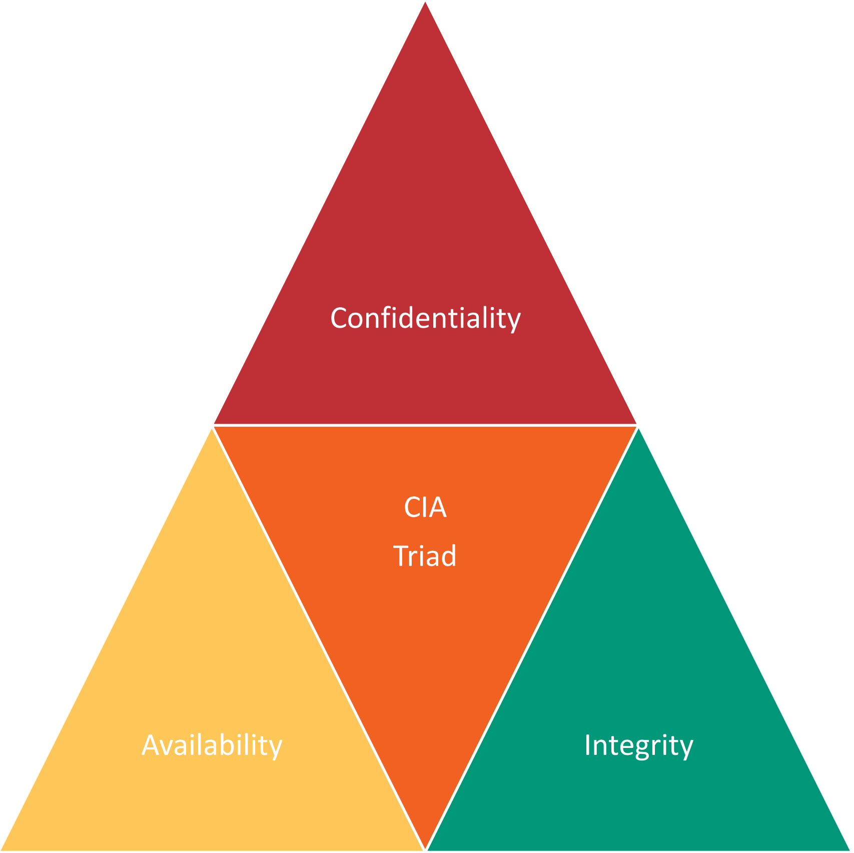
IoT Threats & Security

Goals of Security


Confidentiality

CIA
Triad

Availability

Integrity

IoT Constraints and Limitations

- Low-resources (CPU, RAM, Storage, Power, etc)
- Protocols
- Environment
- Heterogenous

