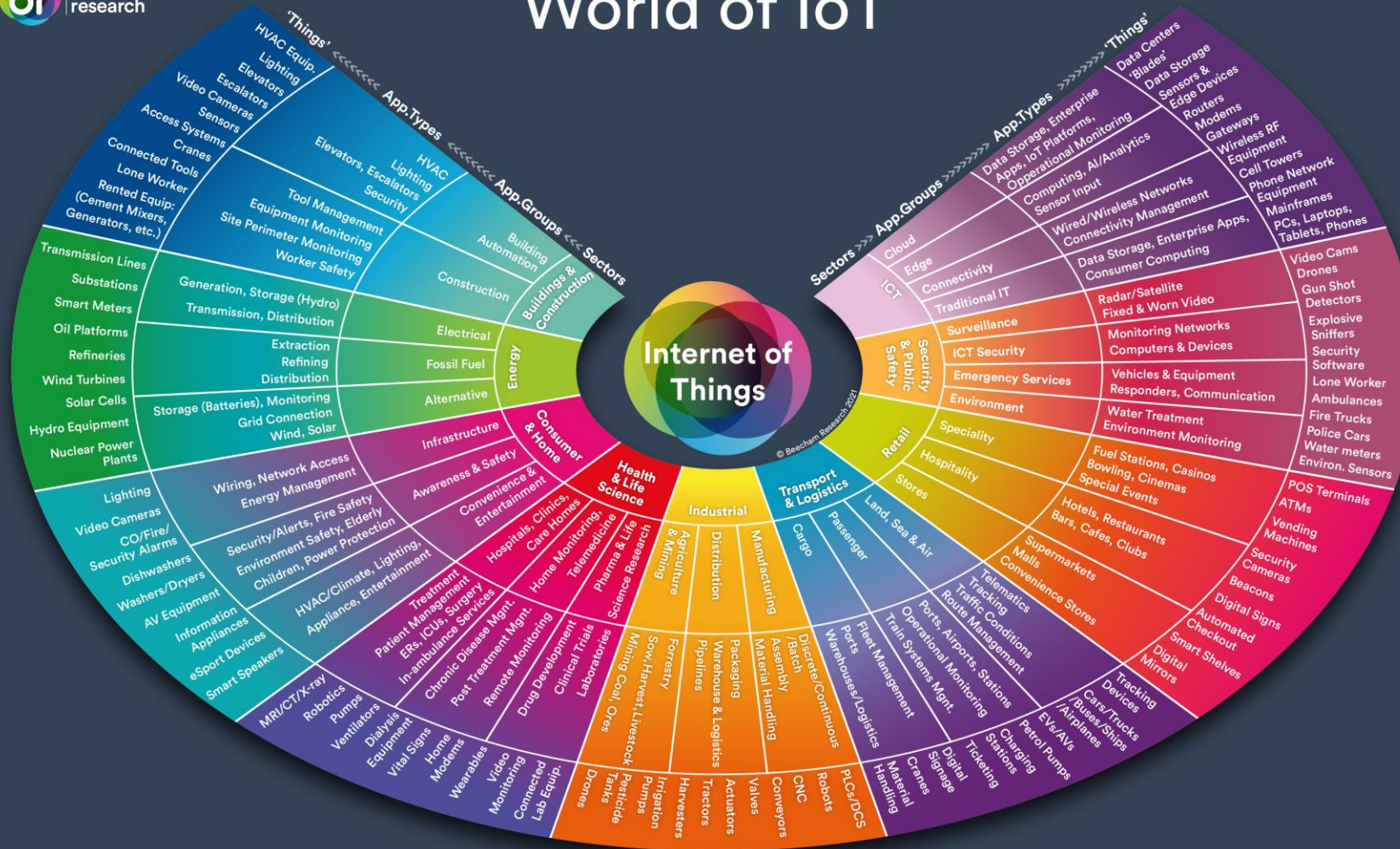
Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023

(forecasts from 2022 to 2030)

(in billions)