Expanding Attack Surface

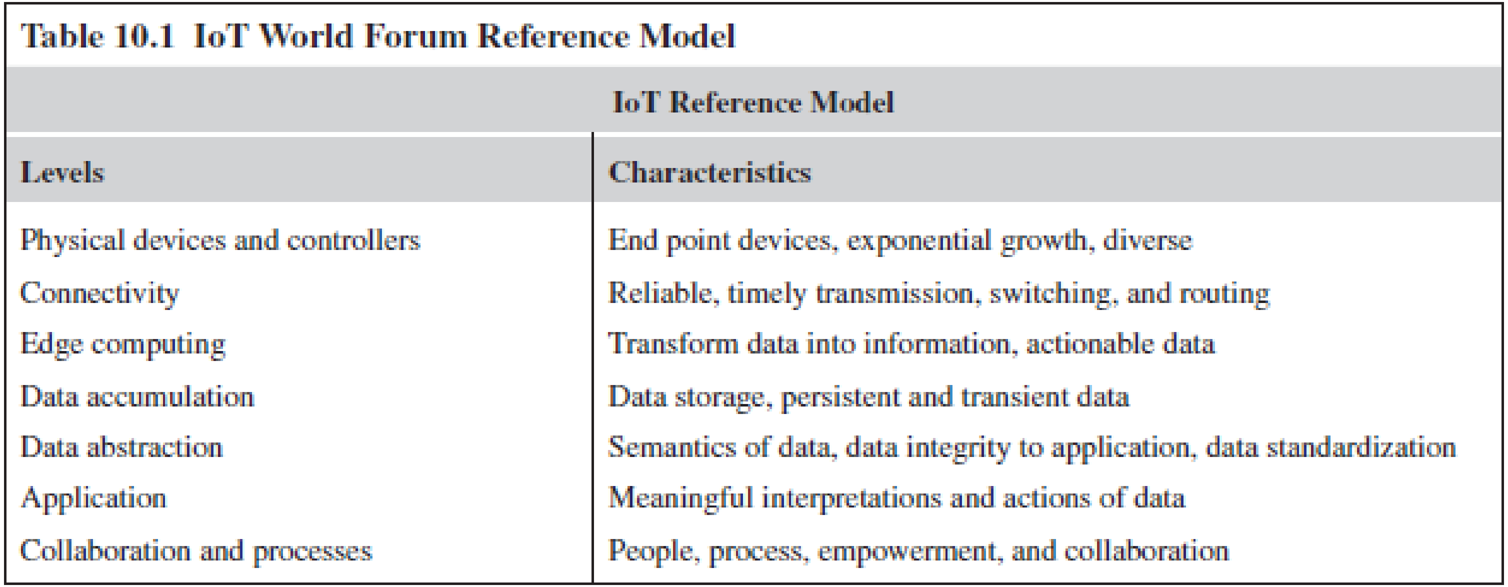


Table 10.1 IoT World Forum Reference Model

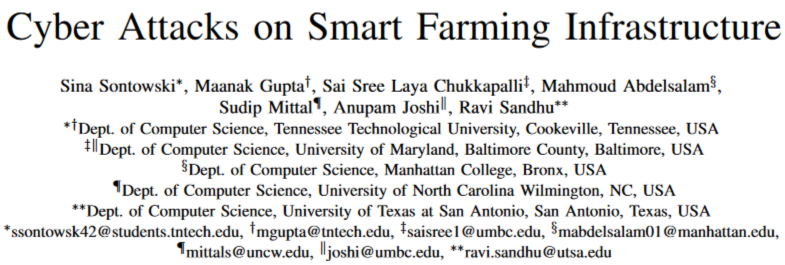
IoT Reference Model	
Levels	**Characteristics**
Physical devices and controllers	End point devices, exponential growth, diverse
Connectivity	Reliable, timely transmission, switching, and routing
Edge computing	Transform data into information, actionable data
Data accumulation	Data storage, persistent and transient data
Data abstraction	Semantics of data, data integrity to application, data standardization
Application	Meaningful interpretations and actions of data
Collaboration and processes	People, process, empowerment, and collaboration

IoT Threats Vs Security

Threats	Security Goals
Capture	Confidentiality
Disrupt	Availability
Manipulate	Integrity

IoT Gateway Security

gateway can extend, and 3 ways
of connecting to the internet



Cyber Attacks on Smart Farming Infrastructure

Sina Sontowski[*], Maanak Gupta[†], Sai Sree Laya Chukkapalli[‡], Mahmoud Abdelsalam[§],
Sudip Mittal[¶], Anupam Joshi[‖], Ravi Sandhu[**]
[*][†]Dept. of Computer Science, Tennessee Technological University, Cookeville, Tennessee, USA
[‡][‖]Dept. of Computer Science, University of Maryland, Baltimore County, Baltimore, USA
[§]Dept. of Computer Science, Manhattan College, Bronx, USA
[¶]Dept. of Computer Science, University of North Carolina Wilmington, NC, USA
[**]Dept. of Computer Science, University of Texas at San Antonio, San Antonio, Texas, USA
[*]ssontowsk42@students.tntech.edu, [†]mgupta@tntech.edu, [‡]saisree1@umbc.edu, [§]mabdelsalam01@manhattan.edu,
[¶]mittals@uncw.edu, [‖]joshi@umbc.edu, [**]ravi.sandhu@utsa.edu

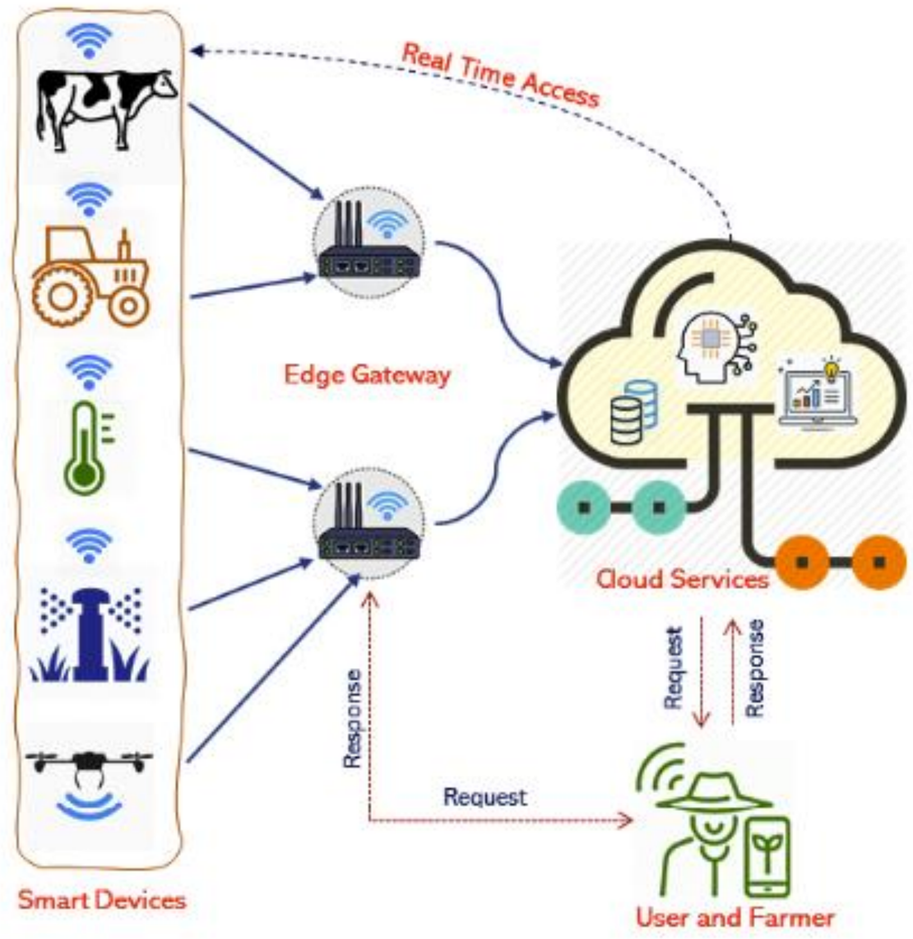
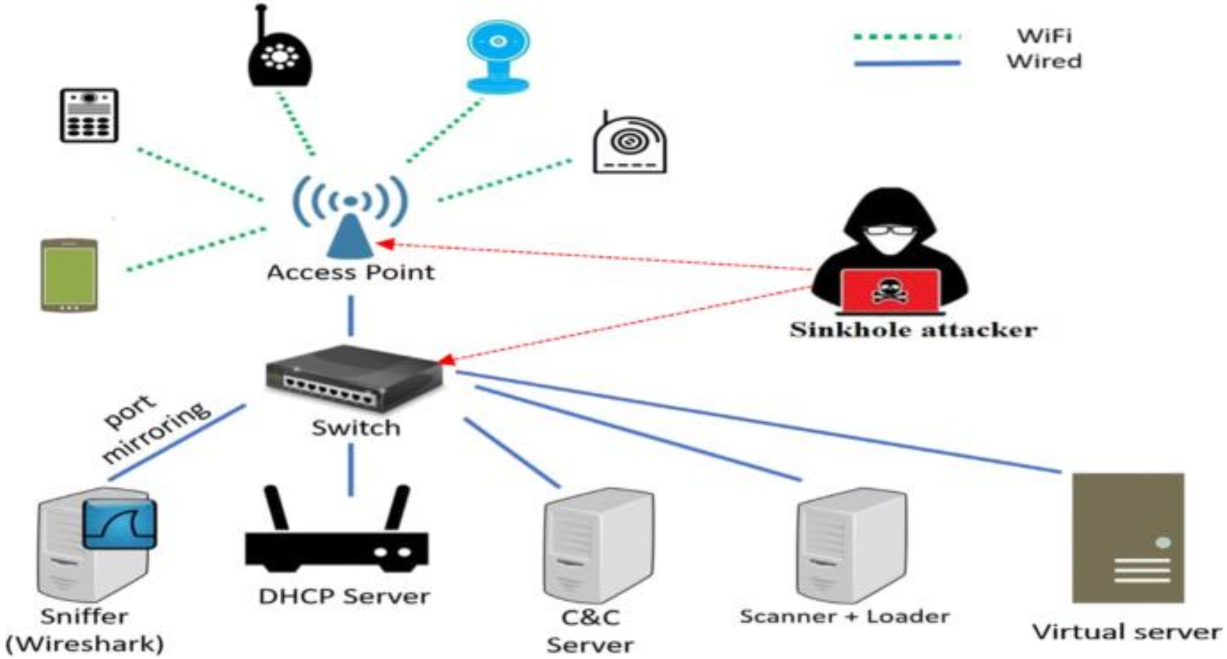