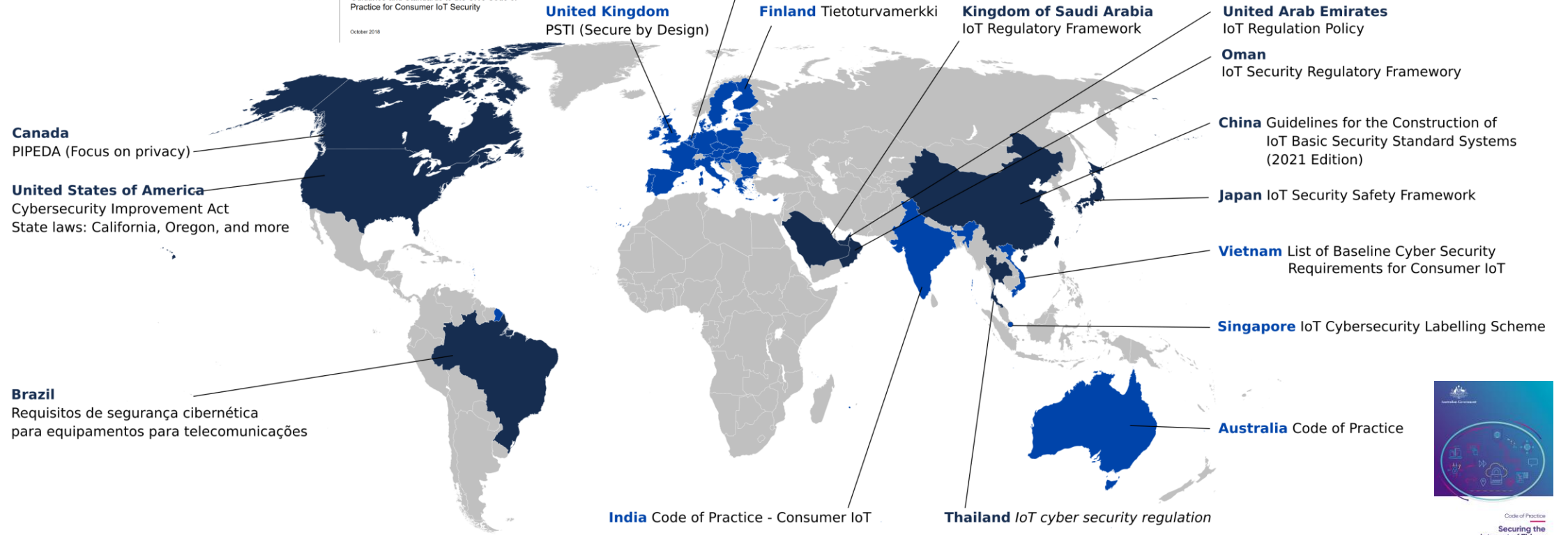
World of IoT



IoT Cyber Security Regulations across the world

Department for Digital, Culture, Media & Sport
 Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security
 October 2019

European Union Radio Equipment Directive: Delegated Act for cyber security
European Union Cybersecurity Act: IoT Certification Scheme
European Union Cyber Resilience Act



■ Regulation based on ETSI EN 303 645
 ■ Possible compliance by following ETSI EN 303 645
 On-going work



Source: <https://cetome.com/panorama>



European Union/United States



- **The General Data Protection Regulation (GDPR)**
Data **created and transmitted** via IoT devices may be subject to the General Data Privacy Regulation (GDPR).
- **Baseline Security Recommendations for IoT**
Critical information infrastructures.
- **Cyber Resilience Act (DRAFT)**
Protect consumers from insecure products by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services.
- **Cyber Security for Consumer Internet of Things: Baseline Requirements**

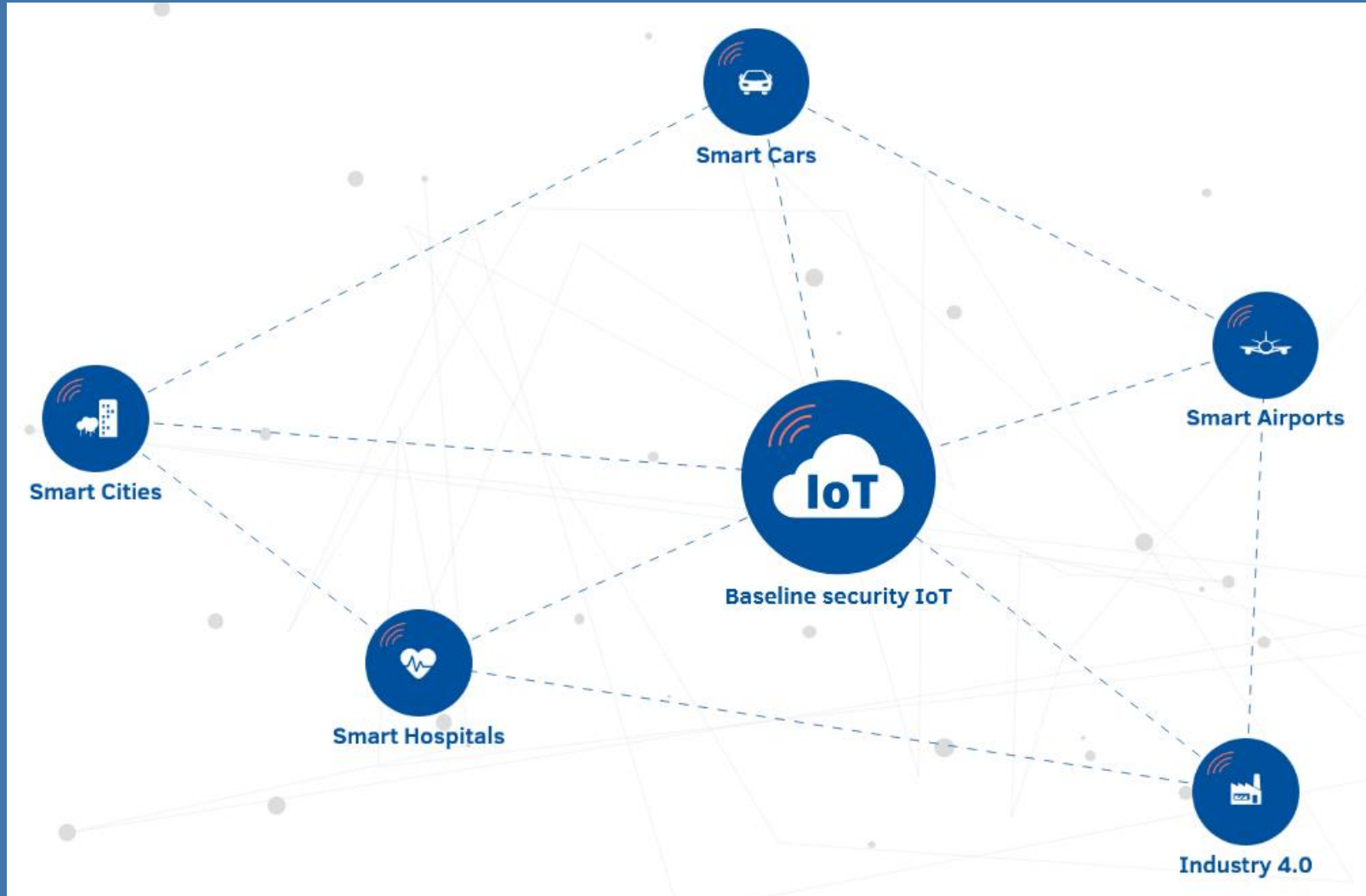
- **NIST Guides**
The Cybersecurity for IoT Program's mission is to cultivate trust in the IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools.
- **White House/OMB
Federal Agencies (CISA, FCC, DHS)**

NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline

ENISA Good practices for IoT and Smart Infrastructures Tool

This tool intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years.



NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8259A>



NISTIR 8259

Foundational Cybersecurity Activities for IoT Device Manufacturers

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8259>



NISTIR 8228

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkowitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8228>



NISTIR 8259B

IoT Non-Technical Supporting Capability Core Baseline

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8259B>



NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold
David Lemire
Brad Hoehn

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-213>

DoD Policy Recommendations for The Internet of Things (IoT)