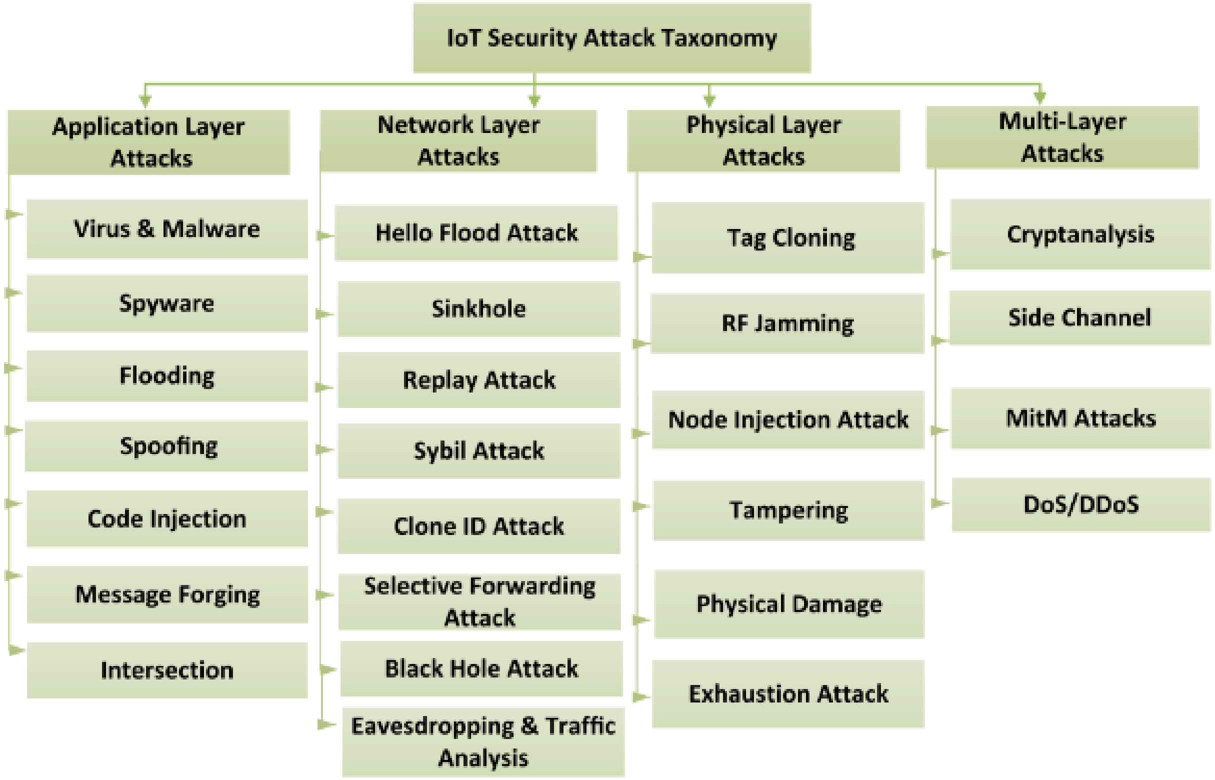


Fig. 1. Smart Farming Conceptual Architecture [10].

IoT Routing Attacks



IoT Attacks Taxonomy



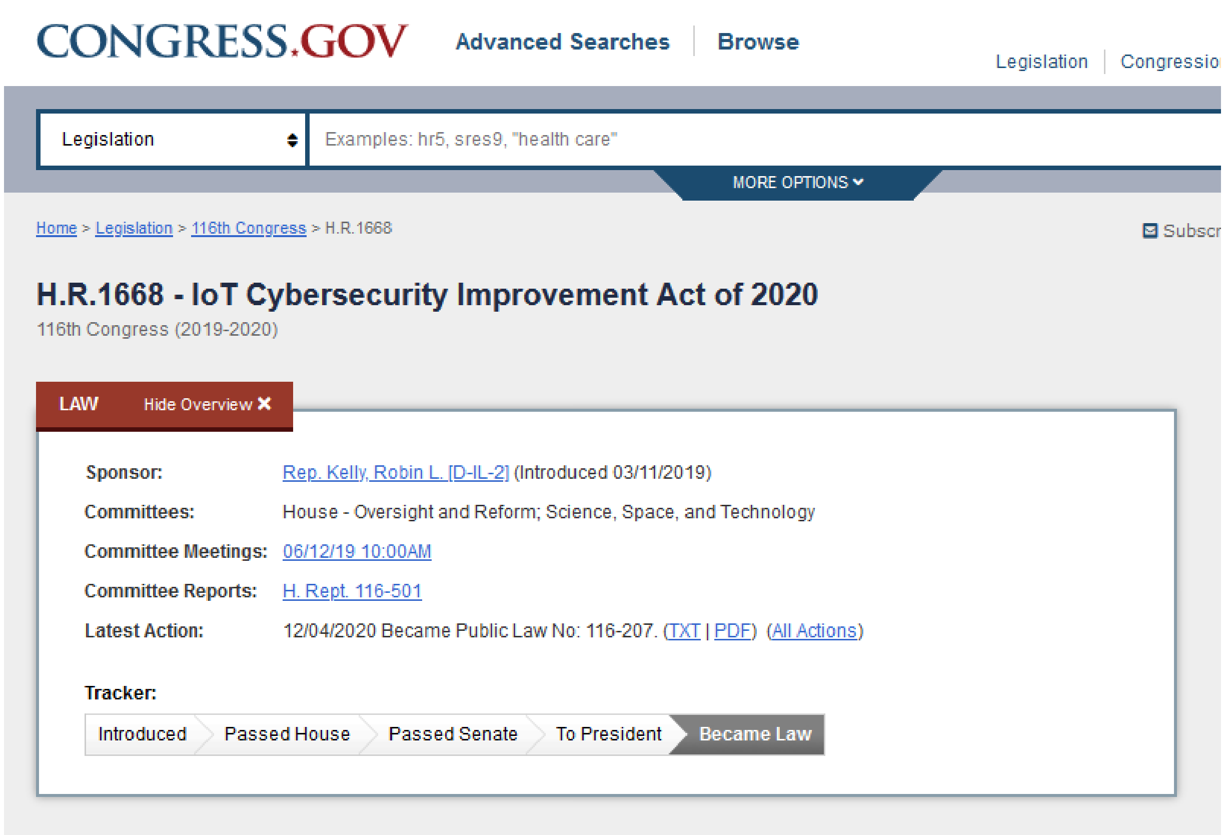
IoT Security Attack Taxonomy

- Application Layer Attacks
  - Virus & Malware
  - Spyware
  - Flooding
  - Spoofing
  - Code Injection
  - Message Forging
  - Intersection
- Network Layer Attacks
  - Hello Flood Attack
  - Sinkhole
  - Replay Attack
  - Sybil Attack
  - Clone ID Attack
  - Selective Forwarding Attack
  - Black Hole Attack
  - Eavesdropping & Traffic Analysis
- Physical Layer Attacks
  - Tag Cloning
  - RF Jamming
  - Node Injection Attack
  - Tampering
  - Physical Damage
  - Exhaustion Attack
- Multi-Layer Attacks
  - Cryptanalysis
  - Side Channel
  - MitM Attacks
  - DoS/DDoS

FIGURE 5. Layer-based IoT security attack taxonomy.

Khanam, et. al. (2020, p.12)

H.R.1668 - IoT Cybersecurity Improvement Act of 2020



Home > Legislation > 116th Congress > H.R.1668

H.R.1668 - IoT Cybersecurity Improvement Act of 2020

116th Congress (2019-2020)