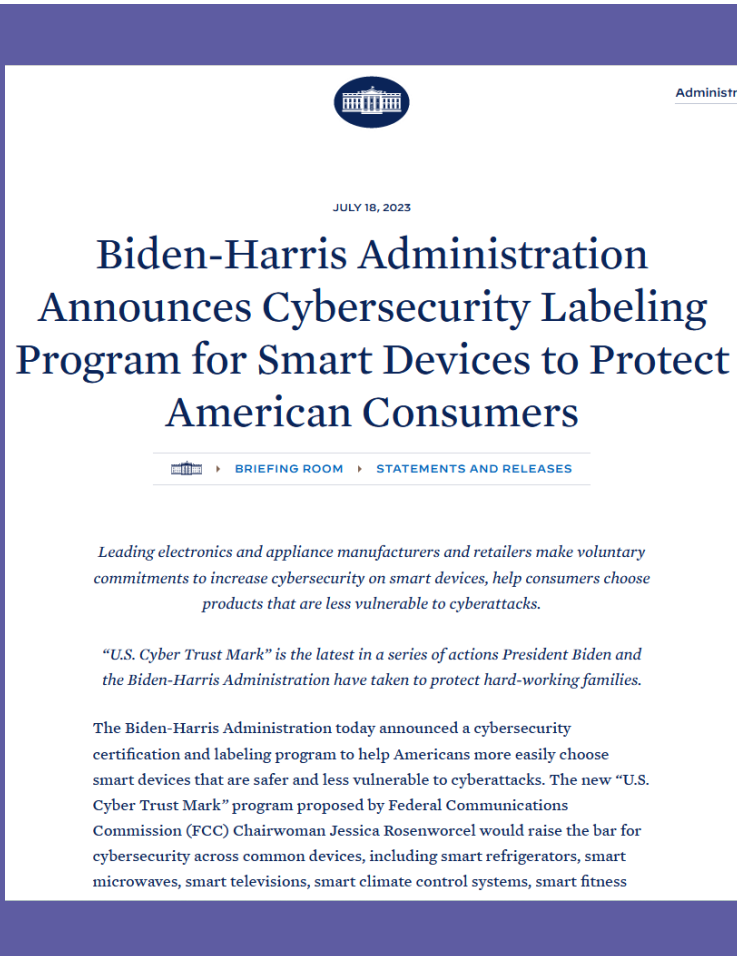
December 2016



Chief Information Officer
U.S. Department of Defense



U.S. Cyber Trust Mark



Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers

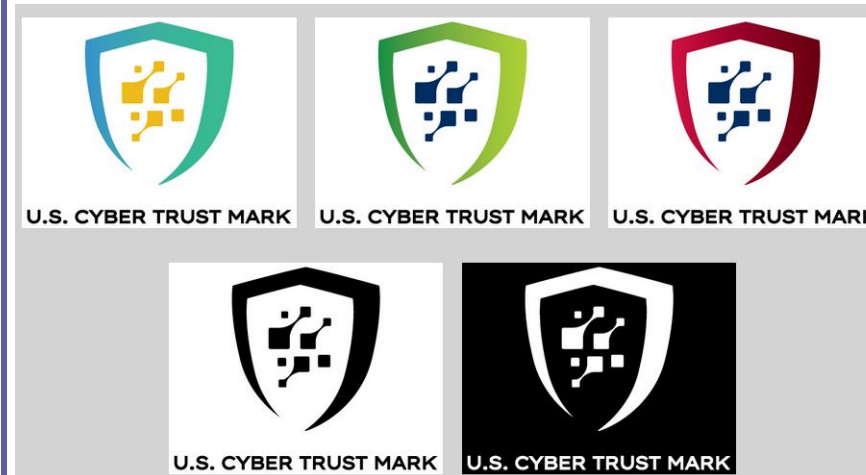
JULY 18, 2023

Leading electronics and appliance manufacturers and retailers make voluntary commitments to increase cybersecurity on smart devices, help consumers choose products that are less vulnerable to cyberattacks.