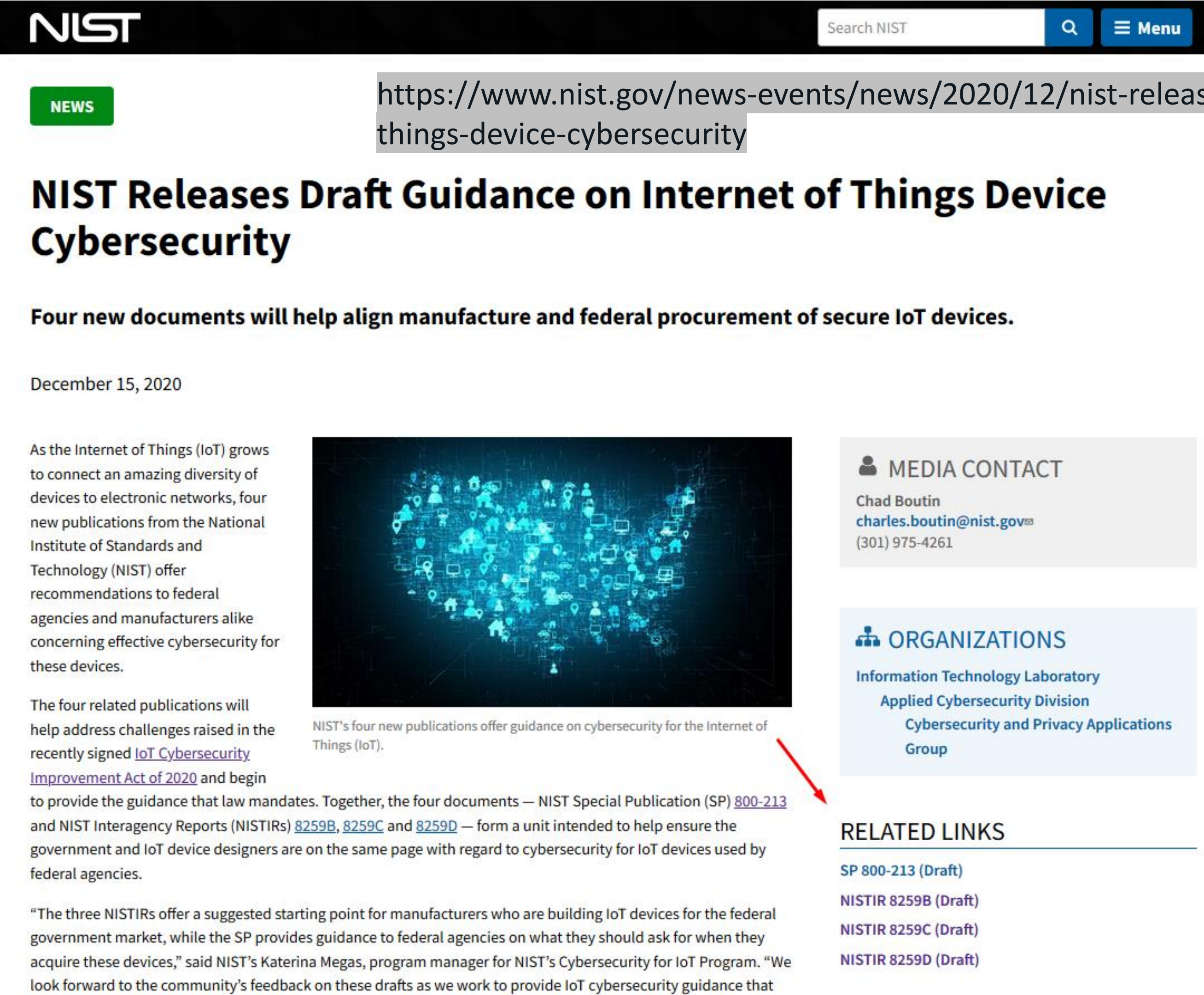
LAW Hide Overview ✖

Sponsor:	Rep. Kelly, Robin L. [D-IL-2] (Introduced 03/11/2019)
Committees:	House - Oversight and Reform; Science, Space, and Technology
Committee Meetings:	06/12/19 10:00AM
Committee Reports:	H. Rept. 116-501
Latest Action:	12/04/2020 Became Public Law No: 116-207. (TXT | PDF) (All Actions)

Tracker:

Introduced > Passed House > Passed Senate > To President > Became Law

https://www.congress.gov/bill/116th-congress/house-bill/1668 https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity



NIST Releases Draft Guidance on Internet of Things Device Cybersecurity

Four new documents will help align manufacture and federal procurement of secure IoT devices.

December 15, 2020

NIST's four new publications offer guidance on cybersecurity for the Internet of Things (IoT).

As the Internet of Things (IoT) grows to connect an amazing diversity of devices to electronic networks, four new publications from the National Institute of Standards and Technology (NIST) offer recommendations to federal agencies and manufacturers alike concerning effective cybersecurity for these devices.

The four related publications will help address challenges raised in the recently signed IoT Cybersecurity Improvement Act of 2020 and begin to provide the guidance that law mandates. Together, the four documents — NIST Special Publication (SP) 800-213 and NIST Interagency Reports (NISTIRs) 8259B, 8259C and 8259D — form a unit intended to help ensure the government and IoT device designers are on the same page with regard to cybersecurity for IoT devices used by federal agencies.

“The three NISTIRs offer a suggested starting point for manufacturers who are building IoT devices for the federal government market, while the SP provides guidance to federal agencies on what they should ask for when they acquire these devices,” said NIST's Katerina Megas, program manager for NIST's Cybersecurity for IoT Program. “We look forward to the community's feedback on these drafts as we work to provide IoT cybersecurity guidance that

MEDIA CONTACT

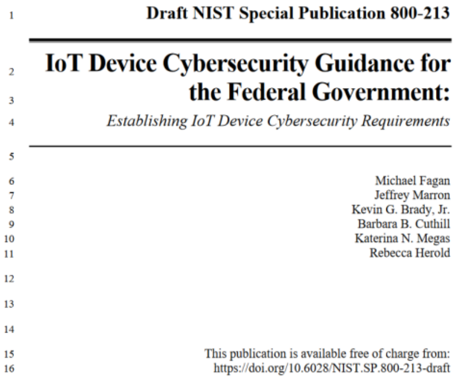
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS

- Information Technology Laboratory
  - Applied Cybersecurity Division
    - Cybersecurity and Privacy Applications Group

RELATED LINKS

- SP 800-213 (Draft)
- NISTIR 8259B (Draft)
- NISTIR 8259C (Draft)
- NISTIR 8259D (Draft)



Draft 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

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