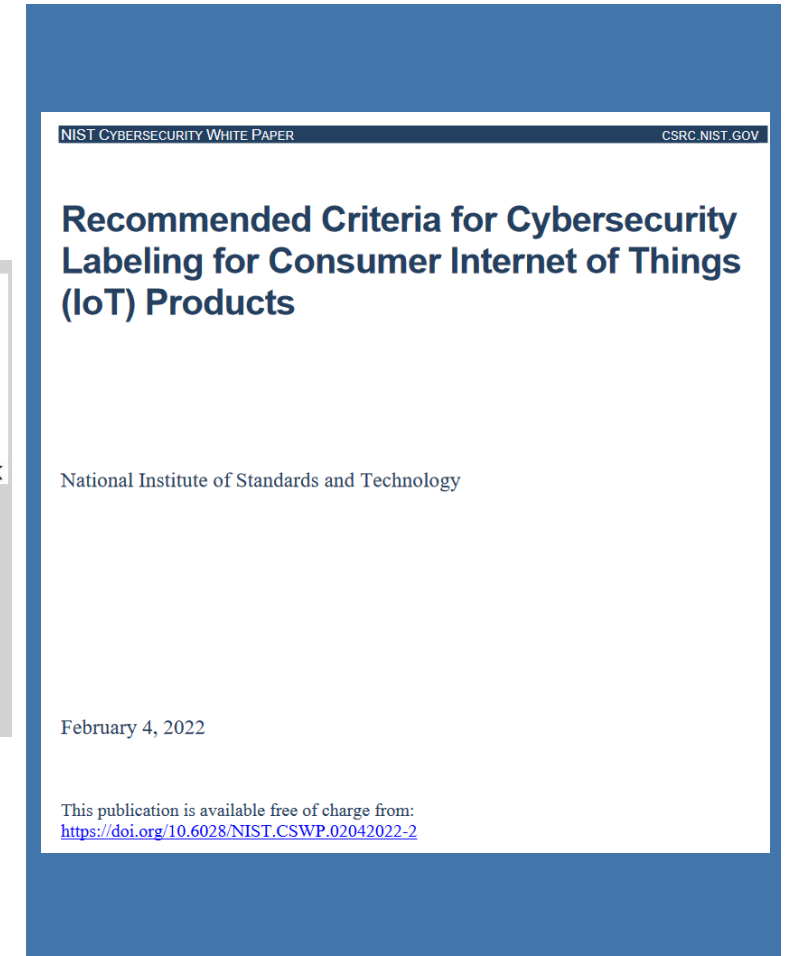
"U.S. Cyber Trust Mark" is the latest in a series of actions President Biden and the Biden-Harris Administration have taken to protect hard-working families.

The Biden-Harris Administration today announced a cybersecurity certification and labeling program to help Americans more easily choose smart devices that are safer and less vulnerable to cyberattacks. The new "U.S. Cyber Trust Mark" program proposed by Federal Communications Commission (FCC) Chairwoman Jessica Rosenworcel would raise the bar for cybersecurity across common devices, including smart refrigerators, smart microwaves, smart televisions, smart climate control systems, smart fitness

The Federal Communications Commission (FCC) is seeking public comment on a proposal to create a voluntary cybersecurity labeling program that would provide consumers with clear information about the security of their internet-enabled devices, commonly called "Internet of Things" (IoT) or "smart" devices.



Easily identify smart devices and products that meet widely accepted security and privacy standards by looking for the U.S. Cyber Trust Mark logo. The logo would appear on packaging alongside a QR code that you could scan for more information. The QR code would link to a national registry of certified devices so that you could compare these devices and get the most and up-to-date security information about each.



NIST CYBERSECURITY WHITE PAPER CSRC.NIST.GOV

Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products

National Institute of Standards and Technology

February 4, 2022

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.02042022-2>

IoT Cybersecurity Improvement Act of 2020



- First federal law in the United States to regulate the security of IoT devices.
- Smartphones, laptops, and other electronic devices are not covered by the statute.
- IoT device manufacturers must follow new standards and regulations in order to meet these government agency requirements.

PUBLIC LAW 116–207—DEC. 4, 2020

134 STAT. 1001

Public Law 116–207
116th Congress

An Act

To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes.

Dec. 4, 2020
[H.R. 1668]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Internet of Things Cybersecurity Improvement Act of 2020” or the “IoT Cybersecurity Improvement Act of 2020”.

Internet of Things Cybersecurity Improvement Act of 2020.
15 USC 271 note.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

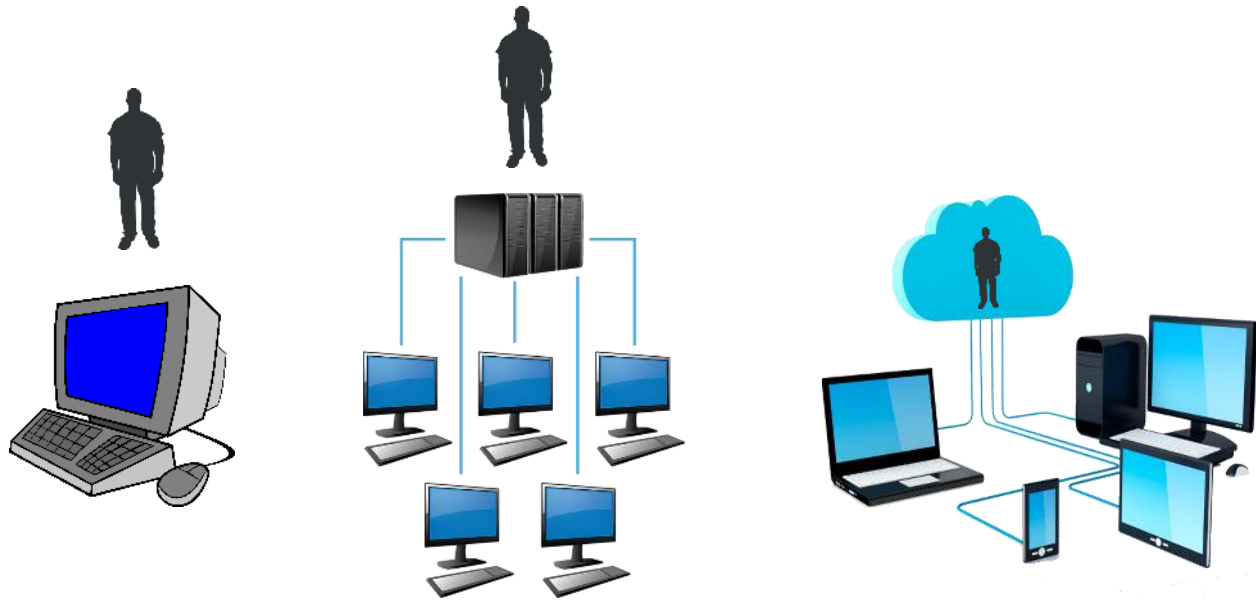
(1) ensuring the highest level of cybersecurity at agencies in the executive branch is the responsibility of the President, followed by the Director of the Office of Management and Budget, the Secretary of Homeland Security, and the head of each such agency;

(2) this responsibility is to be carried out by working collaboratively within and among agencies in the executive branch, industry, and academia;

(3) the strength of the cybersecurity of the Federal Government and the positive benefits of digital technology transformation depend on proactively addressing cybersecurity throughout the acquisition and operation of Internet of Things devices by the Federal Government; and

15 USC 278g–3a note.





TIME

Personally Identifiable Information

Geolocation

The screenshot displays the Strava Global Heatmap interface. At the top, the Strava logo is on the left, and navigation links for Dashboard, Training, Explore, and Challenges are in the center. On the right, there is a 'Start Trial' button, a notification bell, a user profile icon, and a search icon. A search bar in the top right corner contains the text 'San Salvador, San Sal ...'. The main map area shows a heatmap of San Salvador, El Salvador, with a blue location pin in the center. The heatmap is overlaid on a dark map background. On the left side, there is a settings panel titled 'Global Heatmap' with the following options:

- Heatmap Color:** Hot, Blue, Purple (selected), Gray, Red
- Activity Type:** All, Bike, Run, Swim, Snow
- Heat Opacity:** 0%, 40%, 60% (selected), 80%, 100%
- Layers:** Map (selected), Labels
- Map Styles:** Dark (selected), Light, Standard, Satellite, Hybrid, Winter
- Show 3D Terrain:**

At the bottom left of the settings panel, there are links: [Discover](#) how the heatmap was built. and [Learn](#) how Strava Metro can help your community. At the bottom right of the map, there is a copyright notice: © 2023 Strava LLC, Mapbox, OpenStreetMap. Improve this map.

Reduce the Risk!

- Know your risk. Discover IoT devices on the network.
- Patch printers and other easily patchable devices.
- Segment IoT devices across VLANs.
- Enable active monitoring.